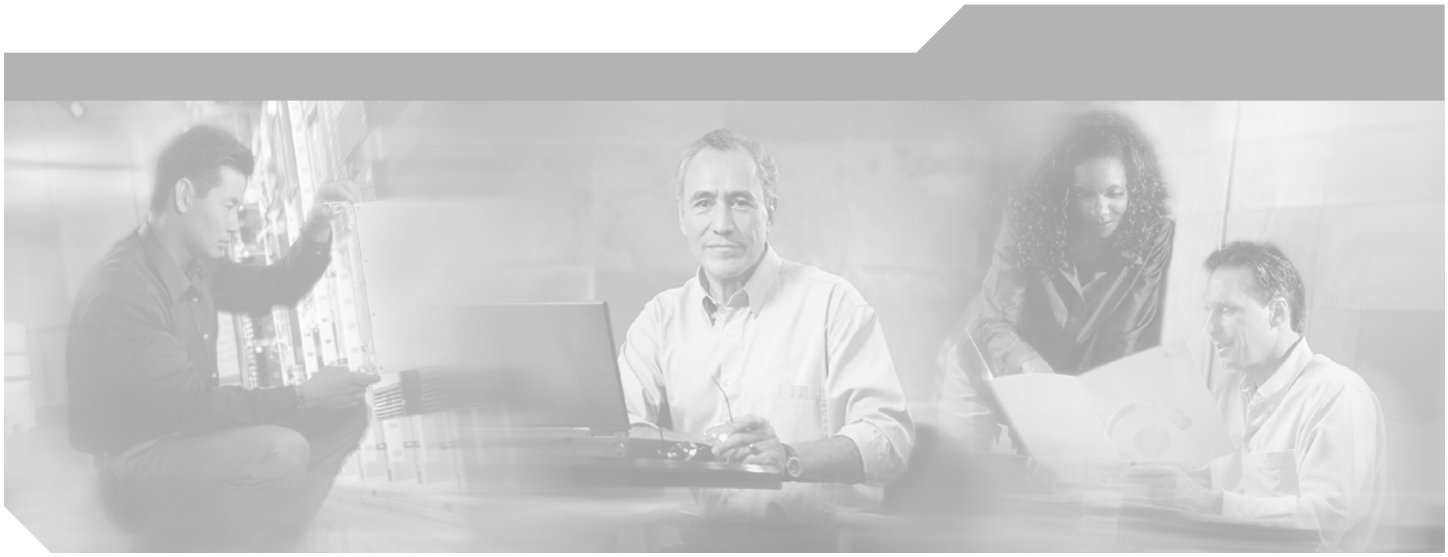

Cisco IOS Security Command Reference

Release 12.3 T

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-4714-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)

Cisco IOS Security Command Reference
Copyright © 2004, Cisco Systems, Inc. All rights reserved.

Introduction SR-1

Security Commands Listed by Technology SR-3

Security Commands SR-23

Introduction

The *Cisco IOS Security Command Reference* contains commands that are used to configure Cisco IOS security features for your Cisco networking devices; specifically, it contains commands used to perform the following functions:

- Configure authentication, authorization, and accounting (AAA).
- Configure security server protocols such as RADIUS, TACACS+, and Kerberos.

Note TACACS and Extended TACACS commands are included in Cisco IOS Release 12.2 software for backward compatibility with earlier Cisco IOS releases; however, these commands are no longer supported and are not documented for this release.

Cisco recommends using only the TACACS+ security protocol with Release 12.1 and later of Cisco IOS software. For a description of TACACS and Extended TACACS commands, refer to the chapter "TACACS, Extended TACACS, and TACACS+ Commands" in Cisco IOS Release 12.0 *Security Command Reference* at Cisco.com.

Table 1 identifies Cisco IOS software commands available to the different versions of TACACS. Although TACACS+ is enabled through AAA and uses commands specific to AAA, there are some commands that are common to TACACS, Extended TACACS, and TACACS+. TACACS and Extended TACACS commands that are not common to TACACS+ are not documented in this release.

Table 1 TACACS Command Comparison

Cisco IOS Command	TACACS	Extended TACACS	TACACS+
aaa accounting	—	—	yes
aaa authentication arap	—	—	yes
aaa authentication enable default	—	—	yes
aaa authentication login	—	—	yes
aaa authentication ppp	—	—	yes
aaa authorization	—	—	yes
aaa group server tacacs+	—	—	yes
aaa new-model	—	—	yes
arap authentication	—	—	yes
arap use-tacacs	yes	yes	—

Table 1 TACACS Command Comparison (continued)

Cisco IOS Command	TACACS	Extended TACACS	TACACS+
enable last-resort	yes	yes	—
enable use-tacacs	yes	yes	—
ip tacacs source-interface	yes	yes	yes
login authentication	—	—	yes
login tacacs	yes	yes	—
ppp authentication	yes	yes	yes
ppp use-tacacs	yes	yes	no
server	—	—	yes
tacacs-server attempts	yes	—	yes
tacacs-server authenticate	yes	yes	—
tacacs-server directed-request	yes	yes	yes
tacacs-server extended	–	yes	—
tacacs-server host	yes	yes	yes
tacacs-server key	—	—	yes
tacacs-server last-resort	yes	yes	—
tacacs-server notify	yes	yes	—
tacacs-server optional-passwords	yes	yes	—
tacacs-server retransmit	yes	yes	—
tacacs-server timeout	yes	yes	yes

- Configure the following traffic filtering and firewall features:
  - Context-Based Access Control (CBAC)
  - Intrusion Detection System (IDS)
  - Port to application mapping (PAM)
  - Reflexive access lists
  - TCP Intercept
- Configures IP Security (IPSec) and encryption features such as public key infrastructure (PKI) and Internet Key Exchange (IKE).
- Configures additional security features such as passwords and privileges, IP Security Options (IPSO), Unicast Reverse Path Forwarding (uRPF), secure shell (SSH), and AutoSecure.

For information on how to configure Cisco IOS security features and configuration examples using the commands in this book, refer to the *Cisco IOS Security Configuration Guide*.

Security Commands Listed by Technology

The following sections list the Cisco IOS Security commands by technology:

- Accounting Commands
- Authentication Commands
- Authentication Proxy Commands
- Authorization Commands
- Certification Authority Interoperability Commands
- Cisco IOS Intrusion Prevention System Commands
- Cisco IOS Secure Infrastructure Commands
- Context-Based Access Control Commands
- Internet Key Exchange Security Protocol Commands
- IPSec Network Security Commands
- IP Security Options Commands
- Kerberos Commands
- Lock-and-Key Commands
- Passwords and Privileges Commands
- Port to Application Mapping Commands
- RADIUS Commands
- Reflexive Access List Commands
- TACACS+ Commands
- TCP Intercept Commands
- Secure Shell Commands
- Unicast Reverse Path Forwarding Commands

Accounting Commands

- **aaa accounting**
- **aaa accounting connection h323**
- **aaa accounting delay-start**

- **aaa accounting nested**
- **aaa accounting resource start-stop group**
- **aaa accounting resource stop-failure group**
- **aaa accounting send stop-record authentication failure**
- **aaa accounting suppress null-username**
- **aaa accounting update**
- **aaa dnis map accounting network**
- **aaa session-id**
- **aaa session-mib**
- **accounting**
- **accounting (gatekeeper)**
- **accounting acknowledge broadcast**
- **ppp accounting**
- **show accounting**

Authentication Commands

- **aaa authentication arap**
- **aaa authentication attempts login**
- **aaa authentication banner**
- **aaa authentication enable default**
- **aaa authentication fail-message**
- **aaa authentication login**
- **aaa authentication password-prompt**
- **aaa authentication ppp**
- **aaa authentication sgbp**
- **aaa authentication username-prompt**
- **aaa dnis map authentication login group**
- **aaa dnis map authentication ppp group**
- **aaa nas redirected-station**
- **aaa new-model**
- **aaa pod server**
- **aaa preauth**
- **aaa processes**
- **access-profile**
- **arap authentication**
- **clear ip trigger-authentication**
- **dnis (authentication)**

- **group (authentication)**
- **ip trigger-authentication (global)**
- **ip trigger-authentication (interface)**
- **login authentication**
- **login block-for**
- **login delay**
- **login on-failure**
- **login on-success**
- **login quiet-mode access-class**
- **ppp authentication**
- **ppp authentication ms-chap-v2**
- **ppp chap hostname**
- **ppp chap password**
- **ppp chap refuse**
- **ppp chap wait**
- **ppp eap identity**
- **ppp eap local**
- **ppp eap password**
- **ppp eap refuse**
- **ppp eap wait**
- **ppp pap refuse**
- **ppp pap sent-username**
- **show ip trigger-authentication**
- **show login**
- **show ppp queues**
- **timeout login response**

Authentication Proxy Commands

- **clear ip auth-proxy cache**
- **ip auth-proxy**
- **ip auth-proxy (interface configuration)**
- **ip auth-proxy auth-proxy-banner**
- **ip auth-proxy name**
- **show ip auth-proxy**

Authorization Commands

- **aaa authorization**
- **aaa authorization config-commands**
- **aaa authorization console**
- **aaa authorization reverse-access**
- **aaa authorization template**
- **aaa dnis map authorization network group**
- **authorization**
- **ppp authorization**

Certification Authority Interoperability Commands

- **authentication command**
- **authentication list (tti-registrar)**
- **authentication terminal**
- **authentication url**
- **authorization list (tti-registrar)**
- **auto-enroll**
- **ca trust-point**
- **cdp-url**
- **certificate**
- **client configuration group**
- **crl**
- **crl optional**
- **crl query**
- **crypto ca authenticate**
- **crypto ca cert validate**
- **crypto ca certificate chain**
- **crypto ca certificate map**
- **crypto ca certificate query (ca-trustpoint)**
- **crypto ca certificate query (global)**
- **crypto ca crl request**
- **crypto ca enroll**
- **crypto ca export pem**
- **crypto ca identity**
- **crypto ca import**
- **crypto ca import pem**

- **crypto ca profile enrollment**
- **crypto ca trusted-root**
- **crypto ca trustpoint**
- **crypto key decrypt rsa**
- **crypto key encrypt rsa**
- **crypto key export pem**
- **crypto key generate rsa (CA)**
- **crypto key import pem**
- **crypto key lock rsa**
- **crypto key unlock rsa**
- **crypto key zeroize rsa**
- **crypto pki authenticate**
- **crypto pki cert validate**
- **crypto pki certificate chain**
- **crypto pki certificate map**
- **crypto pki certificate query (ca-trustpoint)**
- **crypto pki crl request**
- **crypto pki enroll**
- **crypto pki export pem**
- **crypto pki import**
- **crypto pki import pem**
- **crypto pki profile enrollment**
- **crypto pki server**
- **crypto pki server grant**
- **crypto pki server info crl**
- **crypto pki server info requests**
- **crypto pki server password generate**
- **crypto pki server reject**
- **crypto pki server remove**
- **crypto pki server request pkcs10**
- **crypto pki server revoke**
- **crypto pki trustpoint**
- **crypto wui tti petitioner**
- **crypto wui tti registrar**
- **database (certificate server)**
- **database archive**
- **database level**
- **database url**

- **default (ca-trustpoint)**
- **enrollment**
- **enrollment command**
- **enrollment credential**
- **enrollment http-proxy**
- **enrollment mode ra**
- **enrollment profile**
- **enrollment retry count**
- **enrollment retry period**
- **enrollment terminal (ca-profile-enroll)**
- **enrollment terminal (ca-trustpoint)**
- **enrollment url**
- **fqdn (ca-trustpoint)**
- **grant auto trustpoint**
- **grant automatic**
- **grant none**
- **ip-address (ca-trustpoint)**
- **issuer-name**
- **lifetime (certificate server)**
- **lifetime crl**
- **match certificate**
- **match certificate (ca-trustpoint)**
- **match certificate (ISAKMP)**
- **mode ra**
- **ocsp url**
- **override cdp**
- **parameter**
- **password (ca-trustpoint)**
- **pki-server**
- **primary**
- **query certificate**
- **query url**
- **regenerate**
- **revocation-check**
- **root**
- **root CEP**
- **root PROXY**
- **root TFTP**

- **rsakeypair**
- **serial-number (ca-trustpoint)**
- **serial-number (pubkey)**
- **show crypto ca certificates**
- **show crypto ca crls**
- **show crypto ca roots**
- **show crypto ca timers**
- **show crypto ca trustpoints**
- **show crypto pki certificates**
- **show crypto pki crls**
- **show crypto pki server**
- **show crypto pki timers**
- **show crypto pki trustpoints**
- **shutdown**
- **source interface**
- **subject-name**
- **template config**
- **template username**
- **trustpoint**
- **usage**

Cisco IOS Intrusion Prevention System Commands

- **clear ip ips configuration**
- **clear ip sdee**
- **clear ip ips statistics**
- **copy ips-sdf**
- **ip ips**
- **ip ips fail closed**
- **ip ips name**
- **ip ips notify**
- **ip ips po local**[1]
- **ip ips po max-events**[1]
- **ip ips po protected**[1]
- **ip ips po remote**[1]
- **ip ips sdf location**
- **ip ips signature**

1. As of Cisco IOS Release 12.3(11)T, this Cisco IOS IPS command is no longer supported.

- **ip ips signature disable**
- **ip sdee events**
- **ip sdee subscriptions**
- **ip virtual-reassembly**
- **no ip ips sdf builtin**
- **show ip ips**
- **show ip sdee**
- **show ip virtual-reassembly**

Cisco IOS Secure Infrastructure Commands

- **auto secure**
- **bidirectional**
- **incoming**
- **interface (RITE)**
- **ip traffic-export apply profile**
- **ip traffic-export profile**
- **mac-address (RITE)**
- **outgoing**
- **secure boot-config**
- **secure boot-image**
- **show auto secure config**
- **show ip traffic-export**
- **show secure bootset**

Context-Based Access Control Commands

- **clear ip urlfilter cache**
- **ip inspect alert-off**
- **ip inspect audit trail**
- **ip inspect dns-timeout**
- **ip inspect**
- **ip inspect hashtable**
- **ip inspect L2-transparent dhcp-passthrough**
- **ip inspect max-incomplete high**
- **ip inspect max-incomplete low**
- **ip inspect name**
- **ip inspect one-minute high**

- **ip inspect one-minute low**
- **ip inspect tcp finwait-time**
- **ip inspect tcp idle-time**
- **ip inspect tcp max-incomplete host**
- **ip inspect tcp synwait-time**
- **ip inspect udp idle-time**
- **ip urlfilter alert**
- **ip urlfilter allowmode**
- **ip urlfilter audit-trail**
- **ip urlfilter cache**
- **ip urlfilter exclusive-domain**
- **ip urlfilter max-request**
- **ip urlfilter max-resp-pak**
- **ip urlfilter server vendor**
- **ip urlfilter urlf-server-log**
- **no ip inspect**
- **show ip inspect**
- **show ip urlfilter cache**
- **show ip urlfilter config**
- **show ip urlfilter statistics**

Internet Key Exchange Security Protocol Commands

- **access-restrict**
- **acl**
- **address**
- **addressed-key**
- **authentication (IKE policy)**
- **backup-gateway**
- **call admission limit**
- **clear crypto call admission statistics**
- **clear crypto isakmp**
- **clear crypto session**
- **client authentication list**
- **client configuration address**
- **crypto ca export pkcs12**
- **crypto ca import pkcs12**
- **crypto call admission limit**

- **crypto isakmp aggressive-mode disable**
- **crypto isakmp client configuration address-pool local**
- **crypto isakmp client configuration group**
- **crypto isakmp enable**
- **crypto isakmp identity**
- **crypto isakmp keepalive**
- **crypto isakmp key**
- **crypto isakmp peer**
- **crypto isakmp policy**
- **crypto isakmp profile**
- **crypto key generate rsa (IKE)**
- **crypto key pubkey-chain rsa**
- **crypto keyring**
- **crypto map client authentication list**
- **crypto map client configuration address**
- **crypto map isakmp authorization list**
- **crypto map isakmp-profile**
- **crypto pki export pkcs12**
- **crypto pki import pkcs12**
- **description (isakmp peer)**
- **dns**
- **domain (isakmp-group)**
- **encryption (IKE policy)**
- **firewall-are-u-there**
- **group (IKE policy)**
- **group-lock**
- **hash (IKE policy)**
- **include-local-lan**
- **initiate-mode**
- **isakmp authorization list**
- **keepalive (isakmp profile)**
- **key (isakmp-group)**
- **key config-key password-encryption**
- **keyring**
- **key-string (IKE)**
- **lifetime (IKE policy)**
- **match identity**
- **max-logins**

- **max-users**
- **named-key**
- **no crypto xauth**
- **password encryption aes**
- **password logging**
- **pfs**
- **pool (isakmp-group)**
- **pre-shared-key**
- **quit**
- **rsa-pubkey**
- **save-password**
- **self-identity**
- **serial-number**
- **set aggressive-mode client-endpoint**
- **set aggressive-mode password**
- **set isakmp-profile**
- **show call admission statistics**
- **show crypto call admission statistics**
- **show crypto isakmp key**
- **show crypto isakmp peer**
- **show crypto isakmp policy**
- **show crypto isakmp profile**
- **show crypto isakmp sa**
- **show crypto key mypubkey rsa**
- **show crypto key pubkey-chain rsa**
- **show crypto session**
- **show crypto session group**
- **show crypto session summary**
- **split-dns**
- **vrf (isakmp profile)**
- **wins**

IPSec Network Security Commands

- **aaa authentication dot1x**
- **aaa authentication eou default enable group radius**
- **access-group (identity policy)**
- **auth-type**

- **clear crypto engine accelerator counter**
- **clear crypto ipsec client ezvpn**
- **clear crypto sa**
- **clear dot1x**
- **clear eou**
- **clear ip admission cache**
- **crypto dynamic-map**
- **crypto engine accelerator**
- **crypto identity**
- **crypto ipsec client ezvpn (global)**
- **crypto ipsec client ezvpn (interface)**
- **crypto ipsec client ezvpn connect**
- **crypto ipsec client ezvpn xauth**
- **crypto ipsec df-bit (global)**
- **crypto ipsec df-bit (interface)**
- **crypto ipsec fragmentation**
- **crypto ipsec fragmentation (interface)**
- **crypto ipsec optional**
- **crypto ipsec optional retry**
- **crypto ipsec profile**
- **crypto ipsec security-association lifetime**
- **crypto ipsec transform-set**
- **crypto isakmp invalid-spi-recovery**
- **crypto isamkp nat keepalive**
- **crypto map (global IPSec)**
- **crypto map (interface IPSec)**
- **crypto map local-address**
- **crypto map redundancy replay-interval**
- **crypto mib ipsec flowmib history failure size**
- **crypto mib ipsec flowmib history tunnel size**
- **crypto set security-association idle-time**
- **debug ip admission eapoudp**
- **description (dot1x profile)**
- **description (identity policy)**
- **description (identity profile)**
- **device (identity profile)**
- **dn**
- **dot1x default**

- **dot1x initialize**
- **dot1x max-req**
- **dot1x max-start**
- **dot1x multiple hosts**
- **dot1x pae**
- **dot1x port-control**
- **dot1x re-authenticate**
- **dot1x re-authenticate (EtherSwitch)**
- **dot1x reauthentication**
- **dot1x re-authentication (EtherSwitch)**
- **dot1x system-auth-control**
- **dot1x timeout**
- **dot1x timeout (EtherSwitch)**
- **eap**
- **eou allow**
- **eou clientless**
- **eou default**
- **eou initialize**
- **eou logging**
- **eou max-retry**
- **eou port**
- **eou rate-limit**
- **eou revalidate**
- **eou timeout**
- **fqdn (crypto identity)**
- **identity**
- **identity policy**
- **identity profile**
- **identity profile eapoudp**
- **ip admission**
- **ip admission name**
- **ip http ezvpn**
- **match address (IPSec)**
- **mode (IPSec)**
- **qos-group**
- **redirect (identity policy)**
- **redundancy stateful**
- **reverse-route**

- **security ipsec**
- **set ip access-group**
- **set peer (IPSec)**
- **set pfs**
- **set security-association level per-host**
- **set security-association lifetime**
- **set session-key**
- **set transform-set**
- **show crypto debug-condition**
- **show crypto dynamic-map**
- **show crypto engine accelerator logs**
- **show crypto engine accelerator ring**
- **show crypto engine accelerator sa-database**
- **show crypto engine accelerator statistic**
- **show crypto ha**
- **show crypto ipsec client ezvpn**
- **show crypto ipsec sa**
- **show crypto ipsec security-association lifetime**
- **show crypto ipsec transform-set**
- **show crypto map (IPSec)**
- **show crypto mib ipsec flowmib history failure size**
- **show crypto mib ipsec flowmib history tunnel size**
- **show crypto mib ipsec flowmib version**
- **show dot1x**
- **show dot1x (EtherSwitch)**
- **show eou**
- **show ip admission**
- **snmp-server enable traps ipsec**
- **snmp-server enable traps isakmp**
- **template**
- **template (identity policy)**
- **tunnel protection**

IP Security Options Commands

- **dnsix-dmdp retries**
- **dnsix-nat authorized-redirection**
- **dnsix-nat primary**

- **dnsix-nat secondary**
- **dnsix-nat source**
- **dnsix-nat transmit-count**
- **ip security add**
- **ip security aeso**
- **ip security dedicated**
- **ip security eso-info**
- **ip security eso-max**
- **ip security eso-min**
- **ip security extended-allowed**
- **ip security first**
- **ip security ignore-authorities**
- **ip security implicit-labelling**
- **ip security multilevel**
- **ip security reserved-allowed**
- **ip security strip**
- **show dnsix**

Kerberos Commands

- **clear kerberos creds**
- **kerberos clients mandatory**
- **kerberos credentials forward**
- **kerberos instance map**
- **kerberos local-realm**
- **kerberos preauth**
- **kerberos realm**
- **kerberos server**
- **kerberos srvtab entry**
- **kerberos srvtab remote**
- **key config-key**
- **show kerberos creds**

Lock-and-Key Commands

- **access-enable**
- **access-list dynamic-extend**
- **access-template**

- **clear access-template**

Passwords and Privileges Commands

- **commands (view)**
- **enable password**
- **enable secret**
- **li-view**
- **name (view)**
- **parser view**
- **parser view superview**
- **password**
- **password 5**
- **privilege**
- **privilege level**
- **security authentication failure rate**
- **security passwords min-length**
- **service password-encryption**
- **show parser view**
- **show privilege**
- **username**
- **username secret**
- **view**

Port to Application Mapping Commands

- **ip port-map**
- **show ip port-map**

RADIUS Commands

- **aaa attribute**
- **aaa authorization cache filterserver**
- **aaa filterserver**
- **aaa group server radius**
- **aaa nas port extended**
- **aaa user profile**
- **accounting (server-group)**

- **attribute (server-group)**
- **authorization (server-group)**
- **block count**
- **cache clear age**
- **cache disable**
- **cache max**
- **cache refresh**
- **call guard-timer**
- **clear aaa cache filterserver acl**
- **clear radius local-server**
- **clid**
- **ctype**
- **deadtime (server-group configuration)**
- **dialer aaa**
- **dnis (RADIUS)**
- **dnis bypass (AAA preauthentication configuration)**
- **group (local RADIUS server)**
- **group (RADIUS)**
- **ip radius source-interface**
- **ip vrf forwarding (server-group)**
- **nas**
- **password**
- **radius-server attribute 4**
- **radius-server attribute 8 include-in-access-req**
- **radius-server attribute 11 direction default**
- **radius-server attribute 32 include-in-access-req**
- **radius-server attribute 44 extend-with-addr**
- **radius-server attribute 44 include-in-access-req**
- **radius-server attribute 44 sync-with-client**
- **radius-server attribute 55 include-in-acct-req**
- **radius-server attribute 6 mandatory**
- **radius-server attribute 69 clear**
- **radius-server attribute 188 format non-standard**
- **radius-server attribute list**
- **radius-server attribute nas-port extended**
- **radius-server attribute nas-port format**
- **radius-server challenge-noecho**
- **radius-server configure-nas**

- **radius-server dead-criteria**
- **radius-server deadtime**
- **radius-server directed-request**
- **radius-server domain-stripping**
- **radius-server extended-portnames**
- **radius-server host**
- **radius-server host non-standard**
- **radius-server key**
- **radius-server local**
- **radius-server optional passwords**
- **radius-server retransmit**
- **radius-server timeout**
- **radius-server unique-ident**
- **radius-server vsa send**
- **reauthentication time**
- **server (RADIUS)**
- **server-private (RADIUS)**
- **show aaa attributes**
- **show aaa cache filterserver**
- **show aaa dead-criteria**
- **show aaa server-private**
- **show aaa servers**
- **show radius local-server statistics**
- **show radius statistics**
- **show wlccp wds**
- **ssid**
- **test aaa group**
- **user**
- **vlan**
- **vpdn aaa attribute nas-port vpdn-nas**
- **wlccp authentication-server client**
- **wlccp authentication-server infrastructure**
- **wlccp wds priority interface**

Reflexive Access List Commands

- **evaluate**
- **ip reflexive-list timeout**

- **permit (reflexive)**

TACACS+ Commands

- **aaa group server tacacs+**
- **ip tacacs source-interface**
- **server (TACACS+)**
- **server-private (TACACS+)**
- **show tacacs**
- **tacacs-server directed-request**
- **tacacs-server host**
- **tacacs-server key**

TCP Intercept Commands

- **ip tcp intercept connection-timeout**
- **ip tcp intercept drop-mode**
- **ip tcp intercept finrst-timeout**
- **ip tcp intercept list**
- **ip tcp intercept max-incomplete high**
- **ip tcp intercept max-incomplete low**
- **ip tcp intercept mode**
- **ip tcp intercept one-minute high**
- **ip tcp intercept one-minute low**
- **ip tcp intercept watch-timeout**
- **show tcp intercept connections**
- **show tcp intercept statistics**

Secure Shell Commands

- **disconnect ssh**
- **ip scp server enable**
- **ip ssh**
- **ip ssh port**
- **ip ssh rsa keypair-name**
- **ip ssh version**
- **show ip ssh**
- **show ssh**

- **ssh**

Unicast Reverse Path Forwarding Commands

- **ip verify unicast reachable-via**

Security Commands

This book presents the commands to configure and maintain Cisco IOS security features. The commands are presented in alphabetical order. Some commands required for configuring security features may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa accounting {**auth-proxy** | **system | network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*

no aaa accounting {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] [**broadcast**] **group** *groupname*

Syntax Description

auth-proxy	Provides information about all authenticated-proxy user events.
system	Performs accounting for all system-level events not associated with users, such as reloads.
network	Runs accounting for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Protocols (NCPs), and AppleTalk Remote Access Protocol (ARAP).
exec	Runs accounting for EXEC shell session. This keyword might return user profile information such as what is generated by the **autocommand** command.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler and disassembler (PAD), and rlogin.
commands *level*	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
default	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
list-name	Character string used to name the list of at least one of the accounting methods described in Table 2.
vrf *vrf-name*	(Optional) Specifies a virtual route forwarding (VRF) configuration. **Note** VRF is used *only* with system accounting.
start-stop	Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process begins regardless of whether the “start” accounting notice was received by the accounting server.
stop-only	Sends a “stop” accounting notice at the end of the requested user process.
none	Disables accounting services on this line or interface.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, fail over occurs using the backup servers defined within that group.
group *group-name*	At least one of the keywords described in Table 3.

Defaults

AAA accounting is disabled.

Command Modes Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support was added.
12.1(1)T	The **broadcast** keyword was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.
12.1(5)T	The **auth-proxy** keyword was added.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were integrated into Cisco IOS Release 12.2(13)T.
12.2(15)B	The tunnel and tunnel-link accounting methods were introduced.
12.3(4)T	The tunnel and tunnel-link accounting methods were integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines Use the **aaa accounting** command to enable accounting and to create named method lists that define specific accounting methods on a per-line or per-interface basis.

Table 2 contains descriptions of keywords for aaa accounting methods.

Table 2 aaa accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name*.

In Table 2, the **group radius** and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Cisco IOS software supports the following two methods of accounting:

- RADIUS—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- TACACS+—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering the *list-name* and the *method*, where *list-name* is any character string used to name this list (excluding the names of methods, such as radius or tacacs+) and *method* identifies the methods to be tried in sequence as given.

If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

Named accounting method lists are specific to the indicated type of accounting. Method list keywords are described in Table 3.

Table 3 aaa accounting Method List Keywords

Keyword	Description
auth-proxy	Creates a method list to provide accounting information about all authenticated hosts that use the authentication proxy service.
commands	Creates a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level.
connection	Creates a method list to provide accounting information about all outbound connections made from the network access server.
exec	Creates a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times.
network	Creates a method list to provide accounting information for SLIP, PPP, NCPs, and ARAP sessions.
resource	Creates a method list to provide accounting records for calls that have passed user authentication or calls that failed to be authenticated.
tunnel	Creates a method list to provide accounting records (Tunnel-Start, Tunnel-Stop, and Tunnel-Reject) for virtual private dialup network (VPDN) tunnel status changes.
tunnel-link	Creates a method list to provide accounting records (Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject) for VPDN tunnel-link status changes.

Note System accounting does not use named accounting lists; you can define the default list only for system accounting.

For minimal accounting, include the **stop-only** keyword to send a “stop” record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a “start” accounting notice at the beginning of the requested process and a “stop” accounting notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. The **none** keyword disables accounting services for the specified line or interface.

To specify an accounting configuration for a particular VRF, specify a default system accounting method list, and use the **vrf** keyword and *vrf-name* argument. System accounting does not have knowledge of VRF unless specified.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes, refer to the appendix "RADIUS Attributes Overview" in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, refer to the appendix "TACACS+ Attribute-Value Pairs" in the *Cisco IOS Security Configuration Guide*.

Note This command cannot be used with TACACS or extended TACACS.

Examples

The following example defines a default commands accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction.

```
aaa accounting commands 15 default stop-only group tacacs+
```

The following example defines a default auth-proxy accounting method list, where accounting services are provided by a TACACS+ security server with a start-stop restriction. The **aaa accounting** command activates authentication proxy accounting.

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization auth-proxy default group tacacs+
aaa accounting auth-proxy default start-stop group tacacs+
```

The following example defines a default system accounting method list, where accounting services are provided by RADIUS security server "sg_water" with a start-stop restriction. The **aaa accounting** command specifies accounting for vrf "water."

```
aaa accounting system default vrf water start-stop group sg_water
```

The following example shows how to enable network accounting and send tunnel and tunnel-link accounting records to the RADIUS server. (Tunnel-Reject and Tunnel-Link-Reject accounting records are automatically sent if either start or stop records are configured.)

```
aaa accounting network tunnel start-stop group radius
aaa accounting network session start-stop group radius
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ server host.

aaa accounting connection h323

To define the accounting method list H.323with RADIUS as a method with either **stop-only** or **start-stop** accounting options, use the **aaa accounting connection h323** command in global configuration mode. To disable the use of this accounting method list, use the **no** form of this command.

aaa accounting connection h323 {**stop-only** | **start-stop** | **none**} [**broadcast**] **group** *groupname*

no aaa accounting connection h323 {**stop-only** | **start-stop** | **none**} [**broadcast**] **group** *groupname*

Syntax Description

stop-only	Sends a "stop" accounting notice at the end of the requested user process.
start-stop	Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.
none	Disables accounting services on this line or interface.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
group *groupname*	Specifies the server group to be used for accounting services. The following are valid server group names: • *string*: Character string used to name a server group. • **radius**: Uses list of all RADIUS hosts. • **tacacs+**: Uses list of all TACACS+ hosts.

Defaults

No accounting method list

Command Modes

Global configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced.

Usage Guidelines

This command creates a method list called h323 and is applied by default to all voice interfaces if the **gw-accounting h323** command is also activated.

Examples

The following example enables authentication, authorization, and accounting (AAA) services, gateway accounting services, and defines a connection accounting method list (h323). The h323 accounting method lists specifies that RADIUS is the security protocol that will provide the accounting services, and that the RADIUS service will track start-stop records.

```
aaa new model
gw-accounting h323
aaa accounting connection h323 start-stop radius
```

aaa accounting delay-start

To delay generation of accounting "start" records until the user IP address is established, use the **aaa accounting delay-start** command in global configuration mode. To disable this functionality, use the **no** form of this command.

aaa accounting delay-start [all] [**vrf** *vrf-name*]

no aaa accounting delay-start [all] [**vrf** *vrf-name*]

Syntax Description

all	(Optional) Extends the delay of accounting "start" records to all Virtual Route Forwarding (VRF) and non-VRF users.
vrf *vrf-name*	(Optional) Extends the delay of accounting "start" records to individual VRF users.

Defaults

Accounting records are not delayed.

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were integrated into Cisco IOS Release 12.2(13)T.
12.3(1)	The **all** keyword was added.

Usage Guidelines

Use the **aaa accounting delay-start** command to delay generation of accounting "start" records until the IP address of the user has been established. Use the **vrf** *vrf-name* keyword and argument to delay accounting "start" records for individual Virtual Private Network (VPN) routing and forwarding (VRF) users or use the **all** keyword for all VRF and non-VRF users.

Examples

The following example shows how to delay accounting "start" records until the IP address of the user is established:

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop radius
aaa accounting delay-start
radius-server host 172.16.0.0 non-standard
radius-server key rad123
```

The following example shows that accounting "start" records are to be delayed to all VRF and non-VRF users:

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop radius
aaa accounting delay-start all
radius-server host 172.16.0.0 non-standard
```
radius-server key rad123

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ server host.

aaa accounting gigawords

To enable authentication, authorization, and accounting (AAA) 64-bit, high-capacity counters, use the **aaa accounting gigawords** command in global configuration mode. To disable the counters, use the **no** form of this command. (Note that gigaword support is automatically configured unless you unconfigure it using the **no** form of the command.)

aaa accounting gigawords

no aaa accounting gigawords

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, the 64-bit, high-capacity counters that support RADIUS attributes 52 and 53 are automatically enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13.7)T	This command was introduced.

Usage Guidelines

The AAA high-capacity counter process takes approximately 8 percent CPU memory for 24,000 (24 K) sessions running under steady state.

If you have entered the **no** form of this command to turn off the 64-bit counters and you want to reenable them, you will need to enter the **aaa accounting gigawords** command. Also, once you have entered the **no form of the command**, it takes a reload of the router to actually disable the use of the 64-bit counters.

Note The **aaa accounting gigawords** command does not show up in the running configuration unless the **no** form of the command is used in the configuration.

Examples

The following example shows that the AAA 64-bit counters have been disabled:

```
no aaa accounting gigawords
```

aaa accounting nested

To specify that NETWORK records be generated, or nested, within EXEC "start" and "stop" records for PPP users who start EXEC terminal sessions, use the **aaa accounting nested** command in global configuration mode. To allow the sending of records for users with a NULL username, use the **no** form of this command.

aaa accounting nested

no aaa accounting nested

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use this command when you want to specify that NETWORK records be nested within EXEC "start" and "stop" records, such as for PPP users who start EXEC terminal sessions. In some cases, such as billing customers for specific services, is can be desirable to keep NETWORK "start" and "stop" records together, essentially nesting them within the framework of the EXEC "start" and "stop" messages. For example, a user dialing in using PPP can create the following records: EXEC-start, NETWORK-start, EXEC-stop, NETWORK-stop. By nesting the accounting records, NETWORK-stop records follow NETWORK-start messages: EXEC-start, NETWORK-start, NETWORK-stop, EXEC-stop.

Examples

The following example enables nesting of NETWORK accounting records for user sessions:

```
aaa accounting nested
```

aaa accounting resource start-stop group

To enable full resource accounting, which will generate both a "start" record at call setup and a "stop" record at call termination, use the **aaa accounting resource start-stop group** command in global configuration mode. To disable full resource accounting, use the **no** form of this command.

aaa accounting resource *method-list* **start-stop** [**broadcast**] **group** *groupname*

no aaa accounting resource *method-list* **start-stop** [**broadcast**] **group** *groupname*

Syntax Description

method-list	Method used for accounting services. Use one of the following options: • **default**: Uses the listed accounting methods that follow this argument as the default list of methods for accounting services. • *string*: Character string used to name the list of accounting methods.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
groupname	Specifies the server group to be used for accounting services. The following are valid server group names: • *string*: Character string used to name a server group. • **radius**: Uses list of all RADIUS hosts. • **tacacs+**: Uses list of all TACACS+ hosts.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Use the **aaa accounting resource start-stop group** command to send a "start" record at each call setup followed with a corresponding "stop" record at the call disconnect. There is a separate "call setup-call disconnect "start-stop" accounting record tracking the progress of the resource connection to the device, and a separate "user authentication start-stop accounting" record tracking the user management progress. These two sets of accounting records are interlinked by using a unique session ID for the call.

You may want to use this command to manage and monitor wholesale customers from one source of data reporting, such as accounting records.

Note Sending "start-stop" records for resource allocation along with user "start-stop" records during user authentication can lead to serious performance issues and is discouraged unless absolutely required.

All existing AAA accounting method list and server group options are made available to this command.

Examples

The following example shows how to configure resource accounting for "start-stop" records:

```
aaa new-model
aaa authentication login AOL group radius local
aaa authentication ppp default group radius local
aaa authorization exec AOL group radius if-authenticated
aaa authorization network default group radius if-authenticated
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting resource default start-stop group radius
```

Related Commands

Command	Description
aaa accounting start-stop failure	Enables resource failure stop accounting support, which will only generate a stop record at any point prior to user authentication if a call is terminated.

aaa accounting resource stop-failure group

To enable resource failure stop accounting support, which will generate a "stop" record at any point prior to user authentication only if a call is terminated, use the **aaa accounting resource stop-failure group** command in global configuration mode. To disable resource failure stop accounting, use the **no** form of this command.

aaa accounting resource *method-list* **stop-failure** [**broadcast**] **group** *groupname*

no aaa accounting resource *method-list* **stop-failure** [**broadcast**] **group** *groupname*

Syntax Description

method-list	Method used for accounting services. Use one of the following options: • **default**: Uses the listed accounting methods that follow this argument as the default list of methods for accounting services. • *string*: Character string used to name the list of accounting methods.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
groupname	Group to be used for accounting services. Use one of the following options: • *string*: Character string used to name a server group. • **radius**: Uses list of all RADIUS hosts. • **tacacs+**: Uses list of all TACACS+ hosts.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Use the **aaa accounting resource stop-failure group** command to generate a "stop" record for any calls that do not reach user authentication; this function creates "stop" accounting records for the moment of call setup. All calls that pass user authentication will behave as before; that is, no additional accounting records will be seen.

All existing authentication, authorization, and accounting (AAA) accounting method list and server group options are made available to this command.

Examples

The following example shows how to configure "stop" accounting records from the moment of call setup:

```
aaa new-model
aaa authentication login AOL group radius local
aaa authentication ppp default group radius local
aaa authorization exec AOL group radius if-authenticated
aaa authorization network default group radius if-authenticated
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting resource default stop-failure group radius
```

Related Commands

Command	Description
aaa accounting resource start-stop group	Enables full resource accounting, which will generate both a “start” record at call setup and a “stop” record at call termination.

aaa accounting send stop-record authentication failure

To generate accounting "stop" records for users who fail to authenticate at login or during session negotiation, use the **aaa accounting send stop-record authentication failure** command in global configuration mode. To stop generating records for users who fail to authenticate at login or during session negotiation, use the **no** form of this command.

aaa accounting send stop-record authentication failure [**vrf** *vrf-name*]

no aaa accounting send stop-record authentication failure

Syntax Description

vrf *vrf-name*	(Optional) Virtual Route Forwarding (VRF) configuration.

Defaults

The "stop" records are not generated.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to generate accounting "stop" records for users who fail to authenticate at login or during session negotiation. When the **aaa accounting** command is activated, by default the Cisco IOS software does not generate accounting records for system users who fail login authentication or who succeed in login authentication but fail PPP negotiation for some reason.

Use the **vrf** *vrf-name* keyword and argument to generate accounting "stop" records per Virtual Private Network (VPN) routing and forwarding (VRF) configuration.

Examples

The following example shows how to generate "stop" records for users who fail to authenticate at login or during session negotiation:

```
aaa accounting send stop-record authentication failure
```

aaa accounting session-duration ntp-adjusted

To calculate RADIUS attribute 46, Acct-Sess-Time, on the basis of the Network Time Protocol (NTP) clock time, use the **aaa accounting session-duration ntp-adjusted** command in global configuration mode. To disable the calculation that was configured on the basis of the NTP clock time, use the **no** form of this command.

aaa accounting session-duration ntp-adjusted

no aaa accounting session-duration ntp-adjusted

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, RADIUS attribute 46 is calculated on the basis of the 64-bit monotonically increasing counter, which is not NTP adjusted.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

If this command is not configured, RADIUS attribute 46 can skew the session time by as much as 5 to 7 seconds for calls that have a duration of more than 24 hours. However, you may not want to configure the command for short-lived calls or if your device is up for only a short time because of the convergence time required if the session time is configured on the basis of the NTP clock time.

For RADIUS attribute 46 to reflect the NTP-adjusted time, you must configure the **ntp server** command as well as the **aaa accounting session-duration ntp-adjusted** command.

Examples

The following example shows that the attribute 46 session time is to be calculated on the basis of the NTP clock time:

```
aaa new-model
aaa authentication ppp default group radius
aaa accounting session-time ntp-adjusted
aaa accounting network default start-stop group radius
```

Related Commands

Command	Description
ntp server	Allows the software clock to be synchronized by a NTP time server.

aaa accounting suppress null-username

To prevent the Cisco IOS software from sending accounting records for users whose username string is NULL, use the **aaa accounting suppress null-username** command in global configuration mode. To allow sending records for users with a NULL username, use the **no** form of this command.

aaa accounting suppress null-username

no aaa accounting suppress null-username

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When **aaa accounting** is activated, the Cisco IOS software issues accounting records for all users on the system, including users whose username string, because of protocol translation, is NULL. This command prevents accounting records from being generated for those users who do not have usernames associated with them.

Examples

The following example supresses accounting records for users who do not have usernames associated with them:

```
aaa accounting suppress null-username
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

aaa accounting update

To enable periodic interim accounting records to be sent to the accounting server, use the **aaa accounting update** command in global configuration mode. To disable interim accounting updates, use the **no** form of this command.

aaa accounting update [newinfo] [periodic *number* **[jitter {maximum** ***max-value*****}]]**

no aaa accounting update

Syntax Description

newinfo	(Optional) An interim accounting record is sent to the accounting server whenever there is new accounting information to report relating to the user in question.
periodic	(Optional) An interim accounting record is sent to the accounting server periodically, as defined by the argument *number.*
number	(Optional) Integer specifying number of minutes.
jitter	(Optional) Allows you to set the maximum jitter value in periodic accounting.
maximum ***max-value***	(Required) The number of seconds to set for maximum jitter in periodic accounting. The value 0 turns off jitter. Jitter is set to 300 seconds (5 minutes) by default.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(13)T	Introduced support for generation of an additional updated interim accounting record that contains all available attributes when a call leg is connected.
12.2(15)T11	The **jitter** keyword was added.

Usage Guidelines

- When the **aaa accounting update** command is activated, the Cisco IOS software issues interim accounting records for all users on the system. If the **newinfo** keyword is used, interim accounting records will be sent to the accounting server every time there is new accounting information to report. An example of this would be when IP Control Protocol (IPCP) completes IP address negotiation with the remote peer. The interim accounting record will include the negotiated IP address used by the remote peer.
- When the **gw-accounting aaa** command and the **aaa accounting update newinfo** command and keyword are activated, Cisco IOS software generates and sends an additional updated interim accounting record to the accounting server when a call leg is connected. All attributes (for example, h323-connect-time and backward-call-indicators) available at the time of call connection are sent through this interim updated accounting record.

- When used with the **periodic** keyword, interim accounting records are sent periodically as defined by the argument number. The interim accounting record contains all of the accounting information recorded for that user up to the time the accounting record is sent.
- When using both the **newinfo** and **periodic** keywords, interim accounting records are sent to the accounting server every time there is new accounting information to report, and accounting records are sent to the accounting server periodically as defined by the argument number. For example, if you configure the **aaa accounting update newinfo periodic** *number* command, all users currently logged in will continue to generate periodic interim accounting records while new users will generate accounting records based on the **newinfo** algorithm.
- Vendor-specific attributes (VSAs) such as h323-connect-time and backward call indicator (BCI) are transmitted in the interim update RADIUS message when the **aaa accounting update newinfo** command and keyword are enabled.
- Jitter is used to provide an interval of time between records, so that the AAA server does not get overwhelmed by a constant stream of records. If certain applications require that periodic records be sent a exact intervals, you should disable jitter by setting it to 0.

Caution Using the **aaa accounting update periodic** command and keyword can cause heavy congestion when many users are logged into the network.

Examples

The following example sends PPP accounting records to a remote RADIUS server. When IPCP completes negotiation, this command sends an interim accounting record to the RADIUS server that includes the negotiated IP address for this user; it also sends periodic interim accounting records to the RADIUS server at 30-minute intervals.

```
aaa accounting network default start-stop group radius
aaa accounting update newinfo periodic 30
```

The following example sends periodic interim accounting records to the RADIUS server at 30-minute intervals and disables jitter:

```
aaa accounting update newinfo periodic 30 jitter maximum 0
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
gw-accounting aaa	Enables VoIP gateway accounting through the AAA system.

aaa attribute

To add calling line identification (CLID) and dialed number identification service (DNIS) attribute values to a user profile, use the **aaa attribute** command in AAA-user configuration mode. To remove this command from your configuration, use the **no** form of this command.

aaa attribute {**clid** | **dnis**} *attribute-value*

no aaa attribute {**clid** | **dnis**} *attribute-value*

Syntax Description

clid	Adds CLID attribute values to the user profile.
dnis	Adds DNIS attribute values to the user profile.
attribute-value	Specifies a name for CLID or DNIS attribute values.

Defaults

If this command is not enabled, you will have an empty user profile.

Command Modes

AAA-user configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use the **aaa attribute** command to add CLID or DNIS attribute values to a named user profile, which is created by using the **aaa user profile** command. The CLID or DNIS attribute values can be associated with the record that is going out with the user profile (via the **test aaa group** command), thereby providing the RADIUS server with access to CLID or DNIS information when the server receives a RADIUS record.

Examples

The following example shows how to add CLID and DNIS attribute values to the user profile “cat”:

```
aaa user profile cat
 aaa attribute clid clidval
 aaa attribute dnis dnisval
```

Related Commands

Command	Description
aaa user profile	Creates a AAA user profile.
test aaa group	Associates a DNIS or CLID user profile with the record that is sent to the RADIUS server.

aaa authentication arap

To enable an authentication, authorization, and accounting (AAA) authentication method for AppleTalk Remote Access (ARA), use the **aaa authentication arap** command in global configuration mode. To disable this authentication, use the **no** form of this command.

aaa authentication arap {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication arap {**default** | *list-name*} *method1* [*method2*...]

Syntax Description

default	Uses the listed methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string used to name the following list of authentication methods tried when a user logs in.
method1 [*method2*...]	At least one of the keywords described in Table 4.

Defaults

If the **default** list is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication arap default local
```

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server and local-case support were added as method keywords for this command.

Usage Guidelines

The list names and default that you set with the **aaa authentication arap** command are used with the **arap authentication** command. Note that ARAP guest logins are disabled by default when you enable AAA. To allow guest logins, you must use either the **guest** or **auth-guest** method listed in Table 4. You can only use one of these methods; they are mutually exclusive.

Create a list by entering the **aaa authentication arap** *list-name method* command, where *list-name* is any character string used to name this list (such as *MIS-access*). The *method* argument identifies the list of methods the authentication algorithm tries in the given sequence. See Table 4 for descriptions of method keywords.

To create a default list that is used if no list is specified in the **arap authentication** command, use the **default** keyword followed by the methods you want to be used in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Use the **more system:running-config** command to view currently configured lists of authentication methods.

Note In Table 4, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Table 4 aaa authentication arap Methods

Keyword	Description
guest	Allows guest logins. This method must be the first method listed, but it can be followed by other methods if it does not succeed.
auth-guest	Allows guest logins only if the user has already logged in to EXEC. This method must be the first method listed, but can be followed by other methods if it does not succeed.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Examples

The following example creates a list called *MIS-access*, which first tries TACACS+ authentication and then none:

```
aaa authentication arap MIS-access group tacacs+ none
```

The following example creates the same list, but sets it as the default list that is used for all ARA protocol authentications if no other list is specified:

```
aaa authentication arap default group tacacs+ none
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

aaa authentication attempts login

To set the maximum number of login attempts that will be permitted before a session is dropped, use the **aaa authentication attempts login** command in global configuration mode. To reset the number of attempts to the default, use the **no** form of this command.

aaa authentication attempts login *number-of-attempts*

no aaa authentication attempts login

Syntax Description

number-of-attempts	Number of login attempts. Range is from 1 to 25. Default is 3.

Defaults

3 attempts

Command Modes

Global configuration

Command History

Release	Modification
12.2 T	This command was introduced.

Usage Guidelines

The **aaa authentication attempts login** command configures the number of times a router will prompt for username and password before a session is dropped.

The **aaa authentication attempts login** command can be used only if the **aaa new-model** command is configured.

Examples

The following example configures a maximum of 5 attempts at authentication for login:

```
aaa authentication attempts login 5
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

aaa authentication banner

To configure a personalized banner that will be displayed at user login, use the **aaa authentication banner** command in global configuration mode. To remove the banner, use the **no** form of this command.

aaa authentication banner *dstringd*

no aaa authentication banner

Syntax Description

d	Any delimiting character at the beginning and end of the *string* that notifies the system that the *string* is to be displayed as the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.
string	Any group of characters, excluding the one used as the delimiter. The maximum number of characters that you can display is 2996.

Defaults

Not enabled

Command Modes

Global configuration

Command History

Release	Modification
11.3(4)T	This command was introduced.

Usage Guidelines

Use the **aaa authentication banner** command to create a personalized message that appears when a user logs in to the system. This message or banner will replace the default message for user login.

To create a login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

Examples

The following example shows the default login message if **aaa authentication banner** is not configured. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication login default group radius
```

This configuration produces the following standard output:

```
User Verification Access
Username:
Password:
```

The following example configures a login banner (in this case, the phrase "Unauthorized use is prohibited.") that will be displayed when a user logs in to the system. In this case, the asterisk (*) symbol is used as the delimiter. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication banner *Unauthorized use is prohibited.*
aaa authentication login default group radius
```

This configuration produces the following login banner:

```
Unauthorized use is prohibited.
Username:
```

Related Commands

Command	Description
aaa authentication fail-message	Configures a personalized banner that will be displayed when a user fails login.

aaa authentication dot1x

To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the **aaa authentication dot1x** command in global configuration mode. To disable authentication, use the **no** form of this command

aaa authentication dot1x *{***default** | **listname***} method1 [method2...]*

no aaa authentication dot1x *{***default** | **listname***} method1 [method2...]*

Syntax Description

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
listname	Character string used to name the list of authentication methods tried when a user logs in.
method1 [method2...]	At least one of these keywords: • **enable**—Uses the enable password for authentication. • **group radius**—Uses the list of all RADIUS servers for authentication. • **line**—Uses the line password for authentication. • **local**—Uses the local username database for authentication. • **local-case**—Uses the case-sensitive local username database for authentication. • **none**—Uses no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.

Defaults

No authentication is performed.

Command Types

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced for the Cisco Ethernet switch network module.
12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet Switch Module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.3(2)XA	This command was introduced on the following Cisco router platforms: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Router support was added for the following platforms: Cisco 1751, Cisco 2610XM – Cisco 2611XM, Cisco 2620XM – Cisco 2621XM, Cisco 2650XM – Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.

Usage Guidelines

The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence to validate the password provided by the client. The only method that is truly 802.1X-compliant is the group radius method, in which the client data is validated against a RADIUS authentication server. The remaining methods enable AAA to authenticate the client by using locally configured data. For example, the local and local-case methods use the username and password that are saved in the Cisco IOS configuration file. The enable and line methods use the enable and line passwords for authentication.

If you specify group radius, you must configure the RADIUS server by entering the radius-server host global configuration command. If you are not using a RADIUS server, you can use the local or local-case methods, which access the local username database to perform authentication. By specifying the enable or line methods, you can supply the clients with a password to provide access to the switch.

Use the show running-config privileged EXEC command to display the configured lists of authentication methods.

Examples

The following example shows how to enable AAA and how to create an authentication list for 802.1X. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is allowed access with no authentication:

```
Router(config)# aaa new model
Router(config)# aaa authentication dot1x default group radius none
```

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
identity profile default	Creates an identity profile and enters dot1x profile configuration mode.
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

aaa authentication enable default

To enable authentication, authorization, and accounting (AAA) authentication to determine if a user can access the privileged command level, use the **aaa authentication enable default** command in global configuration mode. To disable this authorization method, use the **no** form of this command.

aaa authentication enable default *method1* [*method2*...]

no aaa authentication enable default *method1* [*method2*...]

Syntax Description

method1 [*method2*...]	At least one of the keywords described in Table 5.

Defaults

If the **default** list is not set, only the enable password is checked. This has the same effect as the following command:

```
aaa authentication enable default enable
```

On the console, the enable password is used if it exists. If no password is set, the process will succeed anyway.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support was added as various method keywords for this command.

Usage Guidelines

Use the **aaa authentication enable default** command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in Table 5. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

All **aaa authentication enable default** requests sent by the router to a RADIUS server include the username "$enab15$." Requests sent to a TACACS+ server will include the username that is entered for login authentication.

If a default authentication routine is not set for a function, the default is **none** and no authentication is performed. Use the **more system:running-config** command to view currently configured lists of authentication methods.

Note In Table 5, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Table 5 aaa authentication enable default Methods

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication. **Note** The RADIUS method does not work on a per-username basis.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Examples

The following example creates an authentication list that first tries to contact a TACACS+ server. If no server can be found, AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication enable default group tacacs+ enable none
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict network access to a user.
aaa new-model	Enables the AAA access control model.
enable password	Sets a local password to control access to various privilege levels.

aaa authentication eou default enable group radius

To set authentication lists for Extensible Authentication Protocol over UDP (EAPoUDP), use the **aaa authentication eou default enable group radius** command in global configuration mode. To remove the authentication lists, use the **no** form of this command.

aaa authentication eou default enable group radius

no aaa authentication eou default enable group radius

Syntax Description

This command has no arguments or keywords.

Defaults

Authentication lists for EAPoUDP are not set.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example shows that authentication lists have been set for EAPoUDP:

```
Router (config)# aaa new-model
Router (config)# aaa authentication eou default enable group radius
```

Related Commands

Command	Description
eou	Provides information about EAPoUDP.
ip admission	Creates a Layer 3 network admission control rule to be applied to the interface.

aaa authentication fail-message

To configure a personalized banner that will be displayed when a user fails login, use the **aaa authentication fail-message** command in global configuration mode. To remove the failed login message, use the **no** form of this command.

aaa authentication fail-message *dstringd*

no aaa authentication fail-message

Syntax Description

d	The delimiting character at the beginning and end of the *string* that notifies the system that the *string* is to be displayed as the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.
string	Any group of characters, excluding the one used as the delimiter. The maximum number of characters that you can display is 2996.

Defaults

Not enabled

Command Modes

Global configuration

Command History

Release	Modification
11.3(4)T	This command was introduced.

Usage Guidelines

Use the **aaa authentication fail-message** command to create a personalized message that appears when a user fails login. This message will replace the default message for failed login.

To create a failed-login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

Examples

The following example shows the default login message and failed login message that is displayed if **aaa authentication banner** and **aaa authentication fail-message** are not configured. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication login default group radius
```

This configuration produces the following standard output:

```
User Verification Access
Username:
Password:
```

```
% Authentication failed.
```

The following example configures both a login banner (“Unauthorized use is prohibited.”) and a login-fail message (“Failed login. Try again.”). The login message will be displayed when a user logs in to the system. The failed-login message will display when a user tries to log in to the system and fails. (RADIUS is specified as the default login authentication method.) In this example, the asterisk (*) is used as the delimiting character.

```
aaa new-model
aaa authentication banner *Unauthorized use is prohibited.*
aaa authentication fail-message *Failed login. Try again.*
aaa authentication login default group radius
```

This configuration produces the following login and failed login banner:

```
Unauthorized use is prohibited.
Username:
Password:
Failed login. Try again.
```

Related Commands

Command	Description
aaa authentication banner	Configures a personalized banner that will be displayed at user login.

aaa authentication login

To set authentication, authorization, and accounting (AAA)authentication at login, use the **aaa authentication login** command in global configuration mode. To disable AAA authentication, use the **no** form of this command.

aaa authentication login {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication login {**default** | *list-name*} *method1* [*method2*...]

Syntax Description

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in.
method1 [*method2*...]	At least one of the keywords described in Table 6.

Defaults

If the **default** list is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication login default local
```

Note On the console, login will succeed without any authentication checks if **default** is not set.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server and local-case support were added as method keywords for this command.

Usage Guidelines

The default and optional list names that you create with the **aaa authentication login** command are used with the **login authentication** command.

Create a list by entering the **aaa authentication login** *list-name method* command for a particular protocol, where *list-name* is any character string used to name this list (such as *MIS-access*). The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence. Method keywords are described in Table 6.

To create a default list that is used if no list is assigned to a line, use the **login authentication** command with the default argument followed by the methods you want to use in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

Note In Table 6, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Table 6 aaa authentication login Methods

Keyword	Description
enable	Uses the enable password for authentication.
krb5	Uses Kerberos 5 for authentication.
krb5-telnet	Uses Kerberos 5 telnet authentication protocol when using Telnet to connect to the router.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Examples

The following example creates an AAA authentication list called *MIS-access*. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication login MIS-access group tacacs+ enable none
```

The following example creates the same list, but it sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication login default group tacacs+ enable none
```

The following example sets authentication at login to use the Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router:

```
aaa authentication login default krb5
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
login authentication	Enables AAA authentication for logins.

aaa authentication password-prompt

To change the text displayed when users are prompted for a password, use the **aaa authentication password-prompt** command in global configuration mode. To return to the default password prompt text, use the **no** form of this command.

aaa authentication password-prompt *text-string*

no aaa authentication password-prompt *text-string*

Syntax Description

text-string	String of text that will be displayed when the user is prompted to enter a password. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your password:”).

Defaults

There is no user-defined *text-string*, and the password prompt appears as “Password.”

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use the **aaa authentication password-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The **no** form of this command returns the password prompt to the default value:

```
Password:
```

The **aaa authentication password-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

The **aaa authentication password-prompt** command works when RADIUS is used as the login method. The password prompt that is defined in the command will be shown even when the RADIUS server is unreachable. The **aaa authentication password-prompt** command does not work with TACACS+. TACACS+ supplies the network access server (NAS) with the password prompt to display to the users. If the TACACS+ server is reachable, the NAS gets the password prompt from the server and uses that prompt instead of the one defined in the **aaa authentication password-prompt** command. If the TACACS+ server is not reachable, the password prompt that is defined in the **aaa authentication password-prompt** command may be used.

Examples

The following example changes the text for the password prompt:

```
aaa authentication password-prompt “Enter your password now:”
```

Related Commands

Command	Description
aaa authentication username-prompt	Changes the text displayed when users are prompted to enter a username.
aaa new-model	Enables the AAA access control model.
enable password	Sets a local password to control access to various privilege levels.

aaa authentication ppp

To specify one or more authentication, authorization, and accounting (AAA) authentication methods for use on serial interfaces that are running PPP, use the **aaa authentication ppp** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication ppp {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication ppp {**default** | *list-name*} *method1* [*method2*...]

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods tried when a user logs in.
method1 [*method2*...]	Identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in Table 7.

Defaults

If the **default** list is not set, only the local user database is checked. This has the same effect as that created by the following command:

```
aaa authentication ppp default local
```

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support and **local-case** were added as method keywords.

Usage Guidelines

The lists that you create with the **aaa authentication ppp** command are used with the **ppp authentication** command. These lists contain up to four authentication methods that are used when a user tries to log in to the serial interface.

Create a list by entering the **aaa authentication ppp** *list-name method* command, where *list-name* is any character string used to name this list (such as *MIS-access*). The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in Table 7.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authentication succeed even if all methods return an error.

If authentication is not specifically set for a function, the default is **none** and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

Note In Table 7, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Table 7 aaa authentication ppp Methods

Keyword	Description
if-needed	Does not authenticate if the user has already been authenticated on a tty line.
krb5	Uses Kerberos 5 for authentication (can be used only for Password Authentication Protocol [PAP] authentication).
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Examples

The following example creates a AAA authentication list called *MIS-access* for serial lines that use PPP. This authentication first tries to contact a TACACS+ server. If this action returns an error, the user is allowed access with no authentication.

```
aaa authentication ppp MIS-access group tacacs+ none
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs+	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
more system:running-config	Displays the contents of the currently running configuration file, the configuration for a specific interface, or map class information.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server host	Specifies a RADIUS server host.
tacacs+-server host	Specifies a TACACS host.

aaa authentication sgbp

To specify one or more authentication, authorization, and accounting (AAA) authentication methods for Stack Group Bidding Protocol (SGBP), use the **aaa authentication sgbp** command in global configuration mode. To disable SGBP authentication and return to the default, use the **no** form of this command.

aaa authentication sgbp {**default** | *list-name*} *method1* [*method2...*]

no aaa authentication sgbp {**default** | *list-name*} *method1* [*method2...*]

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods tried when a user logs in.
method1 [*method2...*]	Identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in

Defaults

The **aaa authentication ppp default** command. If the **aaa authentication ppp default** command is not enabled, local authentication will be the default functionality.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command introduced.

Usage Guidelines

The lists that you create with the **aaa authentication sgbp** command are used with the **sgbp aaa authentication** command.

Create a list by entering the **aaa authentication sgbp**p *list-name method* command, where the *list-name* argument is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in Table 8.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authentication succeed even if all methods return an error.

Use the **more system:running-config** command to display currently configured lists of authentication methods.

Table 8 aaa authentication sgbp Methods

Keyword	Description
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Examples

The following example shows how to create a AAA authentication list called SGBP. The user first tries to contact a RADIUS server for authentication. If this action returns an error, the user will try to access the local database.

```
Router(config)# aaa authentication sgbp SGBP group radius local
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
sgbp aaa authentication	Enables a SGBP authentication list.

aaa authentication username-prompt

To change the text displayed when users are prompted to enter a username, use the **aaa authentication username-prompt** command in global configuration mode. To return to the default username prompt text, use the **no** form of this command.

aaa authentication username-prompt *text-string*

no aaa authentication username-prompt *text-string*

Syntax Description

text-string	String of text that will be displayed when the user is prompted to enter a username. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your name:”).

Defaults

There is no user-defined *text-string*, and the username prompt appears as “Username.”

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use the **aaa authentication username-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a username. The **no** form of this command returns the username prompt to the default value:

```
Username:
```

Some protocols (for example, TACACS+) have the ability to override the use of local username prompt information. Using the **aaa authentication username-prompt** command will not change the username prompt text in these instances.

Note The **aaa authentication username-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

Examples

The following example changes the text for the username prompt:

```
aaa authentication username-prompt “Enter your name here:”
```

Related Commands

Command	Description
aaa authentication password-prompt	Changes the text that is displayed when users are prompted for a password.
aaa new-model	Enables the AAA access control model.
enable password	Sets a local password to control access to various privilege levels.

aaa authorization

To set parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To disable authorization for a function, use the **no** form of this command.

aaa authorization {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]

no aaa authorization {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **default** | *list-name*}

Syntax Description

network	Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA).
exec	Runs authorization to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as autocommand information.
commands	Runs authorization for all commands at the specified privilege level.
level	Specific command level that should be authorized. Valid entries are 0 through 15.
reverse-access	Runs authorization for reverse access connections, such as reverse Telnet.
configuration	Downloads the configuration from the authentication, authorization, and accounting (AAA) server.
default	Uses the listed authorization methods that follow this argument as the default list of methods for authorization.
list-name	Character string used to name the list of authorization methods.
method1 [*method2...*]	Specifies an authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in Table 9.

Defaults

Authorization is disabled for all actions (equivalent to the method keyword **none**).

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	Group server support was added as a method keyword for this command.

Usage Guidelines

Use the **aaa authorization** command to enable authorization and to create named methods lists, defining authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways authorization will be performed and the sequence in which these methods will be performed. A method list is a named list describing the authorization methods to be used (such as RADIUS or TACACS+), in sequence. Method lists enable you to designate one or more security

protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle—meaning that the security server or local username database responds by denying the user services—the authorization process stops and no other authorization methods are attempted.

If the **aaa authorization** command for a particular authorization type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place.

Use the **aaa authorization** command to create a list by entering values for the *list-name* and the *method* arguments, where *list-name* is any character string used to name this list (excluding all method names) and *method* identifies the list of authorization method(s) tried in the given sequence.

Note In Table 9, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Method keywords are described in Table 9.

Table 9 aaa authorization Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the **server group** *group-name* command.
if-authenticated	Allows the user to access the requested function if the user is authenticated.
krb5-instance	Uses the instance defined by the **kerberos instance map** command.
local	Uses the local database for authorization.
none	No authorization is performed.

Cisco IOS software supports the following six methods for authorization:

- **RADIUS**—The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.

- **TACACS+**—The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.
- **If-Authenticated**—The user is allowed to access the requested function provided the user has been authenticated successfully.
- **None**—The network access server does not request authorization information; authorization is not performed over this line or interface.
- **Local**—The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled via the local database.
- **Kerberos Instance Map**—The network access server uses the instance defined by the **kerberos instance map** command for authorization.

Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:

- **Network**—Applies to network connections. This can include a PPP, SLIP, or ARA connection.
- **EXEC**—Applies to the attributes associated with a user EXEC terminal session.
- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **Reverse Access**—Applies to reverse Telnet sessions.
- **Configuration**—Applies to the configuration downloaded from the AAA server.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, method lists must be applied to specific lines or interfaces before any of the defined methods will be performed.

The authorization command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and refuse authorization.

For a list of supported RADIUS attributes, refer to the appendix “RADIUS Attributes” in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ AV pairs, refer to the appendix “TACACS+ Attribute-Value Pairs” in the *Cisco IOS Security Configuration Guide*.

Note Five commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

Examples

The following example defines the network authorization method list named mygroup, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, local network authorization will be performed.

```
aaa authorization network mygroup group radius local
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs+	Groups different TACACS+ server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ host.

aaa authorization cache filterserver

To enable authentication, authorization, and accounting (AAA) authorization caches and the downloading of access control list (ACL) configurations from a RADIUS filter server, use the **aaa authorization cache filterserver** command in global configuration mode. To disable AAA authorization caches, use the **no** form of this command.

aaa authorization cache filterserver default *methodlist* [*methodlist2...*]

no aaa authorization cache filterserver default

Syntax Description

default	Default authorization list.
methodlist [*methodlist2...*]	One of the keywords listed in Table 10.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **aaa authorization cache filterserver** command to enable the RADIUS ACL filter server.

Method keywords are described in Table 10.

Table 10 Method Keywords

Keyword	Description
group *group-name*	Uses a subset of RADIUS servers for authentication as defined by the **aaa group server radius** command.
local	Uses the local database for authorization caches and ACL configuration downloading.
none	No authorization is performed.

This command functions similarly to the **aaa authorization** command with the following exceptions:

- Named method-lists cannot be configured.
- Only one instance of this command can be configured.
- TACACS+ groups cannot be configured.

Examples

The following example shows how to configure the default RADIUS server group as the desired filter. If the request is rejected or a reply is not returned, local configuration will be consulted. If the local filter does not respond, the call will be accepted but filtering will not occur.

```
aaa authorization cache filterserver group radius local none
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.

aaa authorization config-commands

To reestablish the default created when the **aaa authorization commands** command was issued, use the **aaa authorization config-commands** command in global configuration mode. To disable authentication, authorization, and accounting (AAA) configuration command authorization, use the **no** form of this command.

aaa authorization config-commands

no aaa authorization config-commands

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(6.02)T	This command was changed from being enabled by default to being disabled by default.

Usage Guidelines

If the **aaa authorization commands** *level method* command is enabled, all commands, including configuration commands, are authorized by authentication, authorization, and accounting (AAA) using the method specified. Because there are configuration commands that are identical to some EXEC-level commands, there can be some confusion in the authorization process. Using the **no aaa authorization config-commands** command stops the network access server from attempting configuration command authorization.

After the **no** form of this command has been entered, AAA authorization of configuration commands is completely disabled. Care should be taken before entering the **no** form of this command because it potentially reduces the amount of administrative control on configuration commands.

Use the **aaa authorization config-commands** command if, after using the **no** form of this command, you need to reestablish the default set by the **aaa authorization commands** *level method* command.

Note You will get the same result if you (1) do not configure this command, or (2) configure **no aaa authorization config-commands**.

The following example specifies that TACACS+ authorization is run for level 15 commands and that AAA authorization of configuration commands is disabled:

```
aaa new-model
aaa authorization command 15 group tacacs+ none
no aaa authorization config-commands
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

aaa authorization console

To apply authorization to a console, use the **aaa authorization console** command in global configuration mode. To disable the authorization, use the **no** form of this command.

aaa authorization console

no aaa authorization console

Syntax Description

This command has no arguments or keywords.

Defaults

Authentication, authorization, and accounting (AAA) authorization is disabled on the console.

Command Modes

Global configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

If the **aaa new-model** command has been configured to enable the AAA access control model, the **no aaa authorization console** command is the default, and the authorization that is configured on the console line will always succeed. If you do not want the default, you need to configure the **aaa authorization console** command.

Note This command by itself does not turn on authorization of the console line. It needs to be used in conjunction with the **authorization** command under console line configurations.

If you are trying to enable authorization and the **no aaa authorization console** command is configured by default, you will see the following message:

```
%Authorization without the global command aaa authorization console is useless.
```

Examples

The following example shows that the default authorization that is configured on the console line is being disabled:

```
Router (config)# aaa authorization console
```

Related Commands

Command	Description
authorization	Enables AAA authorization for a specific line or group of lines.

aaa authorization reverse-access

To configure a network access server to request authorization information from a security server before allowing a user to establish a reverse Telnet session, use the **aaa authorization reverse-access** command in global configuration mode. To restore the default value for this command, use the **no** form of this command.

aaa authorization reverse-access {**group radius** | **group tacacs+**}

no aaa authorization reverse-access {**group radius** | **group tacacs+**}

Syntax Description

group radius	Specifies that the network access server will request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session.
group tacacs+	Specifies that the network access server will request authorization from a TACACS+ security server before allowing a user to establish a reverse Telnet session.

Defaults

This command is disabled by default, meaning that authorization for reverse Telnet is not requested.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(5)T	Group server support was added as various method keywords for this command.

Usage Guidelines

Telnet is a standard terminal emulation protocol used for remote terminal connection. Normally, you log in to a network access server (typically through a dialup connection) and then use Telnet to access other network devices from that network access server. There are times, however, when it is necessary to establish a reverse Telnet session. In reverse Telnet sessions, the Telnet connection is established in the opposite direction—from inside a network to a network access server on the network periphery to gain access to modems or other devices connected to that network access server. Reverse Telnet is used to provide users with dialout capability by allowing them to open Telnet sessions to modem ports attached to a network access server.

It is important to control access to ports accessible through reverse Telnet. Failure to do so could, for example, allow unauthorized users free access to modems where they can trap and divert incoming calls or make outgoing calls to unauthorized destinations.

Authentication during reverse Telnet is performed through the standard AAA login procedure for Telnet. Typically the user has to provide a username and password to establish either a Telnet or reverse Telnet session. This command provides an additional (optional) level of security by requiring authorization in addition to authentication. When this command is enabled, reverse Telnet authorization can use RADIUS or TACACS+ to authorize whether or not this user is allowed reverse Telnet access to specific asynchronous ports, after the user successfully authenticates through the standard Telnet login procedure.

Examples

The following example causes the network access server to request authorization information from a TACACS+ security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization reverse-access default group tacacs+
!
tacacs-server host 172.31.255.0
tacacs-server timeout 90
tacacs-server key goaway
```

The lines in this sample TACACS+ reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group tacacs+** command specifies TACACS+ as the default method for user authentication during login.
- The **aaa authorization reverse-access default group tacacs+** command specifies TACACS+ as the method for user authorization when trying to establish a reverse Telnet session.
- The **tacacs-server host** command identifies the TACACS+ server.
- The **tacacs-server timeout** command sets the interval of time that the network access server waits for the TACACS+ server to reply.
- The **tacacs-server key** command defines the encryption key used for all TACACS+ communications between the network access server and the TACACS+ daemon.

The following example configures a generic TACACS+ server to grant a user, "jim," reverse Telnet access to port tty2 on the network access server named "site1" and to port tty5 on the network access server named site2:

```
user = jim
  login = cleartext lab
  service = raccess {
    port#1 = site1/tty2
    port#2 = site2/tty5
}
```

Note In this example, "site1" and "site2" are the configured host names of network access servers, not DNS names or alias.

The following example configures the TACACS+ server (CiscoSecure) to authorize a user named Jim for reverse Telnet:

```
user = jim
 profile_id = 90
 profile_cycle = 1
 member = Tacacs_Users
 service=shell {
 default cmd=permit
 }
 service=raccess {
 allow "c2511e0" "tty1" ".*"
 refuse ".*" ".*" ".*"
 password = clear "goaway"
```

Note CiscoSecure only supports reverse Telnet using the command line interface in versions 2.1(*x*) through version 2.2(1).

An empty “service=raccess {}” clause permits a user to have unconditional access to network access server ports for reverse Telnet. If no “service=raccess” clause exists, the user is denied access to any port for reverse Telnet.

For more information about configuring TACACS+, refer to the chapter “Configuring TACACS+” in the *Cisco IOS Security Configuration Guide*. For more information about configuring CiscoSecure, refer to the *CiscoSecure Access Control Server User Guide*, version 2.1(2) or later.

The following example causes the network access server to request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group radius
aaa authorization reverse-access default group radius
!
radius-server host 172.31.255.0
radius-server key goaway
```

The lines in this sample RADIUS reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group radius** command specifies RADIUS as the default method for user authentication during login.
- The **aaa authorization reverse-access default group radius** command specifies RADIUS as the method for user authorization when trying to establish a reverse Telnet session.
- The **radius-server host** command identifies the RADIUS server.
- The **radius-server key** command defines the encryption key used for all RADIUS communications between the network access server and the RADIUS daemon.

The following example configures the RADIUS server to grant a user named “jim” reverse Telnet access at port tty2 on network access server site1:

```
Password = “goaway”
User-Service-Type = Shell-User
cisco-avpair = “raccess:port#1=site1/tty2”
```

The syntax "raccess:port=any/any" permits a user to have unconditional access to network access server ports for reverse Telnet. If no "raccess:port={*nasname*}/{*tty number*}" clause exists in the user profile, the user is denied access to reverse Telnet on all ports.

For more information about configuring RADIUS, refer to the chapter “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*.

aaa authorization template

To enable usage of a local or remote customer template on the basis of Virtual Private Network (VPN) routing and forwarding (VRF), use the **aaa authorization template** command in global configuration mode. To disable the new authorization, use the **no** form of this command.

aaa authorization template

no aaa authorization template

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Examples

The following example enables usage of a remote customer template:

```
aaa authorization template
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ server host.
template	Accesses the template configuration mode for configuring a particular customer profile template.

aaa cache filter

To enable filter cache configuration, use the **aaa cache filter** command in global configuration mode. To disable this functionality, use the **no** form of this command.

aaa cache filter

no aaa cache filter

Syntax Description

This command has no arguments or keywords.

Defaults

Filter cache configuration is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **aaa cache filter** command to begin filter cache configuration and enter AAA filter configuration mode (config-aaa-filter).

After enabling this command, you can specify filter cache parameters with the following commands:

- **cache clear age**—Specifies, in minutes, when cache entries expire and the cache is cleared.
- **cache disable**—Disables the cache.
- **cache max**—Refreshes a cache entry when a new sessions begins.
- **cache refresh**—Limits the absolute number of entries the cache can maintain for a particular server.
- **password**—Specifies the optional password that is to be used for filter server authentication requests.

Note Each of these commands is optional; thus, the default value will be enabled for any command that is not specified.

Examples

The following example shows how to enable filter cache configuration and specify cache parameters.

```
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
```

Related Commands

Command	Description
aaa authorization cache filterserver	Enables AAA authorization caches and the downloading of ACL configurations from a RADIUS filter server.
cache clear age	Specifies when, in minutes, cache entries expire and the cache is cleared.
cache disable	Disables the cache.
cache max	Refreshes a cache entry when a new sessions begins.
cache refresh	Limits the absolute number of entries the cache can maintain for a particular server.
password	Specifies the optional password that is to be used for filter server authentication requests.

aaa configuration route

To configure the username and password that are to be used when downloading static routes via RADIUS, use the **aaa configuration route** command in global configuration mode. To disable this feature, use the **no** form of this command.

aaa configuration route username *username* [**password** [**0** | **7**] *password*]

no aaa configuration route username *username* [**password** [**0** | **7**] *password*]

Syntax Description

username *username*	Defines a username to be used instead of the router's hostname.
password *password*	(Optional) Defines an alphanumeric password to be used instead of "cisco."
0 | **7**	(Optional) Defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. • **0**—The text immediately following is not encrypted. **Note** Type 0 passwords are automatically converted to type 7 passwords by enabling the **service password-encryption** command. • **7**—The text is encrypted using a Cisco-defined encryption algorithm .

Defaults

The hostname of the router and the password "cisco" are used during the static route configuration download.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The **aaa configuration route** command allows you to specify a username other than the router's hostname and a stronger password than the default "cisco."

Examples

The following example shows how to specify the username "MyUsername" and the password "MyPass" when downloading a static route configuration:

```
aaa new-model
aaa group server radius rad1
    server 1.1.1.1
    exit
aaa authorization configuration default group radius
aaa authorization configuration foo group rad1
aaa route download 1 authorization foo
aaa configuration route username MyUsername password 0 MyPass
radius-server host 2.2.2.2
radius-server key 0 RadKey
```

Related Commands

Command	Description
aaa route download	Enables the static route download feature and sets the amount of time between downloads.

aaa dnis map accounting network

To map a Dialed Number Information Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group that will be used for AAA accounting, use the **aaa dnis map accounting network** command in global configuration mode. To remove DNIS mapping from the named server group, use the **no** form of this command.

aaa dnis map *dnis-number* **accounting network** [**start-stop** | **stop-only** | **none**] [**broadcast**] **group** *groupname*

no aaa dnis map *dnis-number* **accounting network**

Syntax Description

dnis-number	Number of the DNIS.
start-stop	(Optional) Indicates that the defined security server group will send a "start accounting" notice at the beginning of a process and a "stop accounting" notice at the end of a process. The "start accounting" record is sent in the background. (The requested user process begins regardless of whether the "start accounting" notice was received by the accounting server.)
stop-only	(Optional) Indicates that the defined security server group will send a "stop accounting" notice at the end of the requested user process.
none	(Optional) Indicates that the defined security server group will not send accounting notices.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
group *groupname*	At least one of the keywords described in Table 11.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(1)T	• The optional **broadcast** keyword was added. • The ability to specify multiple server groups was added. • To accommodate multiple server groups, the name of the command was changed from **aaa dnis map accounting network group** to **aaa dnis map accounting network**.

Usage Guidelines

This command lets you assign a DNIS number to a particular AAA server group so that the server group can process accounting requests for users dialing in to the network using that particular DNIS. To use this command, you must first enable AAA, define an AAA server group, and enable DNIS mapping.

Table 11 contains descriptions of accounting method keywords.

Table 11 AAA Accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius command.**
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name*.

In Table 11, the **group radius** and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Examples

The following example maps DNIS number 7777 to the RADIUS server group called group1. Server group group1 will use RADIUS server 172.30.0.0 for accounting requests for users dialing in with DNIS 7777.

```
aaa new-model
radius-server host 172.30.0.0 acct-port 1646 key cisco1
aaa group server radius group1
 server 172.30.0.0
aaa dnis map enable
aaa dnis map 7777 accounting network group group1
```

Related Commands

Command	Description
aaa dnis map authentication ppp group	Maps a DNIS number to a particular authentication server group.
aaa dnis map enable	Enables AAA server selection based on DNIS.
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

aaa dnis map authentication login group

To map a Dialed Number Information Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group for the login service (this server group will be used for AAA authentication), use the **aaa dnis map authentication login group** command in global configuration mode. To unmap this DNIS number from the defined server group, use the **no** form of this command.

aaa dnis map *dnis-number* **authentication login group** *server-group-name*

no aaa dnis map *dnis-number* **authentication login group** *server-group-name*

Syntax Description

dnis-number	Number of the DNIS.
server-group-name	Character string used to name a group of security servers associated in a server group.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

This command lets you assign a DNIS number to a particular AAA server group; thus, the server group can process the AAA authentication requests for login service for users dialing into the network using that particular DNIS.

To use this command, you must first enable AAA, define an AAA server group, and enable DNIS mapping.

Examples

The following example shows how to map DNIS number 7777 to the RADIUS server group called group1. group1 will use RADIUS server 172.30.0.0 for AAA authentication requests for login service for users dialing in with DNIS 7777.

```
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
aaa group server radius group1
 server 172.30.0.0
 exit
aaa dnis map enable
aaa dnis map 7777 authentication login group group1
```

Related Commands

Command	Description
aaa dnis map accounting network group	Maps a DNIS number to a particular accounting server group.
aaa dnis map enable	Enables AAA server selection based on DNIS.
aaa group server	Groups different server hosts into distinct lists and methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

aaa dnis map authentication ppp group

To map a Dialed Number Information Service (DNIS) number to a particular authentication server group (this server group will be used for authentication, authorization, and accounting (AAA) authentication), use the **aaa dnis map authentication ppp group** command in global configuration mode. To remove the DNIS number from the defined server group, use the **no** form of this command.

aaa dnis map *dnis-number* **authentication ppp group** *server-group-name*

no aaa dnis map *dnis-number* **authentication ppp group** *server-group-name*

Syntax Description

dnis-number	Number of the DNIS.
server-group-name	Character string used to name a group of security servers associated in a server group.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

This command lets you assign a DNIS number to a particular AAA server group, so that the server group can process authentication requests for users dialing in to the network using that particular DNIS. To use this command, you must first enable AAA, define an AAA server group, and enable DNIS mapping.

Examples

The following example maps DNIS number 7777 to the RADIUS server group called group1. Server group group1 will use RADIUS server 172.30.0.0 for authentication requests for users dialing in with DNIS 7777.

```
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
aaa group server radius group1
 server 172.30.0.0
aaa dnis map enable
aaa dnis map 7777 authentication ppp group group1
```

Related Commands

Command	Description
aaa dnis map accounting network group	Maps a DNIS number to a particular accounting server group.
aaa dnis map enable	Enables AAA server selection based on DNIS.
aaa group server	Groups different server hosts into distinct lists and distinct methods.

Command	Description
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

aaa dnis map authorization network group

To map a Dialed Number Identification Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group (the server group that will be used for AAA authorization), use the **aaa dnis map authorization network group** command in global configuration mode. To unmap this DNIS number from the defined server group, use the **no** form of this command.

aaa dnis map *dnis-number* **authorization network group** *server-group-name*

no aaa dnis map *dnis-number* **authorization network group** *server-group-name*

Syntax Description

dnis-number	Number of the DNIS.
server-group-name	Character string used to name a group of security servers functioning within a server group.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

This command lets you assign a DNIS number to a particular AAA server group so that the server group can process authorization requests for users dialing in to the network using that particular DNIS number. To use this command, you must first enable AAA, define a AAA server group, and enable DNIS mapping.

Examples

The following example maps DNIS number 7777 to the RADIUS server group called group1. Server group group1 will use RADIUS server 172.30.0.0 for authorization requests for users dialing in with DNIS 7777:

```
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
aaa group server radius group1
server 172.30.0.0
aaa dnis map enable
aaa dnis map 7777 authorization network group group1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
aaa dnis map accounting network group	Maps a DNIS number to a AAA server group used for accounting services.

Command	Description
aaa dnis map authentication ppp group	Maps a DNIS number to a AAA server used for authentication services.
aaa dnis map enable	Enables AAA server selection based on DNIS number.
aaa group server	Groups different server hosts into distinct lists and methods.
radius-server host	Specifies and defines the IP address of the RADIUS server host.

aaa group server radius

To group different RADIUS server hosts into distinct lists and distinct methods, enter the **aaa group server radius** command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

aaa group server radius *group-name*

no aaa group server radius *group-name*

Syntax Description

group-name	Character string used to name the group of servers.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A group server is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts and TACACS+ server hosts. A group server is used in conjunction with a global server host list. The group server lists the IP addresses of the selected server hosts.

Examples

The following example shows the configuration of an AAA group server named radgroup1 that comprises three member servers:

```
aaa group server radius radgroup1
 server 1.1.1.1 auth-port 1700 acct-port 1701
 server 2.2.2.2 auth-port 1702 acct-port 1703
 server 3.3.3.3 auth-port 1705 acct-port 1706
```

Note If auth-port and acct-port are not specified, the default value of auth-port is 1645 and the default value of acct-port is 1646.

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication login	Set AAA authentication at login.

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

aaa group server tacacs+

To group different TACACS+ server hosts into distinct lists and distinct methods, use the **aaa group server tacacs+** command in global configuration mode. To remove a server group from the configuration list, use the **no** form of this command.

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

Syntax Description

group-name	Character string used to name the group of servers.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A server group is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts and TACACS+ server hosts. A server group is used in conjunction with a global server host list. The server group lists the IP addresses of the selected server hosts.

Examples

The following example shows the configuration of an AAA group server named tacgroup1 that comprises three member servers:

```
aaa group server tacacs+ tacgroup1
    server 1.1.1.1
    server 2.2.2.2
    server 3.3.3.3
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security.
aaa authentication login	Enables AAA accounting of requested services for billing or security purposes.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
tacacs-server host	Specifies a TACACS+ host.

aaa nas port extended

To replace the NAS-Port attribute with RADIUS IETF attribute 26 and to display extended field information, use the **aaa nas port extended** command in global configuration mode. To display no extended field information, use the **no** form of this command.

aaa nas port extended

no aaa nas port extended

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation will not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI interface is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 will appear as NAS-Port = 20101 due to the 16-bit field size limitation associated with RADIUS IETF NAS-Port attribute.

In this case, the solution is to replace the NAS-Port attribute with a vendor-specific attribute (RADIUS IETF Attribute 26). Cisco's vendor ID is 9, and the Cisco-NAS-Port attribute is subtype 2. Vendor-specific attributes (VSAs) can be turned on by entering the **radius-server vsa send** command. The port information in this attribute is provided and configured using the **aaa nas port extended** command.

The standard NAS-Port attribute (RADIUS IETF attribute 5) will continue to be sent. If you do not want this information to be sent, you can suppress it by using the **no radius-server attribute nas-port** command. When this command is configured, the standard NAS-Port attribute will no longer be sent.

Examples

The following example specifies that RADIUS will display extended interface information:

```
radius-server vsa send
aaa nas port extended
```

Related Commands

Command	Description
radius-server extended-portnames	Displays expanded interface information in the NAS-Port attribute.
radius-server vsa send	Configures the network access server to recognize and use vendor-specific attributes.

aaa nas redirected-station

To include the original number in the information sent to the authentication server when the number dialed by a device is redirected to another number for authentication, use the **aaa nas redirected-station** command in global configuration mode. To leave the original number out of the information sent to the authentication server, use the **no** form of this command.

aaa nas redirected-station

no aaa nas redirected-station

Syntax Description

This command has no arguments or keywords.

Defaults

The original number is not included in the information sent to the authentication server.

Command Modes

Global configuration

Command History

Release	Modification
12.1 T	This command was introduced.

Usage Guidelines

If a customer is being authenticated by a RADIUS or TACACS+ server and the number dialed by the cable modem (or other device) is redirected to another number for authentication, the **aaa nas redirected-station** command will enable the original number to be included in the information sent to the authentication server.

This functionality allows the service provider to determine whether the customer dialed a number that requires special billing arrangements, such as a toll-free number.

The original number can be sent as a Cisco Vendor Specific Attribute (VSA) for TACACS+ servers and as RADIUS Attribute 93 (Ascend-Redirect-Number) for RADIUS servers. The RADIUS Attribute 93 is sent by default; to also send a VSA attribute for TACACS+ servers, use the **radius-server vsa send accounting** and **radius-server vsa send authentication** commands. To configure the RADIUS server to use RADIUS Attribute 93, add the non-standard option to the **radius-server host** command.

Note This feature is valid only when using port adapters that are configured for a T1 or E1 ISDN PRI or BRI interface. In addition, the telco switch performing the number redirection must be able to provide the redirected number in the Q.931 Digital Subscriber Signaling System Network Layer.

Examples

The following example enables the original number to be forwarded to the authentication server:

```
!
aaa authorization config-commands
aaa accounting exec default start-stop group radius
aaa accounting system default start-stop broadcast group apn23
aaa nas redirected-station
```

```
aaa session-id common
ip subnet-zero
!
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server vsa	Configures the network access server to recognize and use vendor-specific attributes.

aaa new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

aaa new-model

no aaa new-model

Syntax Description

This command has no arguments or keywords.

Defaults

AAA is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command enables the AAA access control system.

Examples

The following example initializes AAA:

```
aaa new-model
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication arap	Enables an AAA authentication method for ARAP using TACACS+.
aaa authentication enable default	Enables AAA authentication to determine if a user can access the privileged command level.
aaa authentication login	Sets AAA authentication at login.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

aaa pod server

To enable inbound user sessions to be disconnected when specific session attributes are presented, use the **aaa pod server** command in global configuration mode. To disable this feature, use the **no** form of this command.

aaa pod server [**port** *port number*] [**auth-type** {**any** | **all** | **session-key**}] **server-key** [*encryption-type*] *string*

no aaa pod server

Syntax Description

port *port number*	(Optional) Network access server User Datagram Protocol (UDP) port to use for packet of disconnect (POD) requests. Default value is 1700.
auth-type	(Optional) Type of authorization required for disconnecting sessions. If no authentication type is specified, **auth-type** is the default.
any	(Optional) Session that matches all of the attributes sent in the POD packet is disconnected. The POD packet may contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key).
all	(Optional) Only a session that matches all four key attributes is disconnected. The default is **all**.
session-key	(Optional) Session with a matching session-key attribute is disconnected. All other attributes are ignored.
server-key	Configures the shared-secret text string.
encryption-type	(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Currently defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using an encryption algorithm defined by Cisco.
string	Shared-secret text string that is shared between the network access server and the client workstation. This shared-secret string must be the same on both systems.

Defaults

The POD server function is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)XH	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(2)XB	The *encryption-type* argument was added, as well as support for the voice applications and the Cisco 3600 series, and Cisco AS5350, and Cisco AS5400 routers.

Release	Modification
12.2(2)XB1	Support for the Cisco AS5800 was added.
12.2(11)T	The *encryption-type* argument and support for the voice applications were added. **Note** Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 is not included in this release.

Usage Guidelines

To disconnect a session, the values in one or more of the key fields in the POD request must match the values for a session on one of the network access server ports. Which values must match depends on the **auth-type** attribute defined in the command. If no **auth-type** attribute is specified, all three values must match. If no match is found, all connections remain intact and an error response is returned. The key fields are as follows:

- An h323-conf-id vendor-specific attribute (VSA) with the same content as received from the gateway for this call.
- An h323-call-origin VSA with the same content as received from the gateway for the leg of interest.
- A 16-byte Message Digest 5 (MD5) hash value that is carried in the *authentication* field of the POD request.

Examples

The following example enables POD and sets the secret key to “xyz123”:

```
aaa pod server server-key xyz123
```

Related Commands

Command	Description
aaa accounting delay-start	Delays generation of the start accounting record until the user IP address is established.
aaa accounting	Enables accounting records.
debug aaa pod	Displays debug messages for POD packets.
radius-server host	Identifies a RADIUS host.

aaa preauth

To enter authentication, authorization, and accounting (AAA) preauthentication configuration mode, use the **aaa preauth** command in global configuration mode. To disable preauthentication, use the **no** form of this command.

aaa preauth

no aaa preauth

Syntax Description

This command has no arguments or keywords.

Defaults

Preauthentication is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

To enter AAA preauthentication configuration mode, use the **aaa preauth** command. To configure preauthentication, use a combination of the **aaa preauth** commands: **group**, **clid**, **ctype**, **dnis**, and **dnis bypass**. You must configure the **group** command. You must also configure one or more of the **clid**, **ctype**, **dnis**, or **dnis bypass** commands.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

You can use the **clid**, **ctype**, or **dnis** commands to define the list of the preauthentication elements. For each preauthentication element, you can also define options such as password (for all the elements, the default password is cisco). If you specify multiple elements, the preauthentication process will be performed on each element according to the order of the elements that you configure with the preauthentication commands. In this case, more than one RADIUS preauthentication profile is returned, but only the last preauthentication profile will be applied to the authentication and authorization later on, if applicable.

Examples

The following example enables dialed number identification service (DNIS) preauthentication using a RADIUS server and the password Ascend-DNIS:

```
aaa preauth
 dnis password Ascend-DNIS
```

Related Commands

Command	Description
dnis (authentication)	Enables AAA preauthentication using DNIS.

group (authentication)	Selects the security server to use for AAA preauthentication.
isdn guard-timer	Sets a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.

aaa processes

To allocate a specific number of background processes to be used to process authentication, authorization, and accounting (AAA) authentication and authorization requests for PPP, use the **aaa processes** command in global configuration mode. To restore the default value for this command, use the **no** form of this command.

aaa processes *number*

no aaa processes *number*

Syntax Description

number	Specifies the number of background processes allocated for AAA requests for PPP. Valid entries are 1 to 2147483647.

Defaults

The default for this command is one allocated background process.

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Usage Guidelines

Use the **aaa processes** command to allocate a specific number of background processes to simultaneously handle multiple AAA authentication and authorization requests for PPP. Previously, only one background process handled all AAA requests for PPP, so only one new user could be authenticated or authorized at a time. This command configures the number of processes used to handle AAA requests for PPP, increasing the number of users that can be simultaneously authenticated or authorized.

The argument *number* defines the number of background processes earmarked to process AAA authentication and authorization requests for PPP. This argument also defines the number of new users that can be simultaneously authenticated and can be increased or decreased at any time.

Examples

The following examples shows the **aaa processes** command within a standard AAA configuration. The authentication method list “dialins” specifies RADIUS as the method of authentication, then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP. Ten background processes have been allocated to handle AAA requests for PPP.

```
aaa new-model
aaa authentication ppp dialins group radius local
aaa processes 10
interface 5
encap ppp
ppp authentication pap dialins
```

Related Commands

Command	Description
show ppp queues	Monitors the number of requests processed by each AAA background process.

aaa session-id

To specify whether the same session ID will be used for each authentication, authorization, and accounting (AAA) accounting service type within a call or whether a different session ID will be assigned to each accounting service type, use the **aaa session-id** command in global configuration mode. To restore the default behavior after the **unique** keyword is enabled, use the **no** form of this command.

aaa session-id [**common** | **unique**]

no aaa session-id [**unique**]

Syntax Description

common	(Optional) Ensures that all session identification (ID) information that is sent out for a given call will be made identical. The default behavior is **common**.
unique	(Optional) Ensures that only the corresponding service access-requests and accounting-requests will maintain a common session ID. Accounting-requests for each service will have a different session ID.

Defaults

The **common** keyword is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

The **common** keyword behavior allows the first session ID request of the call to be stored in a common database; all proceeding session ID requests will retrieve the value of the first session ID. Because a common session ID is the default behavior, this functionality is written to the system configuration after the **aaa new-model** command is configured.

Note The router configuration will always have either the **aaa session-id common** or the **aaa session-id unique** command enabled; it is not possible to have neither of the two enabled. Thus, the **no aaa session-id unique** command will revert to the default functionality, but the **no aaa session-id common** command will not have any effect because it is the default functionality.

The **unique** keyword behavior assigns a different session ID for each accounting type (Auth-Proxy, Exec, Network, Command, System, Connection, and Resource) during a call. To specify this behavior, the unique keyword *must* be specified. The session ID may be included in RADIUS access requests by configuring the **radius-server attribute 44 include-in-access-req** command. The session ID in the access-request will be the same as the session ID in the accounting request for the same service; all other services will provide unique session IDs for the same call.

Examples

The following example shows how to configure unique session IDs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
aaa session-id unique
```

Related Commands

Command	Description
aaa new model	Enables AAA.
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication).

aaa session-mib

To enable disconnect by using Simple Network Management Protocol (SNMP), use the **aaa session-mib** command in global configuration mode. To disable this function, use the **no** form of this command.

aaa session-mib disconnect

no aaa session-mib disconnect

Syntax Description

disconnect	Enables authentication, authorization, and accounting (AAA) session MIB disconnect.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Use the **aaa session-mib** command to terminate authenticated client connections using SNMP.

You must enable the **disconnect** keyword with this command. Otherwise, the network management station cannot perform set operations and disconnect users; it can only poll the table.

Examples

The following example shows how to enable a AAA session MIB to disconnect authenticated clients using SNMP:

```
aaa session-mib disconnect
```

aaa user profile

To create an authentication, authorization, and accounting (AAA) named user profile, use the **aaa user profile** command in global configuration mode. To remove a user profile from the configuration, use the **no** form of this command.

aaa user profile *profile-name*

no aaa user profile *profile-name*

Syntax Description

profile-name	Character string used to name the user profile.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use the **aaa user profile** command to create a AAA user profile. Used in conjunction with the **aaa attribute** command, which adds calling line identification (CLID) and dialed number identification service (DNIS) attribute values, the user profile can be associated with the record that is sent to the RADIUS server (via the **test aaa group** command), which provides the RADIUS server with access to CLID or DNIS attribute information when the server receives a RADIUS record.

Examples

The following example shows how to configure a dnis = dnisvalue user profile named “prfl1”:

```
aaa user profile prfl1
 aaa attribute dnis
 aaa attribute dnis dnisvalue
 no aaa attribute clid
! Attribute not found.
 aaa attribute clid clidvalue
 no aaa attribute clid
```

Related Commands

Command	Description
aaa attribute	Adds DNIS or CLID attribute values to a user profile.
test aaa group	Associates a DNIS or CLID user profile with the record that is sent to the RADIUS server.

access-enable

To enable the router to create a temporary access list entry in a dynamic access list, use the **access-enable** command in EXEC mode.

access-enable [**host**] [**timeout** *minutes*]

Syntax Description

host	(Optional) Tells the software to enable access only for the host from which the Telnet session originated. If not specified, the software allows all hosts on the defined network to gain access. The dynamic access list contains the network mask to use for enabling the new network.
timeout *minutes*	(Optional) Specifies an idle timeout for the temporary access list entry. If the access list entry is not accessed within this period, it is automatically deleted and requires the user to authenticate again. The default is for the entries to remain permanently. We recommend that this value equal the idle timeout set for the WAN connection.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command enables the lock-and-key access feature.

You should always define either an idle timeout (with the **timeout** keyword in this command) or an absolute timeout (with the **timeout** keyword in the **access-list** command). Otherwise, the temporary access list entry will remain, even after the user terminates the session.

Use the **autocommand** command with the **access-enable** command to cause the **access-enable** command to execute when a user opens a Telnet session into the router.

Examples

The following example causes the software to create a temporary access list entry and tells the software to enable access only for the host from which the Telnet session originated. If the access list entry is not accessed within 2 minutes, it is deleted.

```
autocommand access-enable host timeout 2
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
autocommand	Configures the Cisco IOS software to automatically execute a command when a user connects to a particular line.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

access-group (identity policy)

To specify an access group to be applied to an identity policy, use the **access-group** command in identity policy configuration mode. To remove the access group, use the **no** form of this command.

access-group *group-name*

no access-group *group-name*

Syntax Description

group-name	Access list name.

Defaults

An access group is not specified.

Command Modes

Identity policy configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Using this command, you can access only named access lists.

Examples

The following example shows that access group “exempt-acl” is to be applied to the identity policy “bluemoon”:

```
Router (config)# identity policy bluemoon
Router (config-identity-policy)# access-group exempt-acl
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

access-list dynamic-extend

To allow the absolute timer of the dynamic access control list (ACL) to be extended an additional six minutes, use the **access-list dynamic-extend** command in global configuration mode. To disable this functionality, use the **no** form of this command.

access-list dynamic-extend

no access-list dynamic-extend

Syntax Description

This command has no arguments or keywords.

Defaults

6 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

When you try to create a Telnet session to the router to re-authenticate yourself by using the lock-and-key function, use the **access-list dynamic-extend** command to extend the absolute timer of the dynamic ACL by six minutes.

The router must already be configured with the lock-and-key feature, and you must configure the extension *before* the ACL expires.

Examples

The following example shows how to extend the absolute timer of the dynamic ACL:

```
! The router is configured with the lock-and-key feature as follows
access-list 132 dynamic tactik timeout 6 permit ip any any
! The absolute timer will extended another six minutes.
access-list dynamic-extend
```

access-profile

To apply your per-user authorization attributes to an interface during a PPP session, use the **access-profile** command in privileged EXEC mode.

access-profile [**merge** | **replace**] [**ignore-sanity-checks**]

Syntax Description

merge	(Optional) Like the default form of the command, this option removes existing access control lists (ACLs) while retaining other existing authorization attributes for the interface. However, using this option also installs per-user authorization attributes in addition to the existing attributes. (The default form of the command installs only new ACLs.) The per-user authorization attributes come from all attribute-value pairs defined in the authentication, authorization, and accounting (AAA) per-user configuration (the user's authorization profile). The resulting authorization attributes of the interface are a combination of the previous and new configurations.
replace	(Optional) This option removes existing ACLs *and* all other existing authorization attributes for the interface. A complete new authorization configuration is then installed, using all AV pairs defined in the AAA per-user configuration. This option is not normally recommended because it initially deletes *all* existing configurations, including static routes. This could be detrimental if the new user profile does not reinstall appropriate static routes and other critical information.
ignore-sanity-checks	(Optional) Enables you to use any AV pairs, whether or not they are valid.

Defaults

Use the default form of the command (no keywords) to cause existing ACLs to be removed and ACLs defined in your per-user configuration to be installed.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

Remote users can use this command to activate double authentication for a PPP session. Double authentication must be correctly configured for this command to have the desired effect.

You should use this command when remote users establish a PPP link to gain local network access.

After you have been authenticated with CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol), you will have limited authorization. To activate double authentication and gain your appropriate user network authorization, you must open a Telnet session to the network access server and execute the **access-profile** command. (This command could also be set up as an autocommand, which would eliminate the need to enter the command manually.)

This command causes all subsequent network authorizations to be made in *your* username instead of in the remote *host's* username.

Any changes to the interface caused by this command will stay in effect for as long as the interface stays up. These changes will be removed when the interface goes down. This command does not affect the normal operation of the router or the interface.

The default form of the command, **access-profile**, causes existing ACLs to be unconfigured (removed), and new ACLs to be installed. The new ACLs come from your per-user configuration on an AAA server (such as a TACACS+ server). The ACL replacement constitutes a reauthorization of your network privileges.

The default form of the command can fail if your per-user configuration contains statements other than ACL AV pairs. Any protocols with non-ACL statements will be deconfigured, and no traffic for that protocol can pass over the PPP link.

The **access-profile merge** form of the command causes existing ACLs to be unconfigured (removed) and new authorization information (including new ACLs) to be added to the interface. This new authorization information consists of your complete per-user configuration on an AAA server. If any of the new authorization statements conflict with existing statements, the new statements could "override" the old statements or be ignored, depending on the statement and applicable parser rules. The resulting interface configuration is a combination of the original configuration and the newly installed per-user configuration.

Caution The new user authorization profile (per-user configuration) must *not* contain any invalid mandatory AV pairs, otherwise the command will fail and the PPP protocol (containing the invalid pair) will be dropped. If invalid AV pairs are included as *optional* in the user profile, the command will succeed, but the invalid AV pair will be ignored. Invalid AV pair types are listed later in this section.

The **access-profile replace** form of the command causes the entire existing authorization configuration to be removed from the interface, and the complete per-user authorization configuration to be added. This per-user authorization consists of your complete per-user configuration on an AAA server.

Caution Use extreme caution when using the **access-profile replace** form of the command. It might have detrimental and unexpected results, because this option deletes *all* authorization configuration information (including static routes) before reinstalling the new authorization configuration.

Invalid AV Pair Types

- addr
- addr-pool
- zonelist
- tunnel-id
- ip-addresses
- x25-addresses
- frame-relay

- source-ip

Note These AV pair types are "invalid" only when used with double authentication, in the user-specific authorization profile; they cause the **access-profile** command to fail. However, these AV pair types can be appropriate when used in other contexts.

Examples

The following example activates double authentication for a remote user. This example assumes that the **access-profile** command was *not* configured as an autocommand.

The remote user connects to the corporate headquarters network as shown in Figure 1.

Figure 1 Network Topology for Activating Double Authentication (Example)

The remote user runs a terminal emulation application to Telnet to the corporate network access server, a Cisco AS5200 universal access server local host named "hqnas." The remote user, named Bob, has the username "BobUser."

The following example replaces ACLs on the local host PPP interface. The ACLs previously applied to the interface during PPP authorization are replaced with ACLs defined in the per-user configuration AV pairs.

The remote user establishes a Telnet session to the local host and logs in:

```
login: BobUser
Password: <welcome>
hqnas> access-profile
```

Bob is reauthenticated when he logs in to hqnas, because hqnas is configured for login AAA authentication using the corporate RADIUS server. When Bob enters the **access-profile** command, he is reauthorized with his per-user configuration privileges. This causes the access lists and filters in his per-user configuration to be applied to the network access server interface.

After the reauthorization is complete, Bob is automatically logged out of the Cisco AS5200 local host.

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
telnet	Logs in to a host that supports Telnet.

access-restrict

To tie a particular Virtual Private Network (VPN) to a specific interface for access to the Cisco IOS gateway and the services it protects, use the **access-restrict** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove the VPN, use the **no** form of this command.

access-restrict {*interface-name***}**

no access-restrict {*interface-name***}**

Syntax Description

interface-name	Interface to which the VPN should be tied.

Defaults

The VPN is not tied to a specific interface.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The Access-Restrict attribute ties a particular VPN group to a specific interface for access to the Cisco IOS gateway and the services it provides.

It may be a requirement that particular customers or groups connect to the VPN gateway via a specific interface that uses a particular policy (as applied by the crypto map on that interface). If this specific interface is required, using the **access-restrict** command will result in validation that a VPN connection is connecting only via that interface (and hence, crypto map) to which it is allowed. If a violation is detected, the connection is terminated.

Multiple restricted interfaces may be defined per group. The Access-Restrict attribute is configured on a Cisco IOS router or in the RADIUS profile. This attribute has local (gateway) significance only and is not passed to the client.

You must enable the **crypto isakmp client configuration group command, which specifies group policy information that has to be defined or changed, before enabling the access-restrict command.**

Note

- The Access-Restrict attribute can be applied only by a RADIUS user.
- The attribute can be applied on a per-user basis after the user has been authenticated.
- The attribute can override any similar group attributes.
- User-based attributes are available only if RADIUS is used as the database.The attribute can override any similar group attributes.

- The Access-Restrict attribute is not required if ISAKMP profiles are implemented. ISAKMP profiles with specific policies per VPN group (as defined via the **match identity group** command, which is a subcommand of the **crypto isakmp profile** command), will achieve the same result.

An example of an attribute-value (AV) pair for the Access-Restrict attribute is as follows:

```
ipsec:access-restrict=<interface-name>
```

Examples

The following example shows that the VPN is tied to "ethernet 0":

```
crypto isakmp client configuration group cisco
 access-restrict ethernet 0
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

access-template

To manually place a temporary access list entry on a router to which you are connected, use the **access-template** EXEC command.

access-template [*access-list-number* | *name*] [*dynamic-name*] [*source*] [*destination*] [**timeout** *minutes*]

Syntax Description

access-list-number	(Optional) Number of the dynamic access list.
name	(Optional) Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.
dynamic-name	(Optional) Name of a dynamic access list.
source	(Optional) Source address in a dynamic access list. The keywords host and any are allowed. All other attributes are inherited from the original access-list entry.
destination	(Optional) Destination address in a dynamic access list. The keywords host and any are allowed. All other attributes are inherited from the original access-list entry.
timeout *minutes*	(Optional) Specifies a maximum time limit for each entry within this dynamic list. This is an absolute time, from creation, that an entry can reside in the list. The default is an infinite time limit and allows an entry to remain permanently.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command provides a way to enable the lock-and-key access feature.

You should always define either an idle timeout (with the **timeout** keyword in this command) or an absolute timeout (with the **timeout** keyword in the **access-list** command). Otherwise, the dynamic access list will remain, even after the user has terminated the session.

Examples

The following example enables IP access on incoming packets in which the source address is 172.29.1.129 and the destination address is 192.168.52.12. All other source and destination pairs are discarded.

```
access-template 101 payroll host 172.29.1.129 host 192.168.52.12 timeout 2
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
autocommand	Configures the Cisco IOS software to automatically execute a command when a user connects to a particular line.
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

accounting (gatekeeper)

To enable accounting services on the gatekeeper, use the **accounting** command in gatekeeper configuration mode. To disable accounting services, use the **no** form of this command.

accounting [**vsa**]

no accounting [**vsa**]

Syntax Description

vsa	(Optional) Configures the vendor-specific attribute (VSA) method of accounting.

Defaults

Accounting is disabled.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)XM	The **vsa** keyword was added.
12.2(2)T	The **vsa** keyword was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850 universal gateway.

Usage Guidelines

Specify a RADIUS server before using the **accounting** command.

There are three different methods of accounting. The H.323 method sends the call detail record (CDR) to the RADIUS server, the syslog method uses the system logging facility to record the CDRs, and the VSA method collects VSAs.

Examples

The following example enables the gateway to report user activity to the RADIUS server in the form of connection accounting records:

```
aaa accounting connection start-stop group radius
gatekeeper
 accounting
```

The following example shows how to enable VSA accounting:

```
aaa accounting connection start-stop group radius
gatekeeper
 accounting exec vsa
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

accounting (line)

To enable authentication, authorization, and accounting (AAA) accounting services to a specific line or group of lines, use the **accounting** command in line configuration mode. To disable AAA accounting services, use the **no** form of this command.

accounting {**arap** | **commands** *level* | **connection** | **exec**} [**default** | *list-name*]

no accounting {**arap** | **commands** *level* | **connection** | **exec**} [**default** | *list-name*]

Syntax Description

arap	Enables accounting on lines configured for AppleTalk Remote Access Protocol (ARAP).
commands *level*	Enables accounting on the selected lines for all commands at the specified privilege level. Valid privilege level entries are 0 through 15.
connection	Enables both CHAP and PAP, and performs PAP authentication before CHAP.
exec	Enables accounting for all system-level events not associated with users, such as reloads on the selected lines.
default	(Optional) The name of the default method list, created with the **aaa accounting** command.
list-name	(Optional) Specifies the name of a list of accounting methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa accounting** command.

Defaults

Accounting is disabled.

Command Modes

Line configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list) for a particular type of accounting, you must apply the defined lists to the appropriate lines for accounting services to take place. Use the **accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

Examples

The following example enables command accounting services (for level 15) using the accounting method list named charlie on line 10:

```
line 10
 accounting commands 15 charlie
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

accounting (server-group)

To specify an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request, use the **accounting** command in server-group configuration mode.

accounting [**accept** | **reject**] *list-name*

Syntax Description

accept	(Optional) All attributes will be rejected except for required attributes and the attributes specified in the *listname*.
reject	(Optional) All attributes will be accepted except for the attributes specified in the *listname*.
list-name	Given name for the accept or reject list.

Defaults

If specific attributes are not accepted or rejected, all attributes will be accepted.

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401ASR.

Usage Guidelines

An accept or reject list (also known as a filter) for RADIUS accounting allows users to send only the accounting attributes their business requires, thereby reducing unnecessary traffic and allowing users to customize their own accounting data.

Only one filter may be used for RADIUS accounting per server group.

Note The listname must be the same as the listname defined in the **radius-server attribute list** command, which is used with the **attribute** (server-group configuration) command to add to an accept or reject list.

Examples

The following example shows how to specify accept list "usage-only" for RADIUS accounting:

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
 server 1.1.1.1
 accounting accept usage-only
!
radius-server host 1.1.1.1 key mykey1
```

```
radius-server attribute list usage-only
 attribute 1,40,42-43,46
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to the user.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server attribute list	Defines an accept or reject list name.

accounting acknowledge broadcast

To define a designated broadcast accounting server group, use the **accounting acknowledge broadcast** command in server group RADIUS configuration mode. To disable the broadcast functionality, use the **no** form of this command.

accounting acknowledge broadcast

no accounting acknowledge broadcast

Syntax Description

This command has no arguments or keywords.

Defaults

Accounting broadcast functionality is disabled for the RADIUS server group.

Command Modes

Server group RADIUS configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example enables accounting broadcast functionality on RADIUS server group abcgroup:

```
Router(config)# aaa group server radius abcgroup
Router(config-sg-radius)# accounting acknowledge broadcast
```

Related Commands

Command	Description
aaa accounting update	Enables periodic interim accounting records to be sent to the accounting server.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
gw-accounting aaa	Enables VoIP gateway accounting through the AAA system.

acl (ISAKMP)

To configure split tunneling, use the **acl** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration and restore the default value, use the **no** form of this command.

acl *number*

no acl *number*

Syntax Description

number	Specifies a group of access control lists (ACLs) that represent protected subnets for split tunneling purposes.

Defaults

Split tunneling is not enabled; all data is sent via the Virtual Private Network (VPN) tunnel.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **acl** command to specify which groups of ACLs represent protected subnets for split tunneling. Split tunneling is the ability to have a secure tunnel to the central site and simultaneous clear text tunnels to the Internet.

You must enable the **crypto isakmp client configuration group command, which specifies group policy information that has to be defined or changed, before enabling the acl command.**

Examples

The following example shows how to correctly apply split tunneling for the group name “cisco.” In this example, all traffic sourced from the client and destined to the subnet 192.168.1.0 will be sent via the VPN tunnel.

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
!
access-list 199 permit ip 192.168.1.0 0.0.0.255 any
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies the policy profile of the group that will be defined.

address

To specify the IP address of the Rivest, Shamir, and Adelman (RSA) public key of the remote peer that you will manually configure in the keyring, use the **address** command in rsa-pubkey configuration mode. To remove the IP address, use the **no** form of this command.

address *ip-address*

no address *ip-address*

Syntax Description

ip-address	IP address of the remote peer.

Defaults

No default behavior or values

Command Modes

Rsa-pubkey configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Before you can use this command, you must enter the **rsa-pubkey** command in the crypto keyring mode.

Examples

The following example specifies the RSA public key of an IP Security (IPSec) peer:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
crypto keyring	Defines a crypto keyring to be used during IKE authentication.
key-string	Specifies the RSA public key of a remote peer.
rsa-pubkey	Defines the RSA manual key to be used for encryption or signatures during IKE authentication.

addressed-key

To specify which peer's RSA public key you will manually configure, use the **addressed-key** command in public key chain configuration mode.

addressed-key *key-address* [**encryption** | **signature**]

Syntax Description

key-address	Specifies the IP address of the remote peer's RSA keys.
encryption	(Optional) Indicates that the RSA public key to be specified will be an encryption special usage key.
signature	(Optional) Indicates that the RSA public key to be specified will be a signature special usage key.

Defaults

If neither the **encryption** nor **signature** keywords are used, general purpose keys will be specified.

Command Modes

Public key chain configuration. This command invokes public key configuration mode.

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command or the **named-key** command to specify which IP Security peer's RSA public key you will manually configure next.

Follow this command with the **key string** command to specify the key.

If the IPSec remote peer generated general-purpose RSA keys, do not use the **encryption** or **signature** keywords.

If the IPSec remote peer generated special-usage keys, you must manually specify both keys: use this command and the **key-string** command twice and use the **encryption** and **signature** keywords respectively.

Examples

The following example manually specifies the RSA public keys of two IPSec peers. The peer at 10.5.5.1 uses general-purpose keys, and the other peer uses special-usage keys.

```
Router(config)# crypto key pubkey-chain rsa
Router(config-pubkey-chain)# named-key otherpeer.example.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 005C300D 06092A86 4886F70D 01010105
Router(config-pubkey)# 00034B00 30480241 00C5E23B 55D6AB22
Router(config-pubkey)# 04AEF1BA A54028A6 9ACC01C5 129D99E4
Router(config-pubkey)# 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
Router(config-pubkey)# BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
Router(config-pubkey)# D58AD221 B583D7A4 71020301 0001
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
```

```
Router(config-pubkey-chain)# addressed-key 10.1.1.2 encryption
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# addressed-key 10.1.1.2 signature
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 0738BC7A 2BC3E9F0 679B00FE 53987BCC
Router(config-pubkey)# 01030201 42DD06AF E228D24C 458AD228
Router(config-pubkey)# 58BB5DDD F4836401 2A2D7163 219F882E
Router(config-pubkey)# 64CE69D4 B583748A 241BED0F 6E7F2F16
Router(config-pubkey)# 0DE0986E DF02031F 4B0B0912 F68200C4
Router(config-pubkey)# C625C389 0BFF3321 A2598935 C1B1
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# exit
Router(config)#
```

Related Commands

Command	Description
crypto key pubkey-chain rsa	Enters public key configuration mode (to allow you to manually specify the RSA public keys of other devices).
key-string (IKE)	Specifies the RSA public key of a remote peer.
named-key	Specifies which peer RSA public key you will manually configure.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

arap authentication

To enable authentication, authorization, and accounting (AAA) authentication for AppleTalk Remote Access Protocol (ARAP) on a line, use the **arap authentication** command in line configuration mode. To disable authentication for an ARAP line, use the **no** form of this command.

arap authentication {**default** | *list-name*} [**one-time**]

no arap authentication {**default** | *list-name*}

Caution If you use a *list-name* value that was not configured with the **aaa authentication arap** command, ARAP will be disabled on this line.

Syntax Description

default	Default list created with the **aaa authentication arap** command.
list-name	Indicated list created with the **aaa authentication arap** command.
one-time	(Optional) Accepts the username and password in the username field.

Defaults

ARAP authentication uses the default set with **aaa authentication arap** command. If no default is set, the local user database is checked.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.
11.0	The **one-time** keyword was added.

Usage Guidelines

This command is a per-line command that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line). You create defaults and lists with the **aaa authentication arap** command. Entering the **no** version of **arap authentication** has the same effect as entering the command with the **default** keyword. Before issuing this command, create a list of authentication processes by using the **aaa authentication arap** global configuration command.

Examples

The following example specifies that the TACACS+ authentication list called *MIS-access* is used on ARAP line 7:

```
line 7
 arap authentication MIS-access
```

Related Commands

Command	Description
aaa authentication arap	Enables an AAA authentication method for ARAP using TACACS+.

attribute (server-group)

To add attributes to an accept or reject list, use the **attribute** command in server-group configuration mode. To remove attributes from the list, use the **no** form of this command.

attribute *value1* [*value2* [*value3*]...]

no attribute *value1* [*value2* [*value3*]...]

Syntax Description

value1 [*value2* [*value3*]...]	Attributes to include in an accept or reject list. The value can be a single integer, such as 7, or a range of numbers, such as 56–59. At least one attribute value must be specified.

Defaults

If this command is not enabled, all attributes are sent to the network access server (NAS).

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401 ASR.

Usage Guidelines

Used in conjunction with the **radius-server attribute list** command (which defines the list name), the **attribute** command can be used to add attributes to an accept or reject list (also known as a filter). Filters are used to prevent the network access server (NAS) from receiving and processing unwanted attributes for authorization or accounting.

The **attribute** command can be used multiple times to add attributes to a filter. However, if a required attribute is specified in a reject list, the NAS will override the command and accept the attribute. Required attributes are as follows:

- For authorization:
  - 6 (Service-Type)
  - 7 (Framed-Protocol)
- For accounting:
  - 4 (NAS-IP-Address)
  - 40 (Acct-Status-Type)
  - 41 (Acct-Delay-Time)
  - 44 (Acct-Session-ID)

Note The user will not receive an error at the point of configuring a reject list for required attributes because the list does not specify a purpose—authorization or accounting. The server will determine whether an attribute is required when it is known what the attribute is to be used for.

Examples

The following example shows how to add attributes 12, 217, 6–10, 13, 64–69, and 218 to the list name "standard":

```
radius-server attribute list standard
    attribute 12,217,6-10,13
    attribute 64-69,218
```

Related Commands

Command	Description
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server attribute list	Defines an accept or reject list name.

authentication (IKE policy)

To specify the authentication method within an Internet Key Exchange (IKE) policy, use the **authentication** command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the authentication method to the default value, use the **no** form of this command.

authentication {**rsa-sig** | **rsa-encr** | **pre-share**}

no authentication

Syntax Description

rsa-sig	Specifies RSA signatures as the authentication method.
rsa-encr	Specifies RSA encrypted nonces as the authentication method.
pre-share	Specifies preshared keys as the authentication method.

Defaults

RSA signatures

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command to specify the authentication method to be used in an IKE policy.

If you specify RSA signatures, you must configure your peer routers to obtain certificates from a certification authority (CA).

If you specify RSA encrypted nonces, you must ensure that each peer has the other peer's RSA public keys. (See the **crypto key pubkey-chain rsa**, **addressed-key**, **named-key**, **address**, and commands.)

If you specify preshared keys, you must also separately configure these preshared keys. (See the **crypto isakmp identity** and **crypto isakmp key** commands.)

Examples

The following example configures an IKE policy with preshared keys as the authentication method (all other parameters are set to the defaults):

```
crypto isakmp policy 15
 authentication pre-share
 exit
```

Related Commands

Command	Description
crypto isakmp key	Configures a preshared authentication key.
crypto isakmp policy	Defines an IKE policy.

Command	Description
crypto key generate rsa (IKE)	Generates RSA key pairs.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

authentication command

To specify the HTTP command that is sent to the certification authority (CA) for authentication, use the **authentication command** in ca-profile-enroll configuration mode.

authentication command

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Use the **authentication command** to send the HTTP request to the CA server for certificate authentication. Before enabling this command, you must use the **authentication url** command.

After enabling this command, you can use the **parameter** command to specify enrollment parameters for your enrollment profile.

Examples

The following example shows how to configure certificate authentication via HTTP for the enrollment profile named “E”:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
authentication url	Specifies the URL of the CA server to which to send authentication requests.

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.
parameter	Specifies parameters for an enrollment profile.

authentication list (tti-registrar)

To authenticate the introducer in an Easy Secure Device Deployment (EzSDD) transaction, use the **authentication list** command in tti-registrar configuration mode. To disable the authentication, use the **no** form of this command.

authentication list *list-name*

no authentication list *list-name*

Syntax Description

list-name	Name of the list.

Defaults

An introducer is not authenticated.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command is used in EzSDD transactions. When the command is configured, the RADIUS or TACACS+ AAA server checks for a valid account by looking at the username and password.

The authentication list and the authorization list will usually both point to the same AAA list, but it is possible that the lists can be on different databases. This latter scenario is not recommended.

Examples

The following example shows that an authentication list named “authen-tac” has been configured. In this example, the authentication list is on a TACACS+ AAA server and the authorization list is on a RADIUS AAA server.

```
Router(config)# crypto wui tti registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-rad
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

Related Commands

Command	Description
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner in an EzSDD operation.
debug crypto wui	Displays information about an EzSDD operation.

Command	Description
template config	Specifies a remote URL for a Cisco IOS CLI configuration template.
template username	Establishes a template username and password to access the configuration template on the file system.

authentication terminal

To manually cut-and-paste certificate authentication requests, use the **authentication terminal** command in ca-profile-enroll configuration mode. To delete a current authentication request, use the **no** form of this command.

authentication terminal

no authentication terminal

Syntax Description

This command has no arguments or keywords.

Defaults

An authentication request is not specified.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

A user may manually cut-and-paste certificate authentication requests when a network connection between the router and certification authority (CA) is not available. After this command is enabled, the authentication request is printed on the console terminal so that it can be manually copied (cut) by the user.

Examples

The following example shows how to specify manual certificate authentication and certificate enrollment via HTTP:

```
crypto ca profile enrollment E
 authentication terminal
 enrollment terminal
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.

authentication url

To specify the URL of the certification authority (CA) server to which to send authentication requests, use the **authentication url** command in ca-profile-enroll configuration mode. To delete the authentication URL from your enrollment profile, use the **no** form of this command.

authentication url *url*

no authentication url *url*

Syntax Description

url	URL of the CA server to which your router should send authentication requests. If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, the *url* argument must be in the form http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA. If you are using TFTP for enrollment, the *url* argument must be in the form tftp://certserver/file_specification. (If the URL does not include a file specification, the fully qualified domain name [FQDN] of the router will be used.)

Defaults

Your router does not recognize the CA URL until you declare one using this command.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

If you do not specify the **authentication command** after you enable the **authentication url** command, the **authentication url** command functions the same as the **enrollment url** *url* command in trustpoint configuration mode. That is, the **authentication url** command will then be used only for certificate enrollment—not authentication.

This command allows the user to specify a different URL or a different method for authenticating a certificate and enrolling a certificate; for example, manual authentication and TFTP enrollment.

Examples

The following example shows how to configure an enrollment profile for direct HTTP enrollment with a CA server. In this example, the **authentication command** is also present.

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial
```

```
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

The following example shows how to configure the enrollment profile named "E" to perform certificate authentication via HTTP and manual certificate enrollment:

```
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment terminal
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
authentication command	Specifies the HTTP command that is sent to the CA for authentication.
crypto ca profile enrollment	Defines an enrollment profile.
enrollment	Specifies the enrollment parameters of your CA.

authorization

To enable authentication, authorization, and accounting (AAA) authorization for a specific line or group of lines, use the **authorization** command in line configuration mode. To disable authorization, use the **no** form of this command.

authorization {**arap** | **commands** *level* | **exec** | **reverse-access**} [**default** | *list-name*]

no authorization {**arap** | **commands** *level* | **exec** | **reverse-access**} [**default** | *list-name*]

Syntax Description

arap	Enables authorization for lines configured for AppleTalk Remote Access (ARA) protocol.
commands	Enables authorization on the selected lines for all commands at the specified privilege level.
level	Specific command level to be authorized. Valid entries are 0 through 15.
exec	Enables authorization to determine if the user is allowed to run an EXEC shell on the selected lines.
reverse-access	Enables authorization to determine if the user is allowed reverse access privileges.
default	(Optional) The name of the default method list, created with the **aaa authorization** command.
list-name	(Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa authorization** command.

Defaults

Authorization is not enabled.

Command Modes

Line configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list) for a particular type of authorization, you must apply the defined lists to the appropriate lines for authorization to take place. Use the **authorization** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

Examples

The following example enables command authorization (for level 15) using the method list named charlie on line 10:

```
line 10
 authorization commands 15 charlie
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

authorization (server-group)

To filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization, use the **authorization** command in server-group configuration mode. To remove the filter on the authorization request or reply, use the **no** form of the command.

authorization [request | reply] [**accept** | **reject**] *list-name*

Syntax Description

request	(Optional) Defines filters for outgoing authorization Access Requests.
reply	(Optional) Defines filters for incoming authorization Accept or Reject packets and for outgoing accounting requests.
accept	(Optional) Indicates that the required attributes and the attributes specified in the *list-name* argument will be accepted. All other attributes will be rejected.
reject	(Optional) Indicates that the attributes specified in the *list-name* will be rejected. All other attributes will be accepted.
list-name	Defines the given name for the accept or reject list.

Defaults

If specific attributes are not accepted or rejected, all attributes will be accepted.

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401ASR.
12.3(3)B	The **request** and **reply** keywords were added.
12.3(7)T	The **request** and **reply** keywords were integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

An accept or reject list (also known as a filter) for RADIUS authorization allows users to configure the network access server (NAS) to restrict the use of specific attributes, thereby preventing the NAS from processing unwanted attributes.

Only one filter may be used for RADIUS authorization per server group.

Note The listname must be the same as the listname defined in the **radius-server attribute list** command, which is used with the **attribute (server-group configuration)** command to add to an accept or reject list.

Examples

The following example shows how to configure accept list “min-author” in an Access-Accept packet from the RADIUS server:

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
 server 1.1.1.1
 authorization accept min-author
!
radius-server host 1.1.1.1 key mykey1
radius-server attribute list min-author
 attribute 6-7
```

The following example shows that the attribute “all-attr” will be rejected in all outbound authorization Access Request messages:

```
aaa group server radius ras
 server 272.19.192.238 auth-port 1745 acct-port 1746
 authorization request reject all-attr
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to the user.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
radius-server attribute list	Defines an accept or reject list name.

authorization list (global)

To specify the authentication, authorization, and accounting (AAA) authorization list, use the **authorization list** command in global configuration mode. To disable the authorization list, use the **no** form of this command.

authorization list *list-name*

no authorization list *list-name*

Syntax Description

list-name	Name of the AAA authorization list.

Defaults

An authorization list is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use the **authorization list** command to specify a AAA authorization list. For components that do not support specifying the application label, a default label of “any” from the AAA server will provide authorization. Likewise, a label of “none” from the AAA database indicates that the specified certificate is not valid. (The absence of any application label is equivalent to a label of “none,” but “none” is included for completeness and clarity.)

Examples

The following example shows that the AAA authorization list “maxaa” is specified:

```
aaa authorization network maxaaa group tacac+
aaa new-model
crypto ca trustpoint msca
enrollment url http://caserver.mycompany.com
 authorization list maxaa
 authorization username subjectname serialnumber
```

Related Commands

Command	Description
authorization username	Specifies the parameters for the different certificate fields that are used to build the AAA username.

authorization list (tti-registrar)

To specify the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS command-line interface (CLI) snippet that is sent back to the petitioner in an Easy Secure Device Deployment (EzSDD) operation, use the **authorization list** command in tti-registrar configuration mode. To disable the subject name and list of template variables, use the **no** form of this command.

authorization list *list-name*

no authorization list *list-name*

Syntax Description

list-name	Name of the list.

Defaults

There is no authorization list on the AAA server.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command is used in EzSDD operations. When the command is used, the RADIUS or TACACS+ AAA server stores the subject name and template variables. The name and variables are sent back to the petitioner in the Cisco IOS CLI snippets. This list and the authorization list are usually on the same database, but they can be on different AAA databases. (Storing lists on different databases is not recommended.)

When a petitioner makes an introducer request, multiple queries are sent to the AAA list database on the RADIUS or TACACS+ server. The queries search for entries of the following form:

```
user Password <userpassword>
   cisco-avpair="ttti:subjectname=<<DN subjectname>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#=<<value>>"
```

Note The existence of a valid AAA username record is enough to pass the authentication check. The "cisco-avpair=tti" information is necessary only for the authorization check.

If a subject name was received in the authorization response, the TTI registrar stores it in the enrollment database, and that "subjectname" overrides the subject name that is supplied in the subsequent certificate request (PKCS10) from the petitioner device.

The numbered “tti:iosconfig” values are expanded into the TTI Cisco IOS snippet that is sent to the petitioner. The configurations replace any numbered ($1 through $9) template variable. Because the default Cisco IOS snippet template does not include the variables $1 through $9, these variables are ignored unless you configure an external Cisco IOS snippet template. To specify an external configuration, use the **template config** command.

Note The template configuration location may include a variable “$n,” which is expanded to the name with which the user is logged in.

Examples

The following example shows that the authorization list name is “author-rad.” In this example, the authentication list is on a TACACS+ AAA server and the authorization list is on a RADIUS AAA server.

```
Router(config)# crypto wui tti registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-rad
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

Related Commands

Command	Description
authentication list (tti-registrar)	Authenticates the introducer in an EzSDD operation.
debug crypto wui	Displays information about an EzSDD operation.
template config	Specifies a remote URL for a Cisco IOS CLI configuration template.
template username	Establishes a template username and password to access the configuration template on the file system.

authorization username

To specify the parameters for the different certificate fields that are used to build the authentication, authorization and accounting (AAA) username, use the **authorization username** command in global configuration mode. To disable the parameters, use the **no** form of this command.

authorization username {subjectname *subjectname}*

no authorization username {subjectname *subjectname}*

Syntax Description

subjectname	AAA username that is generated from the certificate subject name.
subjectname	Builds the username. The f**ollowing are** options that may be used as the AAA username: • **all**—Entire distinguished name (subject name) of the certificate. • **commonname**—Certificate common name. • **country**—Certificate country. • **email**—Certificate email. • **ipaddress**—Certificate ipaddress. • **locality**—Certificate locality. • **organization**—Certificate organization. • **organizationalunit**—Certificate organizational unit. • **postalcode**—Certificate postal code. • **serialnumber**—Certificate serial number. • **state**—Certificate state field. • **streetaddress**—Certificate street address. • **title**—Certificate title. • **unstructuredname**—Certificate unstructured name.

Defaults

Parameters for the certificate fields are not specified.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.3(11)T	The **all** option for the *subjectname argument* was added.

Examples

The following example shows that the serialnumber option is to be used as the authorization username:

```
aaa authorization network maxaaa group tacac+
```

```
aaa new-model
crypto ca trustpoint msca
enrollment url http://caserver.mycompany.com
 authorization list maxaaa
 authorization username subjectname serialnumber
```

Related Commands

Command	Description
authorization list	Specifies the AAA authorization list.

auth-type

To set policy for devices that are dynamically authenticated or unauthenticated, use the **auth-type** command in identity profile configuration mode. To remove the policy that was specified, use the **no** form of this command.

auth-type {authorize | not-authorize} policy *policy-name*

no auth-type {authorize | not-authorize} policy *policy-name*

Syntax Description

authorize	Policy is specified for all authorized devices.
not-authorize	Policy is specified for all unauthorized devices.
policy *policy-name*	Specifies the name of the identity policy to apply for the associated authentication result.

Defaults

A policy is not set for authorized or unauthorized devices.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command is used when a device is dynamically authenticated or unauthenticated by the network access device, and the device requires the name of the policy that should be applied for that authentication result.

Examples

The following example shows that 802.1x authentication applies to the identity policy “grant” for all dynamically authenticated hosts:

```
Router (config)# ip access-list extended allow-acl
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nacl)# exit

Router (config)# identity policy grant
Router (config-identity-policy)# access-group allow-acl
Router (config-identity-policy)# exit

Router (config)# identity profile dot1x
Router (config-identity-prof)# auth-type authorize policy grant
```

Related Commands

Command	Description
identity policy	Creates an identity policy.
identity profile dot1x	Creates an 802.1x identity profile.

auto secure

To secure the management and forwarding planes of the router, use the **auto secure** command in privileged EXEC mode.

auto secure [**management** | **forwarding**] [**no-interact** | **full**] [**ntp** | **login** | **ssh** | **firewall** | **tcp-intercept**]

Syntax Description

management	(Optional) Only the management plane will be secured.
forwarding	(Optional) Only the forwarding plane will be secured.
no-interact	(Optional) The user will not be prompted for any interactive configurations. If this keyword is not enabled, the command will show the user the noninteractive configuration and the interactive configurations thereafter.
full	(Optional) The user will be prompted for all interactive questions. This is the default.
ntp	(Optional) Specifies the configuration of the Network Time Protocol (NTP) feature in the AutoSecure command line-interface (CLI).
login	(Optional) Specifies the configuration of the Login feature in the AutoSecure CLI.
ssh	(Optional) Specifies the configuration of the Secure Shell (SSH) feature in the AutoSecure CLI.
firewall	(Optional) Specifies the configuration of the firewall feature in the AutoSecure CLI.
tcp-intercept	(Optional) Specifies the configuration of the TCP-Intercept feature in the AutoSecure CLI.

Defaults

Autosecure is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)T.
12.3(4)T	The following keywords were added in Cisco IOS Release 12.3(4)T: **full**, **ntp**, **login**, **ssh**, **firewall**, and **tcp-intercept**.
12.3(8)T	Support for the roll-back functionality and system logging messages were added to Cisco IOS Release 12.3(8)T.

Usage Guidelines

The **auto secure** command allows a user to disable common IP services that can be exploited for network attacks by using a single CLI. This command eliminates the complexity of securing a router both by automating the configuration of security features and by disabling certain features that are enabled by default and that could be exploited for security holes.

Caution If you are using Security Device Manager (SDM), you must manually enable the HTTP server via the **ip http server** command.

This command takes you through a semi-interactive session (also known as the AutoSecure dialogue) in which to secure the management and forwarding planes. This command gives you the option to secure just the management or forwarding plane; if neither option is selected, the dialogue will ask you to configure both planes.

Caution If your device is managed by a network management (NM) application, securing the management plane could turn off vital services and disrupt the NM application support.

This command also allows you to go through all noninteractive configuration portions of the dialogue before the interactive portions. The noninteractive portions of the dialogue can be enabled by selecting the optional **no-interact** keyword.

Roll-back and System Logging Message Support

In Cisco IOS Release 12.3(8)T, support for roll-back of the AutoSecure configuration is introduced. Roll-back enables a router to revert back to its preautosecure configuration state if the AutoSecure configuration fails.

System Logging Messages capture any changes or tampering of the AutoSecure configuration that were applied on the running configuration.

Note Prior to Cisco IOS Release 12.3(8)T, roll-back of the AutoSecure configuration is unavailable; thus, you should always save the running configuration before configuring AutoSecure.

Examples

The following example shows how to enable AutoSecure to secure only the management plane:

```
Router# auto secure management
```

Related Commands

Command	Description
ip http server	Enables the HTTP server on your system, including the Cisco web browser user interface.
show auto secure config	Displays AutoSecure configurations.

auto-enroll

To enable certificate autoenrollment, use the **auto-enroll** command in ca-trustpoint configuration mode. To disable certificate autoenrollment, use the **no** form of this command.

auto-enroll [*percent*] [**regenerate**]

no auto-enroll [*percent*] [**regenerate**]

Syntax Description

percent	(Optional) The renewal percentage parameter causes the router to request a new certificate after the specified percent lifetime of the current certificate is reached. If not specified, the request for a new certificate is made when the old certificate expires. The specified percent value must not be less than 10.
regenerate	(Optional) Generates a new key for the certificate even if the named key already exists.

Defaults

Certificate autoenrollment is not enabled.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(7)T	The *percent* argument was added to support key rollover.

Usage Guidelines

Use the **auto-enroll** command to automatically request a router certificate from the certification authority (CA) that is using the parameters in the configuration. This command will generate a new RSA key only if a new key does not exist with the requested label.

A trustpoint that is configured for certificate autoenrollment will attempt to reenroll when the router certificate expires.

Use the **regenerate** keyword to provide seamless key rollover for manual certificate enrollment. A new key pair is created with a temporary name, and the old certificate and key pair are retained until a new certificate is received from the CA. When the new certificate is received, the old certificate and key pair are discarded and the new key pair is renamed with the name of the original key pair. Some CAs require a new key for reenrollment to work.

If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable:

```
! RSA keypair associated with trustpoint is exportable
```

Examples

The following example shows how to configure the router to autoenroll with the CA named "trustme1" on startup. In this example, the **regenerate** keyword is issued, so a new key will be generated for the certificate. The renewal percentage is configured as 90 so if the certificate has a lifetime of one year, a new certificate is requested 36.5 days before the old certificate expires.

```
crypto ca trustpoint trustme1
 enrollment url http://trustme1.company.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet0
 serial-number none
 auto-enroll 90 regenerate
 password revokeme
 rsakeypair trustme1 2048
 exit
crypto ca authenticate trustme1
```

Related Commands

Command	Description
crypto ca authenticate	Retrieves the CA certificate and authenticates it.
crypto ca trustpoint	Declares the CA that your router should use.

backup-gateway

To configure a server to "push down" a list of backup gateways to the client, use the **backup-gateway** command in global configuration mode. To remove a backup gateway, use the **no** form of this command.

backup-gateway {*ip-address* | *hostname*}

no backup-gateway {*ip-address* | *hostname*}

Syntax Description

ip-address	IP address of the gateway.
hostname	Host name of the gateway.

Defaults

A list of backup gateways is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Before using the **backup-gateway** command, you must first configure the **crypto isakmp client configuration group** command.

An example of an attribute-value (AV) pair for the backup gateway attribute is as follows:

```
ipsec:ipsec-backup-gateway=10.1.1.1
```

Note

- If you have to configure more than one backup gateway, you have to add a **backup-gateway** command line for each.
- You can configure a maximum of 10 backup gateways.

Examples

The following example shows that gateway 10.1.1.1 has been configured as a backup gateway:

```
crypto isakmp client configuration group group1
 backup-gateway 10.1.1.1
```

The following output example shows that five backup gateways have been configured:

```
crypto isakmp client configuration group sdm
 key 6 RMZPPMRQMSdiZNJg`EBbCWTKSTi\d[
 pool POOL1
 acl 150
 backup-gateway 172.12.12.12
 backup-gateway 172.12.12.13
 backup-gateway 172.12.12.14
 backup-gateway 172.12.12.130
```

```
backup-gateway 172.12.12.131
max-users 250
max-logins 2
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

bidirectional

To enable incoming and outgoing IP traffic to be exported across a monitored interface, use the **bidirectional** command in router IP traffic export (RITE) configuration mode. To return to the default functionality, use the **no** form of this command.

bidirectional

no bidirectional

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not enabled, only incoming traffic is exported.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

By default, only incoming IP traffic is exported. If you choose to export outgoing IP traffic, you must issue both the **bidirectional** command, which enables outgoing traffic to be exported, and the **outgoing** command, which specifies how the outgoing traffic will be filtered.

The **ip traffic-export profile** command allows you to begin a profile that can be configured to export IP packets as they arrive or leave a selected router ingress interface. A designated egress interface exports the captured IP packets out of the router. Thus, the router can export unaltered IP packets to a directly connected device.

Examples

The following example shows how to export both incoming and outgoing IP traffic on the FastEthernet interface:

```
Router(config)# ip traffic-export profile johndoe
Router(config-rite)# interface FastEthernet1/0.1
Router(config-rite)# bidirectional
Router(config-rite)# incoming access-list 101
Router(config-rite)# outgoing access-list 101
Router(config-rite)# mac-address 6666.6666.3333
```

Related Commands

Command	Description
interface (RITE)	Specifies the outgoing interface for exporting traffic.

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
outgoing	Configures filtering for outgoing export traffic.

block count

To lock out group members for a length of time after a set number of incorrect passwords, use the **block count** command in local RADIUS server group configuration mode. To remove the user block after invalid login attempts, use the **no** form of this command.

block count *count* **time** {*seconds* | **infinite}**

no block count *count* **time** {*seconds* | **infinite}**

Syntax Description

count	Number of failed passwords that triggers a lockout.
time	Time that the lockout should last.
seconds	Number of seconds that the lockout should last.
infinite	Length of time for the lockout is indefinite until an administrator manually unblocks the locked username.

Defaults

No default behavior or values

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

If the **infinite keyword** is entered, an administrator must manually unblock the locked username.

Examples

The following command locks out group members for 120 seconds after three incorrect passwords are entered:

```
block count 3 time 120
```

Related Commands

Command	Description
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.

Command	Description
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

ca trust-point

To identify the trustpoints that will be used to validate a certificate during Internet Key Exchange (IKE) authentication, use the **ca trust-point** command in ISAKMP profile configuration mode. To remove the trustpoint, use the **no** form of this command.

ca trust-point *trustpoint-name*

no ca trust-point *trustpoint-name*

Syntax Description

trustpoint-name	The trustpoint name as defined in the global configuration.

Defaults

If there is no trustpoint defined in the Internet Security Association and Key Management Protocol (ISAKMP) profile configuration, the default is to validate the certificate using all the trustpoints that are defined in the global configuration.

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The **ca trust-point** command can be used multiple times to define more than one trustpoint.

This command is useful when you want to restrict validation of certificates to a list of trustpoints. For example, the router global configuration has two trustpoints, A and B, which are trusted by VPN1 and VPN2, respectively. Each Virtual Private Network (VPN) wants to restrict validation only to its trustpoint.

Before you can use this command, you must enter the **crypto isakmp profile** command.

Note A router initiating IKE and a router responding to the IKE request should have symmetrical trustpoint configurations. For example, a responding router (in IKE Main Mode) performing RSA signature encryption and authentication might use trustpoints that were defined in the global configuration when sending the CERT-REQ payloads. However, the router might use a restricted list of trustpoints that were defined in the ISAKMP profile for the certificate verification. If the peer (the IKE initiator) is configured to use a certificate whose trustpoint is in the global list of the responding router but not in ISAKMP profile of the responding router, the certificate will be rejected. (However, if the initiating router does not know about the trustpoints in the global configuration of the responding router, the certificate can still be authenticated.)

Examples

The following example specifies two trustpoints, A and B. The ISAKMP profile configuration restricts each VPN to one trustpoint.

```
crypto ca trustpoint A
```

```
enrollment url http://kahului:80
crypto ca trustpoint B
enrollment url http://arjun:80
!
crypto isakmp profile vpn1
 trustpoint A
!
crypto isakmp profile vpn2
 ca trust-point B
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile.

cache clear age

To specify when, in minutes, cache entries expire and the cache is cleared, use the **cache clear age** command in AAA filter configuration mode. To return to the default value, use the **no** form of this command.

cache clear age *minutes*

no cache clear age

Syntax Description

minutes	Any value from 0 to 4294967295; the default value is 1440 minutes.

Defaults

1440 minutes (1 day)

Command Modes

AAA filter configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

After enabling the **aaa cache filter** command, which allows you to configure cache filter parameters, you can use the **cache clear age** command to specify when cache entries should expire. If this command is not specified, the default value (1440 minutes) will be enabled.

Examples

The following example shows how to configure the cache entries to expire every 60 minutes:

```
aaa cache filter
 cache clear age 60
```

Related Commands

Command	Description
aaa cache filter	Enables filter cache configuration.

cache disable

To disable the cache, use the **cache disable** command in AAA filter configuration mode. To return to the default, use the **no** form of this command.

cache disable

no cache disable

Syntax Description

This command has no arguments or keywords.

Defaults

Caching is enabled.

Command Modes

AAA filter configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

After enabling the **aaa cache filter** command, which allows you to configure cache filter parameters, you can use the **cache disable** command to disable filter caching. This command can be used to verify that the access control lists (ACLs) are being downloaded.

Examples

The following example shows how to disable filter caching:

```
aaa cache filter
 cache disable
```

Related Commands

Command	Description
aaa cache filter	Enables filter cache configuration.

cache max

To limit the absolute number of entries that a cache can maintain for a particular server, use the **cache max** command in AAA filter configuration mode. To return to the default value, use the **no** form of this command.

cache max *number*

no cache max

Syntax Description

number	Maximum number of entries the cache can maintain. Any value from 0 to 4294967295; the default value is 100 entries.

Defaults

100 entries

Command Modes

AAA filter configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

After enabling the **aaa cache filter** command, which allows you to configure cache filter parameters, you can use the **cache max** command to specify the maximum number of entries the cache can have at any given time. If this command is not specified, the default value (100 entries) will be enabled.

Examples

The following example shows how to configure the cache to maintain a maximum of 150 entries:

```
aaa cache filter
 password mycisco
 cache max 150
```

Related Commands

Command	Description
aaa cache filter	Enables filter cache configuration.

cache refresh

To refresh a cache entry after a new session begins, use the **cache refresh** command in AAA filter configuration mode. To disable this functionality, use the **no** form of this command.

cache refresh

no cache refresh

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

AAA filter configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The **cache refresh** command is used in an attempt to keep cache entries from the filter server, that are being referred to by new sessions, within the cache. This command resets the idle timer for these entries when they are referenced by new calls.

Examples

The following example shows how to disable the **cache refresh** command:

```
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
```

Related Commands

Command	Description
aaa cache filter	Enables filter cache configuration.

call admission limit

To instruct Internet Key Exchange (IKE) to drop security association (SA) requests (that is, calls for Call Admission Control [CAC]) when a specified percentage of system resources is being consumed, use the **call admission limit** command in global configuration mode. To disable this feature, use the **no** form of this command.

call admission limit *percent*

no call admission limit *percent*

Syntax Description

percent	Percentage of the system resources that, when used, causes IKE to stop accepting new SA requests. Valid values are 1 to 100.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

It is recommended that initially you specify a value of 90. You will have to alter the value depending on the network topology, the capabilities of the router, and the traffic patterns.

Examples

The following example causes IKE to drop calls when 90 percent of system resources are being used:

```
Router(config)# call admission limit 90
```

Related Commands

Command	Description
show call admission statistics	Monitors the global CAC configuration parameters and the behavior of CAC.

call guard-timer

To set a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request, use the **call guard-timer** command in controller configuration mode. To remove the **call guard-timer** command from your configuration file, use the **no** form of this command.

call guard-timer *milliseconds* [**on-expiry** {**accept** | **reject**}]

no call guard-timer *milliseconds* [**on-expiry** {**accept** | **reject**}]

Syntax Description

milliseconds	Specifies the number of milliseconds to wait for a response from the RADIUS server.
on-expiry accept	(Optional) Accepts the call if a response is not received from the RADIUS server within the specified time.
on-expiry reject	(Optional) Rejects the call if a response is not received from the RADIUS server within the specified time.

Defaults

No default behavior or values.

Command Modes

Controller configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

The following example shows a guard timer that is set at 20000 milliseconds. A call will be accepted if the RADIUS server has not responded to a preauthentication request when the timer expires.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
  call guard-timer 20000 on-expiry accept

aaa preauth
group radius
  dnis required
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.

cdp-url

To specify a certificate revocation list (CRL) distribution point (CDP) to be used in certificates that are issued by the certificate server, use the **cdp-url** command in certificate server configuration mode. To remove a CDP from your configuration, use the **no** form of this command.

cdp-url *url*

no cdp-url *url*

Syntax Description

url	HTTP URL where CRLs are published.

Defaults

When verifying a certificate that does not have a specified CDP, Cisco IOS public key infrastructure (PKI) clients will use Simple Certificate Enrollment Protocol (SCEP) to retrieve the CRL directly from their configured certificate server.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

CRLs are issued once every specified time period via the **lifetime crl** command. Thereafter, the CRL is written to the specified database location as *ca-label*.crl (where *ca-label* is the name of the certificate server). It is the responsibility of the network administrator to ensure that the CRL is available from the location that is specified via the **cdp-url** command. If the **cdp-url** command is not specified, the CDP certificate extension will not be included in the certificates that are issued by the certificate server. Thus, Cisco IOS public key infrastructure (PKI)l clients will automatically use SCEP to retrieve a CRL from the certificate server, which puts an additional load on the certificate server because it must provide SCEP server support to for each CRL request.

Note The CRL will always be available via SCEP, which is enabled by default, if the HTTP server is enabled.

Note For large PKI deployments, it is recommended that you configure an HTTP-based CDP; for example, cdp-url http://myhttpserver.company.com/mycs.crl.

The CDP URL may be changed after the certificate server is running, but existing certificates will not be reissued with the new CDP that is specified via the **cdp-url** command.

The certificate server supports only one CDP; thus, all certificates that are issued include the same CDP.

Examples

The following example shows how to configure a CDP:

```
Router(config)# crypto pki server aaa
Router(cs-server)# database level minimum
Router(cs-server)# database url tftp://10.1.1.1/johndoe/
Router(cs-server)# issuer-name CN=aaa
Router(cs-server)# cdp-url http://msca-root.cisco.com/certEnroll/aaa.crl
```

Verifying a CDP Configuration

The following example is sample output from the **show crypto ca certificates** command, which allows you to verify the specified CDP. In this example, the CDP is "http://msca-root.cisco.com/certEnroll/aaa.crl."

```
Router# show crypto ca certificates

Certificate
  Status: Available
  Certificate Serial Number: 03
  Certificate Usage: General Purpose
  Issuer:
    CN = aaa
  Subject:
    Name: Router.cisco.com
    OID.1.2.840.113549.1.9.2 = Router.cisco.com
  CRL Distribution Point:
    http://msca-root.cisco.com/certEnroll/aaa.crl
  Validity Date:
    start date: 18:44:49 GMT Jun 6 2003
    end   date: 18:44:49 GMT Jun 5 2004
    renew date: 00:00:00 GMT Jan 1 1970
  Associated Trustpoints: bbb
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto pki server revoke	Revokes a certificate based on its serial number.
lifetime crl	Defines the lifetime of the CRL that is used by the certificate server.
show crypto ca certificates	Displays information about your certificate, the certification authority certificate, and any registration authority certificates.

certificate

To manually add certificates, use the **certificate** command in certificate chain configuration mode. To delete your router's certificate or any registration authority certificates stored on your router, use the **no** form of this command.

certificate *certificate-serial-number*

no certificate *certificate-serial-number*

Syntax Description

certificate-serial-number	Serial number of the certificate to add or delete.

Defaults

No default behavior or values.

Command Modes

Certificate chain configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

You could use this command to manually specify a certificate. However, this command is rarely used in this manner. Instead, this command is usually used only to add or delete certificates.

Examples

The following example deletes the router's certificate. In this example, the router had a general purpose RSA key pair with one corresponding certificate. The **show** command is used in this example to determine the serial number of the certificate to be deleted.

```
myrouter# show crypto ca certificates

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set

myrouter# configure terminal
myrouter(config)# crypto ca certificate chain myca
myrouter(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
myrouter(config-cert-chain)# exit
```

Related Commands

Command	Description
crypto ca certificate chain	Enters the certificate chain configuration mode.

clear aaa cache filterserver acl

To clear the cache status for a particular filter or all filters, use the **clear aaa cache filterserver acl** command in EXEC mode.

clear aaa cache filterserver acl [*filter-name*]

Syntax Description

filter-name	(Optional) Cache status of a specified filter is cleared.

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

After you clear the cache status for a particular filter or all filters, it is recommended that you enable the **show aaa cache filterserver** command to verify that the cache status.

Examples

The following example shows how to clear the cache for all filters:

```
clear aaa cache filterserver acl
```

Related Commands

Command	Description
show aaa cache filterserver	Displays the cache status.

clear access-template

To manually clear a temporary access list entry from a dynamic access list, use the **clear access-template** command in EXEC mode.

clear access-template [*access-list-number* | *name*] [*dynamic-name*] [*source*] [*destination*]

Syntax Description

access-list-number	(Optional) Number of the dynamic access list from which the entry is to be deleted.
name	(Optional) Name of an IP access list from which the entry is to be deleted. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.
dynamic-name	(Optional) Name of the dynamic access list from which the entry is to be deleted.
source	(Optional) Source address in a temporary access list entry to be deleted.
destination	(Optional) Destination address in a temporary access list entry to be deleted.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command is related to the lock-and-key access feature. It clears any temporary access list entries that match the parameters you define.

Examples

The following example clears any temporary access list entries with a source of 172.20.1.12 from the dynamic access list named vendor:

```
clear access-template vendor 172.20.1.12
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-template	Places a temporary access list entry on a router to which you are connected manually.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

clear crypto call admission statistics

To clear the counters that track the number of accepted and rejected Internet Key Exchange (IKE) requests, use the **call admission limit** command in global configuration mode.

clear crypto call admission statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example sets to zero the number of accepted and rejected IKE requests:

```
Router(config)# clear crypto call admission statistics
```

Related Commands

Command	Description
show crypto call admission statistics	Monitors Crypto CAC statistics.

clear crypto engine accelerator counter

To reset the statistical and error counters of the hardware accelerator of the router to zero, use the **clear crypto engine accelerator counter** command in privileged EXEC mode.

clear crypto engine accelerator counter

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XL	This command was introduced for the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

Examples

The following example shows the statistical and error counters of the router being cleared to zero:

```
clear crypto engine accelerator counter
```

Related Commands

Command	Description
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.

Command	Description
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.
crypto ipsec	Defines the IPSec security associations and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator ring	Displays the contents of command and transmits rings for the crypto engine.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine SA database.
show crypto engine accelerator statistic	Displays the current run-time statistics and error counters for the crypto engine.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

clear crypto ipsec client ezvpn

To reset the Cisco Easy VPN remote state machine and bring down the Cisco Easy VPN remote connection on all interfaces or on a given interface (tunnel), use the **clear crypto ipsec client ezvpn** command in privileged EXEC mode. If a tunnel name is specified, only the specified tunnel is cleared.

clear crypto ipsec client ezvpn [*name*]

Syntax Description

name	(Optional) Identifies the IPSec virtual private network (VPN) tunnel to be disconnected or cleared with a unique, arbitrary name. If no name is specified, all existing tunnels are disconnected or cleared.

Defaults

If no tunnel name is specified, all active tunnels on the machine are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)YA	This command was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(8)YJ	This command was enhanced to specify an IPSec VPN tunnel to be cleared or disconnected for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

The **clear crypto ipsec client ezvpn** command resets the Cisco Easy VPN remote state machine, bringing down the current Cisco Easy VPN remote connection and bringing it back up on the interface. If you specify a tunnel name, only that tunnel is cleared. If no tunnel name is specified, all active tunnels on the machine are cleared.

If the Cisco Easy VPN remote connection for a particular interface is configured for autoconnect, this command also initiates a new Cisco Easy VPN remote connection.

Examples

The following example shows the Cisco Easy VPN remote state machine being reset:

```
Router# clear crypto ipsec client ezvpn
```

Related Commands

Command	Description
crypto ipsec client ezvpn (global)	Creates a Cisco Easy VPN remote configuration.
crypto ipsec client ezvpn (interface)	Assigns a Cisco Easy VPN remote configuration to an interface.

clear crypto isakmp

To clear active Internet Key Exchange (IKE) connections, use the **clear crypto isakmp** command in privileged EXEC mode.

clear crypto isakmp [*connection-id*] [**active** | **standby**]

Syntax Description

connection-id	(Optional) ID of the connection that is to be cleared. If this argument is not used, all existing connections will be cleared.
active	(Optional) Clears only IKE security associations (SAs) in the active state. For each active SA that is cleared, the standby router will be notified to clear the corresponding standby SA.
standby	(Optional) Clears only IKE SAs in the standby (secondary) state. **Note** If the router is in standby mode, the router will immediately resynchronize the standby SAs; thus, it may appear as though the standby SAs were not cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(11)T	The **active** and **standby** keywords were added.

Usage Guidelines

Caution If the *connection-id* argument is not used, all existing IKE connections will be cleared when this command is issued.

Examples

The following example clears an IKE connection between two peers connected by interfaces 172.21.114.123 and 172.21.114.67:

```
Router# show crypto isakmp sa

    dst           src           state        conn-id   slot
172.21.114.123 172.21.114.67  QM_IDLE           1       0
209.165.201.1  209.165.201.2  QM_IDLE           8       0

Router# clear crypto isakmp 1

Router# show crypto isakmp sa

    dst           src           state        conn-id   slot
209.165.201.1  209.165.201.2  QM_IDLE           8       0

Router#
```

Related Commands

Command	Description
show crypto isakmp sa	Displays current IKE SAs.

clear crypto sa

To delete IP Security (IPSec) security associations (SAs), use the **clear crypto sa** command in privileged EXEC mode.

clear crypto sa [**active** | **standby**]

Virtual Routing and Forwarding (VRF) Syntax

clear crypto sa peer [**vrf** *fvrf-name*] *address*

clear crypto sa [**vrf** *ivrf-name*]

Crypto Map Syntax

clear crypto sa map *map-name*

IP Address, Security Protocol Standard, and SPI Syntax

clear crypto sa entry *destination-address protocol spi*

Traffic Counters Syntax

clear crypto sa counters

Syntax Description

active	(Optional) Clears only IPSec SAs that are in the active state.
standby	(Optional) Clears only IPSec SAs that are in the standby state. **Note** If the router is in standby mode, the router will immediately resynchronize the standby SAs; thus, it may appear as though the standby SAs were not cleared.
peer [**vrf** *fvrf-name*] *address*	Deletes any IPSec SAs for the specified peer. The *fvrf-name* argument specifies the front door VRF (FVRF) of the peer address.
vrf *ivrf-name*	(Optional) Clears all IPSec SAs whose inside virtual routing and forwarding (IVRF) is the same as the *ivrf-name*.
map	Deletes any IPSec SAs for the named crypto map set.
map-name	Specifies the name of a crypto map set.
entry	Deletes the IPSec SA with the specified address, protocol, and security parameter index (SPI).
destination-address	Specifies the IP address of the remote peer.
protocol	Specifies either the Encapsulation Security Protocol (ESP) or Authentication Header (AH).
spi	Specifies an SPI (found by displaying the SA database).
counters	Clears the traffic counters maintained for each SA; the **counters** keyword does not clear the SAs themselves.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(15)T	The **vrf** keyword and *fvrf-name* argument for **clear crypto sa peer** were added. The **vrf** keyword and *ivrf-name* argument for **clear crypto sa** were added.
12.3(11)T	The **active** and **standby** keywords were added.

Usage Guidelines

This command clears (deletes) IPSec SAs.

If the SAs were established via Internet Key Exchange (IKE), they are deleted and future IPSec traffic will require new SAs to be negotiated. (When IKE is used, the IPSec SAs are established only when needed.)

If the SAs are manually established, the SAs are deleted and reinstalled. (When IKE is not used, the IPSec SAs are created as soon as the configuration is completed.)

Note If the **peer**, **map**, **entry**, **counters, active**, or **standby** keywords are not used, all IPSec SAs will be deleted.

- The **peer** keyword deletes any IPSec SAs for the specified peer.
- The **map** keyword deletes any IPSec SAs for the named crypto map set.
- The **entry** keyword deletes the IPSec SA with the specified address, protocol, and SPI.
- The **active** and **standby** keywords delete the IPSec SAs in the active or standby state, respectively.

If any of the above commands cause a particular SA to be deleted, all the "sibling" SAs—that were established during the same IKE negotiation—are deleted as well.

The **counters** keyword simply clears the traffic counters maintained for each SA; it does not clear the SAs themselves.

If you make configuration changes that affect SAs, these changes will not apply to existing SAs but to negotiations for subsequent SAs. You can use the **clear crypto sa** command to restart all SAs so that they will use the most current configuration settings. In the case of manually established SAs, if you make changes that affect SAs you must use the **clear crypto sa** command before the changes take effect.

If the router is processing active IPSec traffic, it is suggested that you clear only the portion of the SA database that is affected by the changes, to avoid causing active IPSec traffic to temporarily fail.

Note that this command clears only IPSec SAs; to clear IKE state, use the **clear crypto isakmp** command.

Examples

The following example clears (and reinitializes if appropriate) all IPSec SAs at the router:

```
clear crypto sa
```

The following example clears (and reinitializes if appropriate) the inbound and outbound IPSec SAs established, along with the SA established for address 10.0.0.1 using the AH protocol with the SPI of 256:

```
clear crypto sa entry 10.0.0.1 AH 256
```

The following example clears all the SAs for VRF VPN1:

```
clear crypto sa vrf vpn1
```

Related Commands

Command	Description
clear crypto isakmp	Clears active IKE connections.

clear crypto session

To delete crypto sessions (IP Security [IPSec] and Internet Key Exchange [IKE] security associations [SAs]), use the **clear crypto session** command in privileged EXEC mode.

clear crypto session [local *ip-address* [**port** *local-port*]] [**remote** *ip-address* [**port** *remote-port*]] | [**fvrf** *vrf-name*] [**ivrf** *vrf-name*]

IPSec and IKE Stateful Failover Syntax

clear crypto session [**active** | **standby**]

Syntax Description

local *ip-address*	(Optional) Clears crypto sessions for a local crypto endpoint. • The *ip-address* is the IP address of the local crypto endpoint.
port *local-port*	(Optional) IKE port of the local endpoint. The *local-port* value can be 1 through 65535. The default value is 500.
remote *ip-address*	(Optional) Clears crypto sessions for a remote IKE peer. • The *ip-address* is the IP address of the remote IKE peer.
port *remote-port*	(Optional) IKE port of the remote endpoint to be deleted. The *remote-port* value can be from 1 through 65535. The default value is 500.
fvrf *vrf-name*	(Optional) Specifies the front door virtual routing and forwarding (FVRF) session that is to be cleared.
ivrf *vrf-name*	(Optional) Specifies the inside VRF (IVRF) session that is to be cleared.
active	(Optional) Clears only IPSec and IKE SAs in the active state.
standby	(Optional) Clears only IPSec and IKE SAs in the standby state. **Note** If the router is in standby mode, the router will immediately resynchronize the standby SAs with the active router.

Defaults

If the **clear crypto session** command is entered without any keywords, all existing sessions will be deleted. The IPSec SAs will be deleted first. Then the IKE SAs are deleted. Port default values are 500.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(11)T	The **active** and **standby** keywords were added.

Usage Guidelines

To clear a specific crypto session or a subset of all the sessions, you need to provide session-specific parameters, such as a local or remote IP address, a local or remote port, an FVRF name, or an IVRF name.

If a local IP address is provided as a parameter when you use the **clear crypto session** command, all the sessions (and their IKE SAs and IPSec SAs) that share the IP address as a local crypto endpoint (IKE local address) will be deleted.

Examples

The following example shows that all crypto sessions will be deleted:

```
Router# clear crypto session
```

The following example shows that the crypto session of the FVRF named “blue” will be deleted:

```
Router# clear crypto session fvrf blue
```

The following example shows that the crypto sessions of the FVRF “blue” and the IVRF session “green” will be deleted:

```
Router# clear crypto session fvrf blue ivrf green
```

The following example shows that the crypto sessions of the local endpoint 10.1.1.1 and remote endpoint 10.2.2.2 will be deleted. The local endpoint port is 5, and the remote endpoint port is 10.

```
Router# clear crypto session local 10.1.1.1 port 5 remote 10.2.2.2 port 10
```

Related Commands

Command	Description
description	Adds a description for an IKE peer.
show crypto isakmp peer	Displays peer descriptions.
show crypto session	Displays status information for active crypto sessions in a router.

clear dot1x

To clear 802.1X interface information, use the **clear dot1x** command in privileged EXEC mode.

clear dot1x {all | interface *interface-name}*

Syntax Description

all	Clears 802.1X information for all interfaces.
interface *interface-name*	Clears 802.1X information for the specified interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Examples

The following configuration shows that 802.1X information will be cleared for all interfaces:

```
Router# clear dot1x all
```

The following configuration shows that 802.1X information will be cleared for the Ethernet 0 interface:

```
Router# clear dot1x interface ethernet 0
```

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
identity profile default	Creates an identity profile and enters dot1x profile configuration mode.
show dot1x	Shows details for an identity profile.

clear eou

To clear all client device entries that are associated with a particular interface or that are on the network access device (NAD), use the **clear eou** command in privileged EXEC mode.

clear eou {all | authentication {clientless | eap | static} | interface {*interface-type***} | ip {***ip-address***} | mac {***mac-address***} | posturetoken {***name***}}**

Syntax Description

all	Clears all client device entries.
authentication	Authentication type.
clientless	Authentication type is clientless.
eap	Authentication type is Extensible Authentication Procotol (EAP).
static	Authentication type is static.
interface	Provides information about the interface.
interface-type	Type of interface (see Table 12 for a list of interface types).
ip	Specifies an IP address.
ip-address	IP address of the client device.
mac	Specifies a MAC address.
mac-address	The 48-bit address of the client device.
posturetoken	Posture token name.
name	Name of the posture token.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Table 12 lists the interface types that may be used for the *interface-type* **argument**.

Table 12 Description of Interface Types

Interface Type	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	Code division multiple access Internet exchange (CDMA Ix) interface
CTunnel	Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface
Dialer	Dialer interface
Ethernet	IEEE 802.3 standard interface
Lex	Lex interface

Table 12 Description of Interface Types (continued)

Interface Type	Description
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink-group interface
Null	Null interface
Serial	Serial interface
Tunnel	Tunnel interface
Vif	Pragmatic General Multicast (PGM) Multicase Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following example shows that all client device entries are to be cleared:

```
Router# clear eou all
```

Related Commands

Command	Description
eou	Displays information about EAPoUDP.

clear ip admission cache

To clear IP admission cache entries from the router, use the **clear ip admission cache** command in privileged EXEC mode.

clear ip admission cache {* | host ip address}

Syntax Description

*****	Clears all IP admission cache entries and associated dynamic access lists.
host ip address	Clears all IP admission cache entries and associated dynamic access lists for the specified host.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use this command to clear entries from the admission control cache before they time out.

Examples

The following example shows that all admission entries are to be deleted:

```
Router# clear ip admission cache *
```

The following example shows that the authentication proxy entry for the host with the IP address 192.168.4.5 is to be deleted:

```
Router# clear ip admission cache 192.168.4.5
```

Related Commands

Command	Description
show ip admission cache	Displays the admission control entries or the running admission control configuration.

clear ip auth-proxy cache

To clear authentication proxy entries from the router, use the **clear ip auth-proxy cache** command in EXEC mode.

clear ip auth-proxy cache {***** | *host-ip-address*}

Syntax Description

*****	Clears all authentication proxy entries, including user profiles and dynamic access lists.
host-ip-address	Clears the authentication proxy entry, including user profiles and dynamic access lists, for the specified host.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use this command to clear entries from the translation table before they time out.

Examples

The following example deletes all authentication proxy entries:

```
clear ip auth-proxy cache *
```

The following example deletes the authentication proxy entry for the host with IP address 192.168.4.5:

```
clear ip auth-proxy cache 192.168.4.5
```

Related Commands

Command	Description
show ip auth-proxy	Displays the authentication proxy entries or the running authentication proxy configuration.

clear ip ips configuration

To disable Cisco IOS Firewall Intrusion Prevention System (IPS), remove all intrusion detection configuration entries, and release dynamic resources, use the **clear ip ips configuration** command in EXEC mode.

clear ip ips configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **clear ip audit configuration** command to the **clear ip ips configuration** command.

Examples

The following example clears the existing IPS configuration:

```
clear ip ips configuration
```

clear ip ips statistics

To reset statistics on packets analyzed and alarms sent, use the **clear ip ips statistics** command in EXEC mode.

clear ip ips statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **clear ip audit statistics** command to the **clear ip ips statistics** command.

Examples

The following example clears all IPS statistics:

clear ip ips statistics

clear ip sdee

To clear Security Device Event Exchange (SDEE) events or subscriptions, use the **clear ip sdee** command in privileged EXEC mode.

clear ip sdee {**events** | **subscriptions**}

Syntax Description

events	Clears SDEE events from the event buffer.
subscriptions	Clears SDEE subscriptions.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Because subscriptions are properly closed by the Cisco IOS Intrusion Prevention System (IPS) client, this command is typically used only to help with error recovery.

Examples

The following example shows how to clear all open SDEE subscriptions on the router:

```
Router# clear ip sdee subscriptions
```

Related Commands

Command	Description
ip ips notify	Specifies the method of event notification.
ip sdee events	Sets the maximum number of SDEE events that can be stored in the event buffer.
ip sdee subscriptions	Sets the maximum number of SDEE subscriptions that can be open simultaneously.

clear ip trigger-authentication

To clear the list of remote hosts for which automated double authentication has been attempted, use the **clear ip trigger-authentication** command in privileged EXEC mode.

clear ip trigger-authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command when troubleshooting automated double authentication. This command clears the entries in the list of remote hosts displayed by the **show ip trigger-authentication** command.

Examples

The following example clears the remote host table:

```
Router# show ip trigger-authentication

Trigger-authentication Host Table:
Remote Host          Time Stamp
172.21.127.114       2940514234
Router# clear ip trigger-authentication
Router# show ip trigger-authentication
```

Related Commands

Command	Description
show ip trigger-authentication	Displays the list of remote hosts for which automated double authentication has been attempted.

clear ip urlfilter cache

To clear the cache table, use the **clear ip urlfilter cache** command in EXEC mode.

clear ip urlfilter cache {*ip-address* | **all**}

Syntax Description

ip-address	Clears the cache table of a specified server IP address.
all	Clears the cache table completely.

Command Modes

EXEC

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

The cache table consists of the most recently requested IP addresses and the respective authorization status for each IP address.

Examples

The following example shows how to clear the cache table of IP address 172.18.139.21:

```
clear ip urlfilter cache 172.18.139.21
```

The following example shows how to clear the cache table of all IP addresses:

```
clear ip urlfilter cache all
```

Related Commands

Command	Description
ip urlfilter cache	Configures cache parameters.
show ip urlfilter cache	Displays the destination IP addresses that are cached into the cache table.

clear kerberos creds

To delete the contents of the credentials cache, use the **clear kerberos creds** command in privileged EXEC mode.

clear kerberos creds

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Credentials are deleted when this command is issued.

Cisco supports Kerberos 5.

Examples

The following example illustrates the **clear kerberos creds** command:

```
Router# show kerberos creds
Default Principal: chet@cisco.com
Valid Starting          Expires                 Service Principal
18-Dec-1995 16:21:07    19-Dec-1995 00:22:24    krbtgt/CISCO.COM@CISCO.COM

Router# clear kerberos creds
Router# show kerberos creds
No Kerberos credentials.
```

Related Commands

Command	Description
show kerberos creds	Displays the contents of your credentials cache.

clear radius local-server

To clear the display on the local server or to unblock a locked username, use the **clear radius local-server** command in privileged EXEC mode.

clear radius local-server {statistics | user *username*}

Syntax Description

statistics	Clears the display of statistical information.
user	Unblocks the locked username specified.
username	Locked username.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following example unblocks the locked username “smith”:

```
Router# clear radius local-server user smith
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.

Command	Description
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

clid

To preauthenticate calls on the basis of the Calling Line Identification (CLID) number, use the **clid** command in AAA preauthentication configuration mode. To remove the **clid** command from your configuration, use the **no** form of this command.

clid [**if-avail** | **required**] [**accept-stop**] [**password** *password*]

no clid [**if-avail** | **required**] [**accept-stop**] [**password** *password*]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as **ctype** or **dnis** from being tried once preauthentication has succeeded for a call element.
password *password*	(Optional) Defines the password for the preauthentication element.

Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the authentication, authorization and accounting (AAA) preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the CLID number:

```
aaa preauth
```

```
group radius
clid required
```

Related Commands

Command	Description
ctype	Preauthenticates calls on the basis of the call type.
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (RADIUS)	Specifies the AAA RADIUS server group to use for preauthentication.

client authentication list

To configure Internet Key Exchange (IKE) extended authentication (Xauth) in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client authentication list** command in ISAKMP profile configuration mode. To restore the default behavior, which is that Xauth is not enabled, use the **no** form of this command.

client authentication list *list-name*

no client authentication list *list-name*

Syntax Description

list-name	Character string used to name the list of authentication methods activated when a user logs in. The list name must match the list name that was defined during the authentication, authorization, and accounting (AAA) configuration.

Defaults

No default behaviors or values

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Before configuring Xauth, you must set up an authentication list using AAA commands.

Examples

The following example shows that user authentication is configured. User authentication is a list of authentication methods called “xauthlist” in an ISAKMP profile called “vpnprofile.”

```
crypto isakmp profile vpnprofile
 client authentication list xauthlist
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.

client configuration address

To configure Internet Key Exchange (IKE) configuration mode in the Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client configuration address** command in ISAKMP profile configuration mode. To disable IKE configuraton mode, use the **no** form of this command.

client configuration address {**initiate** | **respond**}

no client configuration address {**initiate** | **respond**}

Syntax Description

initiate	Router will attempt to set IP addresses for each peer.
respond	Router will accept requests for IP addresses from any requesting peer.

Defaults

IKE configuration is not enabled.

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Before you can use this command, you must enter the **crypto isakmp profile** command.

Examples

The following example shows that IKE mode is configured to either initiate or respond in an ISAKMP profile called “vpnprofile”:

```
crypto isakmp profile vpnprofile
 client configuration address initiate
 client configuration address respond
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile.

client configuration group

To associate a group with the peer that has been assigned an Internet Security Association Key Management Protocol (ISAKMP) profile, use the **client configuration group** command in crypto ISAKMP profile configuration mode. To disable this option, use the **no** form of this command.

client configuration group *group-name*

no client configuration group *group-name*

Syntax Description

group-name	Name of the group to be associated with the peer.

Defaults

No default behavior or values

Command Modes

Crypto ISAKMP profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **client configuration group** command is used after the crypto map has been configured and the ISAKMP profiles have been assigned to them.

Examples

The following example shows that the group “some_group” is to be associated with the peer:

```
crypto isakmp profile id_profile
   ca trust-point 2315
   match identity host domain cisco.com
   client configuration group some_group
```

Related Commands

Command	Description
match certificate (ISAKMP)	Assigns an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate.

commands (view)

To add commands or an interface to a command-line interface (CLI) view, use the **commands** command in view configuration mode. To delete a command or an interface from a CLI view, use the **no** form of this command.

Syntax for Adding and Deleting Commands to a View

commands *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [*command*]

no commands *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [*command*]

Syntax for Adding and Deleting Interfaces to a View

commands *parser-mode* {**include** | **include-exclusive**} [**all**] [**interface** *interface-name*] [*command*]

no commands *parser-mode* {**include** | **include-exclusive**} [**all**] [**interface** *interface-name*] [*command*]

Syntax Description

parser-mode	Mode in which the specified command exists. See Table 13 in the "Usage Guidelines" section for a list of available options for this argument.
include	Adds a specified command or a specified interface to the view and allows the same command or interface to be added to an additional view.
include-exclusive	Adds a specified command or a specified interface to the view and excludes the same command or interface from being added to all other views.
exclude	Denies access to commands in the specified parser mode. **Note** This keyword is available only for command-based views.
all	(Optional) A "wildcard" that allows every command in a specified configuration mode that begins with the same keyword or every subinterface within a specified interface to be part of the view.
interface *interface-name*	(Optional) Interface that is added to the view.
command	(Optional) Command that is added to the view. **Note** If no commands are specified, all commands within the specified parser mode are included or excluded, as appropriate.

Defaults

If this command is not enabled, a view will not have adequate information to deny or allow access to users.

Command Modes

View configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	The **exclude** keyword and the **interface** *interface-name* option were added.

Usage Guidelines

If a network administrator does not enter a specific command (via the *command* argument) or interface (via the **interface** *interface-name* option), users are granted access (via the **include** or **include-exclusive** keywords) or denied access (via the **exclude** keyword) to all commands within the specified parser-mode.

parser-mode Options

Table 13 shows some of the keyword options for the *parser-mode* argument in the **commands** command. The available mode keywords vary depending on your hardware and software version. To see a list of available mode options on your system, use the **commands ?** command.

Table 13 Parser -Mode Options

Command	Description
accept-dialin	VPDN group accept dialin configuration mode
accept-dialout	VPDN group accept dialout configuration mode
address-family	Address Family configuration mode
alps-ascu	ALPS ASCU configuration mode
alps-circuit	ALPS circuit configuration mode
atm-bm-config	ATM bundle member configuration mode
atm-bundle-config	ATM bundle configuration mode
atm-vc-config	ATM virtual circuit configuration mode
atmsig_e164_table_mode	ATMSIG E164 Table
cascustom	Channel-associated signalling (cas) custom configuration mode
config-rtr-http	RTR HTTP raw request Configuration
configure	Global configuration mode
controller	Controller configuration mode
crypto-map	Crypto map config mode
crypto-transform	Crypto transform config modeCrypto transform configuration mode
dhcp	DHCP pool configuration mode
dspfarm	DSP farm configuration mode
exec	EXEC mode
flow-cache	Flow aggregation cache configuration mode
gateway	Gateway configuration mode
interface	Interface configuration mode
interface-dlci	Frame Relay DLCI configuration mode
ipenacl	IP named extended access-list configuration mode
ipsnacl	IP named simple access-list configuration mode
ip-vrf	Configure IP VRF parameters
lane	ATM Lan Emulation Lecs Configuration Table
line	Line configuration mode

Table 13 Parser -Mode Options

Command	Description
map-class	Map class configuration mode
map-list	Map list configuration mode
mpoa-client	MPOA Client
mpoa-server	MPOA Server
null-interface	Null interface configuration mode
preaut	AAA Preauth definitions
request-dialin	VPDN group request dialin configuration mode
request-dialout	VPDN group request dialout configuration mode
route-map	Route map configuration mode
router	Router configuration mode
rsvp_policy_local	RSVP local policy configuration mode
rtr	RTR Entry Configuration
sg-radius	RADIUS server group definition
sg-tacacs+	TACACS+ server group
sip-ua	SIP UA configuration mode
subscriber-policy	Subscriber policy configuration mode
tcl	Tcl mode
tdm-conn	TDM connection configuration mode
template	Template configuration mode
translation-rule	Translation Rule configuration mode
vc-class	VC class configuration mode
voiceclass	Voice Class configuration mode
voiceport	Voice configuration mode
voipdialpeer	Dial Peer configuration mode
vpdn-group	VPDN group configuration mode

Examples

The following example shows how to add the privileged EXEC command **show version** to both CLI views “first” and “second.” Because the **include** keyword was issued, the **show version** command can be added to both views.

```
Router(config)# parser view first
Router(config-view)# password 5 secret
Router(config-view)# commands exec include show version
!
Router(config)# parser view second
Router(config-view)# password 5 myview
Router(config-view)# commands exec include show version
```

The following example shows how to allow users in the view “first” to execute all commands that start with the word “show” except the **show interfaces** command, which is excluded by the view “second”:

```
Router(config)# parser view first
```

```
Router(config-view)# password 5 secret
Router(config-view)# commands exec include all show
!
Router(config)# parser view second
Router(config-view)# password 5 myview
Router(config-view)# commands exec include-exclusive show interfaces
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.
password 5	Associates a CLI view or a superview with a password.

copy ips-sdf

To load or save the signature definition file (SDF) in the router, use the **copy ips-sdf** command in EXEC mode.

Syntax for Loading the SDF

copy [**/erase**] *url* **ips-sdf**

Syntax for Saving the SDF

copy ips-sdf *url*

Syntax Description

/erase	(Optional) Erases the current SDF in the router before loading the new SDF. **Note** This option is typically available only on platforms with limited memory.
url	Description for the *url* argument is one of the following options: • If you want to load the SDF in the router, the *url* argument specifies the location in which to search for the SDF. • If you are saving the SDF, the *url* argument represents the location in which the SDF is saved after it has been generated. Regardless of what option the URL is used for, available URL locations are as follows: • local flash, such as flash:sig.xml • FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml • rcp, such as rcp://myuser@rcp_server/sig.xml • TFTP server, such as tftp://tftp_server/sig.xml

Command Modes

EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Loading Signatures From the SDF

Issue the **copy** *url* **ips-sdf** command to load the SDF in the router from the location specified via the *url* argument. When the new SDF is loaded, it is merged with the SDF that is already loaded in the router, unless the **/erase** keyword is issued, which overwrites the current SDF with the new SDF.

Cisco IOS Intrusion Prevention System (IPS) will attempt to retrieve the SDF from each specified location in the order in which they were configured in the startup configuration. If Cisco IOS IPS cannot retrieve the signatures from any of the specified locations, the built-in signatures will be used.

If the **no ip ips sdf built-in** command is used, Cisco IOS IPS will fail to load. IPS will then rely on the configuration of the **ip ips fail** command to either fail open or fail closed.

Note For Cisco IOS Release 12.3(8)T, the SDF should be loaded directly from Flash.

After the signatures are loaded in the router, the signature engines are built. Only after the signature engines are built can Cisco IOS IPS beginning scanning traffic.

Note Whenever signatures are replaced or merged, the router is suspended while the signature engines for the newly added or merged signatures are being built. The router prompt will be available again after the engines are built.

Depending on your platform and how many signatures are being loaded, building the engine can take up to several minutes. It is recommended that you enable logging messages to monitor the engine building status.

The **ip sdf ips location** command can also be used to load the SDF. However, unlike the **copy ips-sdf** command, this command does not force and immediately load the signatures. Signatures are not loaded until the router reboots or IPS is initially applied to an interface (via the **ip ips** command).

Saving a Generated or Merges SDF

Issue the **copy ips-sdf** *url* command to save a newly created SDF file to a specified location. The next time the router is reloaded, IPS can refer to the SDF from the saved location by including the **ip ips sdf location** command in the configuration.

Tip It is recommended that you save the SDF back out to Flash. Also, you should save the file to a different name than the original attack-drop.sdf file; otherwise, you risk loosing the original file.

Examples

The following example shows how to configure the router to load and merge the attack-drop.sdf file with the default signatures. After you have merged the two files, it is recommended to copy the newly merged signatures to a separate file. The router can then be reloaded (via the **reload** command) or reinitalized to so as to recognize the newly merged file (as shown the following example)

```
!
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
!
! Merge the flash-based SDF (attack-drop.sdf) with the built-in signatures.
copy disk2:attack-drop.sdf ips-sdf
! Save the newly merged signatures to a separate file.
copy ips-sdf disk2:my-signatures.sdf
!
! Configure the router to use the new file, my-signatures.sdf
```

```
configure terminal
ip ips sdf location disk2:my-signatures.sdf
! Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.
interface gig 0/1
 no ip ips MYIPS in
!
*Apr 8 14:05:38.243:%IPS-2-DISABLED:IPS removed from all interfaces - IPS disabled
!
 ip ips MYIPS in
!
exit
```

Related Commands

Command	Description
ip ips sdf location	Specifies the location in which the router should load the SDF.

crl

To query the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked, use the **crl** command in ca-trustpoint configuration mode. To return to the default behavior in which the router will check the URL that is embedded in the certificate, use the **no** form of this command.

crl query *url*

no crl query *url*

Syntax Description

query url	The Lightweight Directory Access Protocol (LDAP) URL published by the certification authority (CA) server is specified to query the CRL; for example, ldap://another_server.

Defaults

If the **query** *url* option is not enabled, the router will check the CRL distribution point (CDP) that is embedded in the certificate. The **query** *url* option does not need to be configured if the CDP that is in the certificate is formatted as a URL (for example, http:// url or ldap:// url), including the fully qualified domain name (FQDN) of the host where the CRL is held.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(2)T	The **optional** and **best-effort** keywords were replaced by the **revocation-check** command.

Usage Guidelines

Use the **query** url option if the CDP is in LDAP form, which means that the CDP location in the certificate will indicate only where the CDP is located in the directory; that is, the CDP will not indicate the actual query location for the directory.

Note The **optional** and **best-effort** keywords have been replaced by the **revocation-check** command. If you enter the **crl optional** command, it will be written back as the **revocation-check none** command; if you enter the **crl best-effort** command, it will be written back as the **revocation-check crl none** command.

Note The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to configure your router to query the CRL with the LDAP URL that is published by the CA named “bar”:

```
crypto ca trustpoint bar
 enrollment url http://bar.cisco.com
 crl query ldap://bar.cisco.com
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
revocation-check	Checks the revocation status of a certificate.

crl optional

The **crl optional** command is replaced by the **crl** command. See the **crl** command for more information.

crl query

The **crl query** command is replaced by the **crl** command. See the **crl** command for more information.

crypto ca authenticate

Note This command was replaced by the **crypto pki authenticate** command effective with Cisco IOS Release 12.3(7)T.

To authenticate the certification authority (by getting the certificate of the CA), use the **crypto ca authenticate** command in global configuration mode.

crypto ca authenticate *name*

Syntax Description

name	Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command is required when you initially configure CA support at your router.

This command authenticates the CA to your router by obtaining the self-signed certificate of the CA that contains the public key of the CA. Because the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator when you perform this command.

If you are using RA mode (using the **enrollment mode ra** command) when you issue the **crypto ca authenticate** command, then registration authority signing and encryption certificates will be returned from the CA as well as the CA certificate.

This command is not saved to the router configuration. However. the public keys embedded in the received CA (and RA) certificates are saved to the configuration as part of the RSA public key record (called the "RSA public key chain").

Note If the CA does not respond by a timeout period after this command is issued, the terminal control will be returned so it will not be tied up. If this happens, you must re-enter the command. Cisco IOS software will not recognize CA certificate expiration dates set for beyond the year 2049. If the validity period of the CA certificate is set to expire after the year 2049, the following error message will be displayed when authentication with the CA server is attempted:

```
error retrieving certificate :incomplete chain
```

If you receive an error message similar to this one, check the expiration date of your CA certificate. If the expiration date of your CA certificate is set after the year 2049, you must reduce the expiration date by a year or more.

Examples

In the following example, the router requests the certificate of the CA. The CA sends its certificate and the router prompts the administrator to verify the certificate of the CA by checking the CA certificate's fingerprint. The CA administrator can also view the CA certificate's fingerprint, so you should compare what the CA administrator sees to what the router displays on the screen. If the fingerprint on the router's screen matches the fingerprint viewed by the CA administrator, you should accept the certificate as valid.

```
Router(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
```

Related Commands

Command	Description
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
show crypto pki certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto ca cert validate

Note This command was replaced by the **crypto pki cert validate** command effective with Cisco IOS Release 12.3(8)T.

To determine if a trustpoint has been successfully authenticated, a certificate has been requested and granted, and if the certificate is currently valid, use the **crypto ca cert validate** command in global configuration mode.

crypto ca cert validate *trustpoint*

Syntax Description

trustpoint	The trustpoint to be validated.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **crypto ca cert validate** command validates the router's own certificate for a given trustpoint. Use this command as a sanity check after enrollment to verify that the trustpoint is properly authenticated, a certificate has been requested and granted for the trustpoint, and that the certificate is currently valid. A certificate is valid if it is signed by the trustpoint certification authority (CA), not expired, and so on.

Examples

The following examples show the possible output from the **crypto ca cert validate** command:

```
Router(config)# crypto ca cert validate ka

Validation Failed: trustpoint not found for ka


Router(config)# crypto ca cert validate ka

Validation Failed: can't get local certificate chain


Router(config)# crypto ca cert validate ka

Certificate chain has 2 certificates.
Certificate chain for ka is valid


Router(config)# crypto ca cert validate ka
```

```
Certificate chain has 2 certificates.
Validation Error: no certs on chain


Router(config)# crypto ca cert validate ka

Certificate chain has 2 certificates.
Validation Error: unspecified error
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the certification authority that the router should use.
show crypto pki trustpoints	Displays the trustpoints that are configured in the router.

crypto ca certificate chain

Note This command was replaced by the **crypto pki certificate chain** command effective with Cisco IOS Release 12.3(7)T.

To enter the certificate chain configuration mode, use the **crypto ca certificate chain** command in global configuration mode. (You need to be in certificate chain configuration mode to delete certificates.)

crypto ca certificate chain *name*

Syntax Description

name	Specifies the name of the CA. Use the same name as when you declared the CA using the **crypto pki trustpoint** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command puts you into certificate chain configuration mode. When you are in certificate chain configuration mode, you can delete certificates using the **certificate** command.

Examples

The following example deletes the router's certificate. In this example, the router had a general-purpose RSA key pair with one corresponding certificate. The show command is used to determine the serial number of the certificate to be deleted.

```
Router# show crypto ca certificates

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set

Router# configure terminal
Rrouter(config)# crypto ca certificate chain myca
Router(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
```

```
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
Router(config-cert-chain)# exit
```

Related Commands

Command	Description
certificate	Adds certificates manually.

crypto ca certificate map

Note This command was replaced by the **crypto pki certificate map** command effective with Cisco IOS Release 12.3(7)T.

To define certificate-based access control lists (ACLs), use the **crypto ca certificate map** command in ca-certificate-map configuration mode. To remove the certificate-based ACLs, use the **no** form of this command.

crypto ca certificate map *label sequence-number*

no crypto ca certificate map *label sequence-number*

Syntax Description

label	A user-specified label that is referenced within the **crypto ca trustpoint** command.
sequence-number	A number that orders the ACLs with the same label. ACLs with the same label are processed from lowest to highest sequence number. When an ACL is matched, processing stops with a successful result.

Defaults

No default behavior or value.

Command Modes

Ca-certificate-map configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Issuing this command places the router in CA certificate map configuration mode where you can specify several certificate fields together with their matching criteria. The general form of these fields is as follows:

```
field-name match-criteria match-value
```

The *field-name* in the above example is one of the certificate fields. Field names are similar to the names used in the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) X.509 standard. The **name** field is a special field that matches any subject name or related name field in the certificate, such as the **alt-subject-name, subject-name**, and **unstructured-subject-name** fields.

- **alt-subject-name**—Case-insensitive string.
- **expires-on**—Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.
- **issuer-name**—Case-insensitive string.
- **name**—Case-insensitive string.
- **subject-name**—Case-insensitive string.

- **unstructured-subject-name**—Case-insensitive string.
- **valid-start**—Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.

Note The time portion is optional in both the **expires-on** date and **valid-start** field and defaults to 00:00:00 if not specified. The time is interpreted according to the time zone offset configured for the router. The string **utc** can be appended to the date and time when they are configured as Universal Time, Coordinated (UTC) rather than local time.

The *match-criteria* in the example is one of the following logical operators:

- **eq**—equal (valid for name and date fields)
- **ne**—not equal (valid for name and date fields)
- **co**—contains (valid only for name fields)
- **nc**—does not contain (valid only for name fields)
- **lt**—less than (valid only for date fields)
- **ge**—greater than or equal to (valid only for date fields)

The *match-value* is a case-insensitive string or a date.

Examples

The following example shows how to configure a certificate-based ACL that will allow any certificate issued by Cisco Systems to an entity within the cisco.com domain. The label is Cisco, and the sequence is 10.

```
crypto ca certificate map Cisco 10
 issuer-name co Cisco Systems
 unstructured-subject-name co cisco.com
```

The following example accepts any certificate issued by Cisco Systems for an entity with DIAL or organizationUnit component ou=WAN. This certificate-based ACL consists of two separate ACLs tied together with the common label Group. Because the check for DIAL has a lower sequence number, it is performed first. Note that the string “DIAL” can occur anywhere in the subjectName field of the certificate, but the string WAN must be in the organizationUnit component.

```
crypto ca certificate map Group 10
 issuer-name co Cisco Systems
 subject-name co DIAL
crypto ca certificate map Group 20
 issuer-name co Cisco Systems
 subject-name co ou=WAN
```

Case is ignored in string comparisons; therefore, DIAL in the previous example will match dial, DIAL, Dial, and so on. Also note that the component identifiers (o=, ou=, cn=, and so on) are not required unless it is desirable that the string to be matched occurs in a specific component of the name. (Refer to the ITU-T security standards for more information about certificate fields and components such as ou=.)

If a component identifier is specified in the match string, the exact string, including the component identifier, must appear in the certificate. This requirement can present a problem if more than one component identifier is included in the match string. For example, “ou=WAN,o=Cisco Systems” will not match a certificate with the string “ou=WAN,ou=Engineering,o=Cisco Systems” because the “ou=Engineering” string separates the two desired component identifiers.

To match both “ou=WAN” and “o=Cisco Systems” in a certificate while ignoring other component identifiers, you could use this certificate map:

```
crypto ca certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
```

Any space character proceeding or following the equal sign (=) character in component identifiers is ignored. Therefore “o=Cisco” in the proceeding example will match “o = Cisco,” “o= Cisco,” “o =Cisco,” and so on.

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

crypto ca certificate query (ca-trustpoint)

Note This command was replaced by the **crypto pki certificate query (ca-trustpoint)** command effective with Cisco IOS Release 12.3(7)T.

To specify that certificates should not be stored locally but retrieved from a certification authority (CA) trustpoint, use the **crypto ca certificate query** command in ca-trustpoint configuration mode. To cause certificates to be stored locally per trustpoint, use the **no** form of this command.

crypto ca certificate query

no crypto ca certificate query

Syntax Description

This command has no arguments or keywords.

Defaults

CA trustpoints are stored locally in the router's NVRAM.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Normally, certain certificates are stored locally in the router's NVRAM, and each certificate uses a moderate amount of memory. To save NVRAM space, you can use this command to put the router into query mode, preventing certificates from being stored locally; instead, they are retrieved from a specified CA trustpoint when needed. This will save NVRAM space but could result in a slight performance impact.

The **crypto ca certificate query** command is a subcommand for each trustpoint; thus, this command can be disabled on a per-trustpoint basis.

Before you can configure this command, you must enable the **crypto pki trustpoint** command, which puts you in ca-trustpoint configuration mode.

Note This command replaces the **crypto ca certificate query** command in global configuration mode. Although you can still enter the global configuration command, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to prevent certificates and certificate revocation lists (CRLs) from being stored locally on the router; instead, they are retrieved from the "ka" trustpoint when needed.

```
crypto ca trustpoint ka
```

```
.
.
.
crypto ca certificate query
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

crypto ca certificate query (global)

The **crypto ca certificate query** command in global configuration mode is replaced by the **crypto ca certificate query** command in ca-trustpoint configuration mode. See the **crypto ca certificate query** command for more information.

crypto ca crl request

Note This command was replaced by the **crypto pki crl request** command effective with Cisco IOS Release 12.3(7)T.

To request that a new certificate revocation list (CRL) be obtained immediately from the certification authority, use the **crypto ca crl request** command in global configuration mode.

crypto ca crl request *name*

Syntax Description

name	Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto pki trustpoint** command.

Defaults

Normally, the router requests a new CRL only after the existing one expires.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

A CRL lists all the network's devices' certificates that have been revoked. Revoked certificates will not be honored by your router; therefore, any IPSec device with a revoked certificate cannot exchange IP Security traffic with your router.

The first time your router receives a certificate from a peer, it will download a CRL from the CA. Your router then checks the CRL to make sure the peer's certificate has not been revoked. (If the certificate appears on the CRL, it will not accept the certificate and will not authenticate the peer.)

A CRL can be reused with subsequent certificates until the CRL expires. If your router receives a peer's certificate after the applicable CRL has expired, it will download the new CRL.

If your router has a CRL which has not yet expired, but you suspect that the CRL's contents are out of date, use the **crypto ca crl request** command to request that the latest CRL be immediately downloaded to replace the old CRL.

This command is not saved to the configuration.

Examples

The following example immediately downloads the latest CRL to your router:

```
crypto ca crl request
```

crypto ca enroll

Note This command was replaced by the **crypto pki enroll** command effective with Cisco IOS Release 12.3(7)T.

To obtain the certificate(s) of your router from the certification authority, use the **crypto ca enroll** command in global configuration mode. To delete a current enrollment request, use the **no** form of this command.

crypto ca enroll *name*

no crypto ca enroll *name*

Syntax Description

name	Specifies the name of the CA. Use the same name as when you declared the CA using the **crypto pki trustpoint** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command requests certificates from the CA for all of your router's RSA key pairs. This task is also known as enrolling with the CA. (Technically, enrolling and obtaining certificates are two separate events, but they both occur when this command is issued.)

Your router needs a signed certificate from the CA for each RSA key pairs of your router; if you previously generated general purpose keys, this command will obtain the one certificate corresponding to the one general purpose RSA key pair. If you previously generated special usage keys, this command will obtain two certificates corresponding to each of the special usage RSA key pairs.

If you already have a certificate for your keys you will be unable to complete this command; instead, you will be prompted to remove the existing certificate first. (You can remove existing certificates with the **no certificate** command.)

The **crypto ca enroll** command is not saved in the router configuration.

Note If your router reboots after you issue the **crypto ca enroll** command but before you receive the certificate(s), you must reissue the command.

Responding to Prompts

When you issue the **crypto ca enroll** command, you are prompted a number of times.

First, you are prompted to create a challenge password. This password can be up to 80 characters in length. This password is necessary in the event that you ever need to revoke your router's certificate(s). When you ask the CA administrator to revoke your certificate, you must supply this challenge password as a protection against fraudulent or mistaken revocation requests.

Note This password is not stored anywhere, so you need to remember this password.

If you lose the password, the CA administrator may still be able to revoke the router's certificate but will require further manual authentication of the router administrator identity.

You are also prompted to indicate whether or not your router's serial number should be included in the obtained certificate. The serial number is not used by IP Security or Internet Key Exchange but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular router. (Note that the serial number stored is the serial number of the internal board, not the one on the enclosure.) Ask your CA administrator if serial numbers should be included. If you are in doubt, include the serial number.

Normally, you would not include the IP address because the IP address binds the certificate more tightly to a specific entity. Also, if the router is moved, you would need to issue a new certificate. Finally, a router has multiple IP addresses, any of which might be used with IPSec.

If you indicate that the IP address should be included, you will then be prompted to specify the interface of the IP address. This interface should correspond to the interface that you apply your crypto map set to. If you apply crypto map sets to more than one interface, specify the interface that you name in the **crypto map local-address** command.

Examples

In the following example, a router with a general-purpose RSA key pair requests a certificate from the CA. When the router displays the certificate fingerprint, the administrator verifies this number by calling the CA administrator, who checks the number. The fingerprint is correct, so the router administrator accepts the certificate.

There can be a delay between when the router administrator sends the request and when the certificate is actually received by the router. The amount of delay depends on the CA method of operation.

```
Router(config)# crypto ca enroll myca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: <mypassword>
Re-enter password: <mypassword>

% The subject name in the certificate will be: myrouter.example.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 03433678
% Include an IP address in the subject name [yes/no]? yes
Interface: ethernet0/0
Request certificate from CA [yes/no]? yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificates' command will also show the fingerprint.
```

Some time later, the router receives the certificate from the CA and displays the following confirmation message:

```
Router(config)#   Fingerprint: 01234567 89ABCDEF FEDCBA98 75543210

%CRYPTO-6-CERTRET: Certificate received from Certificate Authority

Router(config)#
```

If necessary, the router administrator can verify the displayed Fingerprint with the CA administrator.

If there is a problem with the certificate request and the certificate is not granted, the following message is displayed on the console instead:

```
%CRYPTO-6-CERTREJ: Certificate enrollment request was rejected by Certificate Authority
```

The subject name in the certificate is automatically assigned to be the same as the RSA key pair's name. In the above example, the RSA key pair was named "myrouter.example.com." (The router assigned this name.)

Requesting certificates for a router with special usage keys would be the same as the previous example, except that two certificates would have been returned by the CA. When the router received the two certificates, the router would have displayed the same confirmation message:

```
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
```

Related Commands

Command	Description
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the router.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
show crypto pki certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto ca export pem

Note This command was replaced by the **crypto pki export pem** command effective with Cisco IOS Release 12.3(7)T.

To export certificates and Rivest, Shamir, and Adelman (RSA) keys that are associated with a trustpoint in a privacy-enhanced mail (PEM)-formatted file, use the **crypto ca export pem** command in global configuration mode.

crypto ca export *trustpoint* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase*

Syntax Description

trustpoint	Name of the trustpoint that the associated certificate and RSA key pair will export. The *trustpoint* argument must match the name that was specified via the **crypto pki trustpoint** command.
terminal	Certificate and RSA key pair that will be displayed in PEM format on the console terminal.
url *url*	URL of the file system where your router should export the certificate and RSA key pairs.
3des	Export the trustpoint using the Triple Data Encryption Standard (3DES) encryption algorithm.
des	Export the trustpoint using the DES encryption algorithm.
passphrase	Passphrase that is used to encrypt the PEM file for import. **Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **crypto ca export pem** command allows you to export certificate and RSA key pairs in PEM-formatted files. The PEM files can then be imported back into the Cisco IOS router (via the **crypto pki import pem** command) or other public key infrastructure (PKI) applications.

Examples

The following example shows how to generate and export the RSA key pair "aaa" and certificates of the router in PEM files that are associated with the trustpoint "mycs":

```
Router(config)# crypto key generate rsa general-keys label aaa exportable
The name for the keys will be:aaa
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
!
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
!
Router(config)# crypto pki trustpoint mycs
Router(ca-trustpoint)# enrollment url http://mycs
Router(ca-trustpoint)# rsakeypair aaa
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate mycs
Certificate has the following attributes:
Fingerprint:C21514AC 12815946 09F635ED FBB6CF31
% Do you accept this certificate? [yes/no]:y
Trustpoint CA certificate accepted.
!
Router(config)# crypto pki enroll mycs
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The fully-qualified domain name in the certificate will be:Router
% The subject name in the certificate will be:bizarro.cisco.com
% Include the router serial number in the subject name? [yes/no]:n
% Include an IP address in the subject name? [no]:n
Request certificate from CA? [yes/no]:y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

Router(config)# Fingerprint: 8DA777BC 08477073 A5BE2403 812DD157

00:29:11:%CRYPTO-6-CERTRET:Certificate received from Certificate Authority

Router(config)# crypto ca export aaa pem terminal 3des cisco123

% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAa2gAwIBAgIBATANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJVUzES
<snip>
waDeNOSI3WlDa0AWq5DkVBkxwgn0TqIJXJOCttjHnWHK1LMcMVGn
-----END CERTIFICATE-----

% Key name:aaa
    Usage:General Purpose Key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type:4,ENCRYPTED
DEK-Info:DES-EDE3-CBC,ED6B210B626BC81A

Urguv0jnjwOgowWVUQ2XR5nbzzYHI2vGLunpH/IxIsJuNjRVjbAAUpGk7VnPCT87
<snip>
kLCOtxzEv7JHc72gMku9uUlrLSnFH5slzAtoC0czfU4=
```

```
-----END RSA PRIVATE KEY-----

% Certificate:
-----BEGIN CERTIFICATE-----
MIICTjCCAfigAwIBAgICIQUwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
<snip>
6xlBaIsuMxnHmr89KkKkYlU6
-----END CERTIFICATE-----
```

Related Commands

Command	Description
crypto pki import pem	Imports certificates and RSA keys to a trustpoint from PEM-formatted files.
crypto pki trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of a CA.

crypto ca export pkcs12

Note This command was replaced by the **crypto pki export pkcs12** command effective with Cisco IOS Release 12.3(7)T.

To export Rivest, Shamir, and Adelman (RSA) keys within a PKCS12 file at a specified location, use the **crypto ca export pkcs12** command in global configuration mode.

crypto ca export *trustpointname* **pkcs12** *destination url passphrase*

Syntax Description

trustpointname	Name of the trustpoint who issues the certificate that a user is going to export. When you export the PKCS12 file, the trustpoint name is the RSA key name.
destination url	Location of the PKCS12 file to which a user wants to import the RSA key pair.
passphrase	Passphrase that is used to encrypt the PKCS12 file for export.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The **crypto ca export pkcs12** command creates a PKCS 12 file that contains an RSA key pair. The PKCS12 file, along with a certificate authority (CA), is exported to the location that you specify with the destination URL. If you decide not to import the file to another router, you must delete the file.

Security Measures

Keep the PKCS12 file stored in a secure place with restricted access.

An RSA keypair is more secure than a passphrase because the private key in the key pair is not known by multiple parties. When you export an RSA key pair to a PKCS#12 file, the RSA key pair now is only as secure as the passphrase.

To create a good passphrase, be sure to include numbers, as well as both lowercase and uppercase letters. Avoid publicizing the passphrase by mentioning it in e-mail or cell phone communications because the information could be accessed by an unauthorized user.

Examples

The following example exports an RSA key pair with a trustpoint name “mytp” to a Flash file:

```
Router(config)# crypto ca export mytp pkcs12 flash:myexport mycompany
```

Related Commands

Command	Description
crypto pki import pkcs12	Imports RSA keys.

crypto ca identity

The **crypto ca identity** command is replaced by the **crypto ca trustpoint** command. See the **crypto ca trustpoint** command for more information.

crypto ca import

Note This command was replaced by the **crypto pki import** command effective with Cisco IOS Release 12.3(7)T.

To import a certificate manually via TFTP or as a cut-and-paste at the terminal, use the **crypto ca import** command in global configuration mode.

crypto ca import *name* **certificate**

Syntax Description

name **certificate**	Name of the certification authority (CA). This name is the same name used when the CA was declared with the **crypto pki trustpoint** command.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

You must enter the **crypto ca import** command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.)

Examples

The following example shows how to import a certificate via cut-and-paste. In this example, the CA trustpoint is "MS."

```
crypto pki trustpoint MS
 enroll terminal
 crypto pki authenticate MS
!
crypto pki enroll MS
crypto ca import MS certificate
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of your CA.
enrollment terminal	Specifies manual cut-and-paste certificate enrollment.

crypto ca import pem

Note This command was replaced by the **crypto pki import pem** command effective with Cisco IOS Release 12.3(7)T.

To import certificates and Rivest, Shamir, and Adelman (RSA) keys to a trustpoint from privacy-enhanced mail (PEM)-formatted files, use the **crypto ca import pem** command in global configuration mode.

crypto ca import *trustpoint* **pem** [**usage-keys**] {**terminal** | **url** *url*} [**exportable**] *passphrase*

Syntax Description

trustpoint	Name of the trustpoint that is associated with the imported certificates and RSA key pairs. The *trustpoint* argument must match the name that was specified via the **crypto pki trustpoint** command.
usage-keys	(Optional) Specifies that two RSA special usage key pairs will be imported (that is, one encryption pair and one signature pair), instead of one general-purpose key pair.
terminal	Certificates and RSA key pairs will be manually imported from the console terminal.
url *url*	URL of the file system where your router should import the certificates and RSA key pairs.
exportable	(Optional) Specifies that the imported RSA key pair can be exported again to another Cisco device such as a router.
passphrase	Passphrase that is used to encrypt the PEM file for import. **Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **crypto ca import pem** command allows you import certificates and RSA key pairs in PEM-formatted files. The files can be previously exported from another router or generated from other public key infrastructure (PKI) applications.

Examples

The following example shows how to import PEM files to trustpoint "ggg" via TFTP:

```
Router(config)# crypto ca import ggg pem url tftp://10.1.1.2/johndoe/msca cisco1234

% Importing CA certificate...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.ca]?
Reading file from tftp://10.1.1.2/johndoe/msca.ca
Loading johndoe/msca.ca from 10.1.1.2 (via Ethernet0):!
[OK - 1082 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.prv]?
Reading file from tftp://10.1.1.2/johndoe/msca.prv
Loading johndoe/msca.prv from 10.1.1.2 (via Ethernet0):!
[OK - 573 bytes]

% Importing  certificate PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.crt]?
Reading file from tftp://10.1.1.2/johndoe/msca.crt
Loading johndoe/msca.crt from 10.1.1.2 (via Ethernet0):!
[OK - 1289 bytes]
% PEM files import succeeded.
Router(config)#
```

Related Commands

Command	Description
crypto pki export pem	Exports certificates and RSA keys that are associated with a trustpoint in a PEM-formatted file.
crypto pki trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of a CA.

crypto ca import pkcs12

Note This command was replaced by the **crypto pki import pkcs12** command effective with Cisco IOS Release 12.3(7)T.

To import Rivest, Shamir, and Adelman (RSA) keys, use the **crypto ca import pkcs12** command in global configuration mode.

crypto ca import *trustpointname* **pkcs12** *source url passphrase*

Syntax Description

trustpointname	Name of the trustpoint who issues the certificate that a user is going to export or import. When importing, the trustpoint name will become the RSA key name.
source url	The location of the PKCS12 file to which a user wants to export the RSA key pair.
passphrase	Passphrase that must be entered to undo encryption when the RSA keys are imported.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

When you enter the **cyrpto ca import pkcs12** command, a ke pair and a trustpoint are generated. If you then decide you want to remove the key pair and trustpoint that were generated, enter the **crypto key zeroize rsa** command to zeroize the key pair and enter the **no crypto ca trustpoint** command to remove the trustpoint.

Note After you import RSA keys to a target router, you cannot export those keys from the target router to another router.

Examples

In the following example, an RSA key pair that has been associated with the trustpoint “forward” is to be imported:

```
Router(config)# crypto ca import forward pkcs12 flash:myexport mycompany
```

Related Commands

Command	Description
crypto pki export pkcs12	Exports RSA keys.
crypto pki trustpoint	Declares the CA that your router should use.
crypto key zeroize rsa	Deletes all RSA keys from your router.

crypto ca profile enrollment

Note This command was replaced with the **crypto pki profile enrollment** command effective with Cisco IOS Release 12.3(7)T.

To define an enrollment profile, use the **crypto ca profile enrollment** command in global configuration mode. To delete all information associated with this enrollment profile, use the **no** form of this command.

crypto ca profile enrollment *label*

no crypto ca profile enrollment *label*

Syntax Description

label	Name for the enrollment profile; the enrollment profile name must match the name specified in the **enrollment profile** command.

Defaults

An enrollment profile does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Before entering this command, you must specify a named enrollment profile using the **enrollment profile** in ca-trustpoint configuration mode.

After entering the **crypto ca profile enrollment** command, you can use any of the following commands to define the profile parameters:

- **authentication command**—Specifies the HTTP command that is sent to the certification authority (CA) for authentication.
- **authentication terminal**—Specifies manual cut-and-paste certificate authentication requests.
- **authentication url**—Specifies the URL of the CA server to which to send authentication requests.
- **enrollment command**—Specifies the HTTP command that is sent to the CA for enrollment.
- **enrollment terminal**—Specifies manual cut-and-paste certificate enrollment.
- **enrollment url**—Specifies the URL of the CA server to which to send enrollment requests.
- **parameter**—Specifies parameters for an enrollment profile. This command can be used only if the **authentication command** or the **enrollment command** is used.

Note The **authentication url**, **enrollment url**, **authentication terminal**, and **enrollment terminal** commands allow you to specify different methods for certificate authentication and enrollment, such as TFTP authentication and manual enrollment.

Examples

The following example shows how to define the enrollment profile named "E" and associated profile parameters:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
enrollment profile	Specifies that an enrollment profile can be used for certificate authentication and enrollment.

crypto ca trusted-root

The **crypto ca trusted-root** command is replaced by the **crypto ca trustpoint** command. See the **crypto ca trustpoint** command for more information.

crypto ca trustpoint

Note Effective with Cisco IOS Release 12.3(8)T, the **crypto ca trustpoint** command is replaced with the **crypto pki trustpoint** command. See the **crypto pki trustpoint** command for more information.

To declare the certification authority (CA) that your router should use, use the **crypto ca trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the CA, use the **no** form of this command.

crypto ca trustpoint *name*

no crypto ca trustpoint *name*

Syntax Description

name	Creates a name for the CA. (If you previously declared the CA and just want to update its characteristics, specify the name you previously created.)

Defaults

Your router does not recognize any CAs until you declare a CA using this command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(15)T	The **match certificate** subcommand was introduced.
12.3(7)T	This command was replaced by the **crypto pki trustpoint** command. You can still enter the **crypto ca trusted-root** or **crypto ca trustpoint** command, but the command will be written in the configuration as "crypto pki trustpoint."

Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA, which can be a self-signed root CA or a subordinate CA. Issuing the **crypto ca trustpoint** command puts you in ca-trustpoint configuration mode.

You can specify characteristics for the trustpoint CA using the following subcommands:

- **crl**—Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.
- **default (ca-trustpoint)**—Resets the value of ca-trustpoint configuration mode subcommands to their defaults.
- **enrollment**—Specifies enrollment parameters (optional).
- **enrollment http-proxy**—Accesses the CA by HTTP through the proxy server.
- **match certificate**—Associates a certificate-based access control list (ACL) defined with the **crypto ca certificate map** command.

- **primary**—Assigns a specified trustpoint as the primary trustpoint of the router.
- **root**—Defines the Trivial File Transfer Protocol (TFTP) to get the CA certificate and specifies both a name for the server and a name for the file that will store the CA certificate.

Note Beginning with Cisco IOS Release 12.2(8)T, the **crypto ca trustpoint** command unified the functionality of the **crypto ca identity** and **crypto ca trusted-root** commands, thereby replacing these commands. Although you can still enter the **crypto ca identity** and **crypto ca trusted-root** commands, the configuration mode and command will be written in the configuration as **"crypto ca trustpoint**."

The following example shows how to declare the CA named "ka" and specify enrollment and CRL parameters:

```
crypto ca trustpoint ka
 enrollment url http://kahului:80
```

The following example shows a certificate-based access control list (ACL) with the label "Group" defined in a **crypto ca certificate map** command and included in the **match certificate** subcommand of the **crypto ca | pki trustpoint** command:

```
crypto ca certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto ca trustpoint pki
 match certificate Group
```

Related Commands

Command	Description
crl	Queries the CRL to ensure that the certificate of the peer has not been revoked.
default (ca-trustpoint)	Resets the value of a ca-trustpoint configuration subcommand to its default.
enrollment	Specifies the enrollment parameters of your CA.
enrollment http-proxy	Accesses the CA by HTTP through the proxy server.
primary	Assigns a specified trustpoint as the primary trustpoint of the router.
root	Obtains the CA certificate via TFTP.

crypto call admission limit

To specify the maximum number of Internet Key Exchange (IKE) security associations (SAs) that the router can establish before IKE begins rejecting new SA requests, use the **crypto call admission limit** command in global configuration mode. To disable this feature, use the **no** form of this command.

crypto call admission limit ike sa *number*

no crypto call admission limit ike sa *number*

Syntax Description

ikd sa *number*	Number of active IKE SAs allowed on the router. The value must be greater than 1.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use this command to limit the number of IKE SAs permitted to or from a router. By limiting the amount of dynamic tunnels that can be created to the router, you can prevent the router from being overwhelmed if it is suddenly inundated with IKE SA requests. The ideal limit depends on the particular platform, the network topology, the application, and traffic patterns. When the specified limit is reached, IKE rejects all new SA requests. If you specify an IKE SA limit that is less than the current number of active IKE SAs, a warning is displayed, but SAs are not terminated. New SA requests are rejected until the active SA count is below the configured limit.

Examples

The following example specifies that there can be a maximum of 50 IKE SAs before IKE begins rejecting new SA requests.

```
Router(config)# crypto call admission limit ike sa 50
```

Related Commands

Command	Description
show crypto call admission statistics	Monitors Crypto CAC statistics.

crypto dynamic-map

To create a dynamic crypto map entry and enter the crypto map configuration command mode, use the **crypto dynamic-map** command in global configuration mode. To delete a dynamic crypto map set or entry, use the **no** form of this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num*

no crypto dynamic-map *dynamic-map-name* [*dynamic-seq-num*]

Syntax Description

dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the number of the dynamic crypto map entry.

Defaults

No dynamic crypto maps exist.

Command Modes

Global configuration.

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use dynamic crypto maps to create policy templates that can be used when processing negotiation requests for new security associations from a remote IP Security peer, even if you do not know all of the crypto map parameters required to communicate with the remote peer (such as the peer's IP address). For example, if you do not know about all the IPSec remote peers in your network, a dynamic crypto map allows you to accept requests for new security associations from previously unknown peers. (However, these requests are not processed until the Internet Key Exchange authentication has completed successfully.)

When a router receives a negotiation request via IKE from another IPSec peer, the request is examined to see if it matches a crypto map entry. If the negotiation does not match any explicit crypto map entry, it will be rejected unless the crypto map set includes a reference to a dynamic crypto map.

The dynamic crypto map is a policy template; it will accept "wildcard" parameters for any parameters not explicitly stated in the dynamic crypto map entry. This allows you to set up IPSec security associations with a previously unknown IPSec peer. (The peer still must specify matching values for the "non-wildcard" IPSec security association negotiation parameters.)

If the router accepts the peer's request, at the point that it installs the new IPSec security associations it also installs a temporary crypto map entry. This entry is filled in with the results of the negotiation. At this point, the router performs normal processing, using this temporary crypto map entry as a normal entry, even requesting new security associations if the current ones are expiring (based upon the policy specified in the temporary crypto map entry). Once the flow expires (that is, all of the corresponding security associations expire), the temporary crypto map entry is removed.

Dynamic crypto map sets are not used for initiating IPSec security associations. However, they are used for determining whether or not traffic should be protected.

The only configuration required in a dynamic crypto map is the **set transform-set** command. All other configuration is optional.

Dynamic crypto map entries, like regular static crypto map entries, are grouped into sets. After you define a dynamic crypto map set (which commonly contains only one map entry) using this command, you include the dynamic crypto map set in an entry of the "parent" crypto map set using the **crypto map** (IPSec global configuration) command. The parent crypto map set is then applied to an interface.

You should make crypto map entries referencing dynamic maps the lowest priority map entries, so that negotiations for security associations will try to match the static crypto map entries first. Only after the negotiation request does not match any of the static map entries do you want it to be evaluated against the dynamic map.

To make a dynamic crypto map the lowest priority map entry, give the map entry referencing the dynamic crypto map the highest *seq-num* of all the map entries in a crypto map set.

For both static and dynamic crypto maps, if unprotected inbound traffic matches a **permit** statement in an access list, and the corresponding crypto map entry is tagged as "IPSec," then the traffic is dropped because it is not IPSec-protected. (This is because the security policy as specified by the crypto map entry states that this traffic must be IPSec-protected.)

For static crypto map entries, if outbound traffic matches a **permit** statement in an access list and the corresponding security association (SA) is not yet established, the router will initiate new SAs with the remote peer. In the case of dynamic crypto map entries, if no SA existed, the traffic would simply be dropped (because dynamic crypto maps are not used for initiating new SAs).

Note Use care when using the **any** keyword in **permit** entries in dynamic crypto maps. If it is possible for the traffic covered by such a **permit** entry to include multicast or broadcast traffic, the access list should include **deny** entries for the appropriate address range. Access lists should also include **deny** entries for network and subnet broadcast traffic, and for any other traffic that should not be IPSec protected.

Examples

The following example configures an IPSec crypto map set.

Crypto map entry "mymap 30" references the dynamic crypto map set "mydynamicmap," which can be used to process inbound security association negotiation requests that do not match "mymap" entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in "mydynamicmap," for a flow "permitted" by the access list 103, IPSec will accept the request and set up security associations with the remote peer without previously knowing about the remote peer. If accepted, the resulting security associations (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with "mydynamicmap 10" is also used as a filter. Inbound packets that match a **permit** statement in this list are dropped for not being IPSec protected. (The same is true for access lists associated with static crypto maps entries.) Outbound packets that match a **permit** statement without an existing corresponding IPSec SA are also dropped.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
crypto map mymap 20 ipsec-isakmp
 match address 102
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
```

```
crypto dynamic-map mydynamicmap 10
 match address 103
 set transform-set my_t_set1 my_t_set2 my_t_set3
```

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for this crypto map entry, or that IPSec requires PFS when receiving requests for new security associations.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto engine accelerator logs	Displays a dynamic crypto map set.
show crypto map (IPSec)	Displays the crypto map configuration.

crypto engine accelerator

To enable the onboard hardware accelerator of the router for IP security (IPSec) encryption, use the **crypto engine accelerator** command in global configuration mode. To disable the use of the onboard hardware IPSec accelerator, and thereby perform IPSec encryption or decryption in software, use the **no** form of this command.

crypto engine accelerator

no crypto engine accelerator

Syntax Description

This command has no arguments or keywords.

Defaults

The hardware accelerator for IPSec encryption is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco 1700 series router and other Cisco routers that support hardware accelerators for IPSec encryption.
12.1(3)XL	Support was added for the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

Usage Guidelines

This command is not normally needed for typical operations because the onboard hardware accelerator of the router is enabled for IPSec encryption by default. The hardware accelerator should not be disabled except on instruction from Cisco Technical Assistance Center (TAC) personnel.

Examples

The following example shows how to disable the onboard hardware accelerator of the router for IPSec encryption. This is normally needed only after the accelerator has been disabled for testing or debugging purposes.

```
Router(config)# no crypto engine accelerator

Warning! all current connections will be torn down.
```

```
Do you want to continue? [yes/no]:
```

Related Commands

Command	Description
clear crypto engine accelerator counter	Resets the statistical and error counters for the hardware accelerator to zero.
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
crypto ipsec	Defines the IPSec security associations and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator ring	Displays the contents of command and transmits rings for the crypto engine.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine SA database.
show crypto engine accelerator statistic	Displays the current run-time statistics and error counters for the crypto engine.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

crypto identity

To configure the identity of the router with a given list of distinguished names (DNs) in the certificate of the router, use the **crypto identity** command in global configuration mode. To delete all identity information associated with a list of DNs, use the **no** form of this command.

crypto identity *name*

no crypto identity *name*

Syntax Description

name	Identity of the router, which is associated with the given list of DNs.

Defaults

If this command is not enabled, the IP address is associated with the identity of the router.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

The **crypto identity** command allows you to configure the identity of a router with a given list of DNs. Thus, when used with the **dn** and **fqdn** commands, you can set restrictions in the router configuration that prevent peers with specific certificates, especially certificates with particular DNs, from having access to selected encrypted interfaces.

Note The identity of the peer must be the same as the identity in the exchanged certificate.

Examples

The following example shows how to configure a DN-based crypto map:

```
! The following is an IPSec crypto map (part of IPSec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
 set peer 172.21.114.196
 set transform-set my-transformset
 match address 124
 identity to-bigbiz
!
crypto identity to-bigbiz
 dn ou=BigBiz
!
!
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
 set peer 172.21.115.119
 set transform-set my-transformset
```

```
 match address 125
 identity to-little-com
!
crypto identity to-little-com
 fqdn little.com
!
```

Related Commands

Command	Description
crypto mib ipsec flowmib history failure size	Associates the identity of the router with the DN in the certificate of the router.
fqdn	Associates the identity of the router with the hostname that the peer used to authenticate itself.

crypto ipsec client ezvpn (global)

To create a Cisco Easy VPN remote configuration and enter the Cisco Easy VPN remote configuration mode, use the **crypto ipsec client ezvpn** command in global configuration mode. To delete the Cisco Easy VPN remote configuration, use the **no** form of this command.

crypto ipsec client ezvpn *name*

no crypto ipsec client ezvpn *name*

Note A separate **crypto ipsec client ezvpn** command in interface configuration mode assigns a Cisco Easy VPN remote configuration to the interface.

Syntax Description

name	Identifies the Cisco Easy VPN remote configuration with a unique, arbitrary name.

Defaults

Newly created Cisco Easy VPN remote configurations default to **client** mode.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)YA	This command was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(8)YJ	This command was enhanced to enable you to manually establish and terminate an IPSec VPN tunnel on demand for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(4)T	The **username** subcommand was added, and the **peer** subcommand was changed so that the command may now be input multiple times.
12.3(7)XR	The **acl** and **backup** subcommands were added.
12.3(11)T	The **acl** subcommand was integrated into Cisco IOS Release 12.3(11)T. However, the **backup** subcommand was not integrated into Cisco IOS 12.3(11)T.

Usage Guidelines

The **crypto ipsec client ezvpn** command creates a Cisco Easy VPN remote configuration and then enters the Cisco Easy VPN Remote configuration mode, at which point you can enter the following subcommands:

- **acl** {*acl-name* | *acl-number*}—Specifies multiple subnets in a Virtual Private Network (VPN) tunnel. Up to 50 subnets may be configured.
  - The *acl-name* argument is the name of the access control list (ACL).
  - The *acl-number* argument is the number of the ACL.
- **backup** {*ezvpn-config-name*} **track** {*tracked-object-number*}—Specifies the Easy VPN configuration that will be activated when backup is triggered.
  - **backup** {*ezvpn-config-name*}—Specifies the Easy VPN configuration that will be activated when backup is triggered.
  - **track** {*tracked-object-number*}—Specifies the link to the tracking system so that the Easy VPN state machine can get the notification to trigger the backup.
- **connect** [**auto** | **manual | acl**]—To manually establish and terminate an IP Security (IPSec) Virtual Private Network (VPN) tunnel on demand.
  - The **auto** option is the default setting, because it was the initial Cisco Easy VPN remote functionality. The IPSec VPN tunnel is automatically connected when the Cisco Easy VPN Remote feature is configured on an interface.
  - The **manual** option specifies the manual setting to direct the Cisco Easy VPN remote to wait for a command or application programming interface (API) call before attempting to establish the Cisco Easy VPN Remote connection. When the tunnel times out or fails, subsequent connections have to wait for the command to reset to manual or to an API call.
  - The **acl** option specifies the ACL-triggered setting, which is used for transactional-based applications and dial backup. Using this option, you can define the “interesting” traffic that triggers the tunnel to be established.
- **default**—Sets the following command to its default values.
- **exit**—Exits the Cisco Easy VPN configuration mode and returns to global configuration mode.
- **group** *group-name* **key** *group-key*—Specifies the group name and key value for the VPN connection.
- **local-address** *interface-name*—Informs the Cisco Easy VPN remote which interface is used to determine the public IP address, which is used to source the tunnel. This applies only to the Cisco uBR905 and Cisco uBR925 cable access routers.
  - The value of the *interface-name* argument specifies the interface used for tunnel traffic.

  After specifying the local address used to source tunnel traffic, the IP address can be obtained in two ways:
  - The **local-address** subcommand can be used with the **cable-modem dhcp-proxy** {**interface loopback** *number} command to obtain a public IP address and automatically assign it to the loopback interface.*
  - The IP address can be manually assigned to the loopback interface.
- **mode** {**client** | **network-extension | network extension plus**}—Specifies the VPN mode of operation of the router:
  - The **client** mode (default) automatically configures the router for Cisco Easy VPN client mode operation, which uses Network Address Translation (NAT) or Peer Address Translation (PAT) address translations. When the Cisco Easy VPN remote configuration is assigned to an interface,the router automatically creates the NAT or PAT and access list configuration needed for the VPN connection.

  - The **network-extension** option specifies that the router should become a remote extension of the enterprise network at the other end of the VPN connection. The PCs that are connected to the router typically are assigned an IP address in the address space of the enterprise network.
  - The **network extension plus** mode is identical to network extension mode with the additional capability of being able to request an IP address via mode configuration and automatically assign it to an available loopback interface. The IPSec security associations (SAs) for this IP address are automatically created by Easy VPN Remote. The IP address is typically used for troubleshooting (using ping, Telnet, and Secure Shell).

- **no**—Removes the command or sets it to its default values.
- **peer** {*ipaddress* | *hostname*}—Sets the peer IP address or hostname for the VPN connection. A hostname can be specified only when the router has a Domain Name System (DNS) server available for hostname resolution.

  The **peer** subcommand may be input multiple times.
- **username** *name* **password** {**0** | **6**} {*password*}—Allows you to save your extended authentication (Xauth) password locally on the PC. On subsequent authentications, you may activate the save-password tick box on the software client or add the username and password to the Cisco IOS hardware client profile. The setting remains until the save-password attribute is removed from the server group profile.
  - **0** specifies that an unencrypted password will follow.
  - **6** specifies that an encrypted password will follow.
  - *password specifies an unencrypted (cleartext) user password.*

  The save-password option is useful only if the user password is static, that is, it is not a one-time password (OTP), such as a password generated by a token.

After configuring the Cisco Easy VPN remote configuration, use the **exit** command to exit the Cisco Easy VPN Remote configuration mode and return to global configuration mode.

Note You cannot use the **no crypto ipsec client ezvpn** command to delete a Cisco Easy VPN remote configuration that is assigned to an interface. You must remove that Cisco Easy VPN remote configuration from the interface before you can delete the configuration.

Examples

The following example shows a Cisco Easy VPN remote configuration named “telecommuter-client” being created on a Cisco uBR905 or Cisco uBR925 cable access router and being assigned to cable interface 0:

```
Router# configure terminal
Router(config)# crypto ipsec client ezvpn telecommuter-client
Router(config-crypto-ezvpn)# group telecommute-group key secret-telecommute-key
Router(config-crypto-ezvpn)# peer telecommuter-server
Router(config-crypto-ezvpn)# mode client
Router(config-crypto-ezvpn)# exit
Router(config)# interface c0
Router(config-if)# crypto ezvpn telecommuter-client
Router(config-if)# exit
```

Note Specifying the **mode client** option as shown above is optional, because this is default configuration for these options.

The following example shows the Cisco Easy VPN remote configuration named “telecommuter-client” being removed from the interface and then deleted:

```
Router# configure terminal
Router(config)# interface e1
Router(config-if)# no crypto ipsec client ezvpn telecommuter-client
Router(config-if)# exit
Router(config)# no crypto ipsec client ezvpn telecommuter-client
```

Related Commands

Command	Description
crypto ipsec client ezvpn (interface)	Assigns a Cisco Easy VPN Remote configuration to an interface.

crypto ipsec client ezvpn (interface)

To assign a Cisco Easy VPN Remote configuration to an interface, specify whether the interface is outside or inside, and configure multiple outside and inside interfaces, use the **crypto ipsec client ezvpn** command in interface configuration mode. To remove the Cisco Easy VPN Remote configuration from the interface, use the **no** form of this command.

crypto ipsec client ezvpn *name* [**outside** | **inside**]

no crypto ipsec client ezvpn *name* [**outside** | **inside**]

Note A separate **crypto ipsec client ezvpn** command exists in global configuration mode that creates a Cisco Easy VPN Remote configuration.

Syntax Description

name	Specifies the Cisco Easy VPN Remote configuration to be assigned to the interface.
outside	(Optional) Specifies the outside interface of the IP Security (IPSec) client router. You can add up to four outside tunnels for all platforms, one tunnel per outside interfaces.
inside	(Optional) Specifies the inside interface of the IPSec client router. The Cisco 1700 series has no default inside interface, and any inside interface must be configured. The Cisco 800 series routers and Cisco uBR905 and Cisco uBR925 cable access routers have default inside interfaces. However, you can configure any inside interface. You can add up to three inside interfaces for all platforms.

Defaults

The default inside interface is the Ethernet interface on Cisco 800 series routers and Cisco uBR905 and Cisco uBR925 cable access routers.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)YA	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(8)YJ	This command was enhanced to enable you to configure multiple outside and inside interfaces for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

The **crypto ipsec client ezvpn** command assigns a Cisco Easy VPN Remote configuration to an interface, enabling the creation of a Virtual Private Network (VPN) connection over that interface to the specified VPN peer. If the Cisco Easy VPN Remote configuration is configured for the client mode of operation, this also automatically configures the router for network address translation (NAT) or port address translation (PAT) and for an associated access list.

In Cisco IOS Release 12.2(8)YJ, the **crypto ipsec client ezvpn** command was enhanced to allow you to configure multiple outside and inside interfaces. To configure multiple outside and inside interfaces, you must use the **interface** *interface-name* command to first define the type of interface on the IPSec client router.

- In client mode for the Cisco Easy VPN Client, a single security association (SA) connection is used for encrypting and decrypting the traffic coming from all the inside interfaces. In network extension mode, one SA connection is established for each inside interface.
- When a new inside interface is added or an existing one is removed, all established SA connections are deleted and new ones are initiated.
- Configuration information for the default inside interface is shown with the **crypto ipsec client ezvpn name inside** command. All inside interfaces, whether they belong to a tunnel, are listed in interface configuration mode as an inside interface, along with the tunnel name.

The following Cisco IOS Release 12.2(4)YA restrictions apply to the **crypto ipsec client ezvpn** command:

- The Cisco Easy VPN Remote feature supports only one tunnel, so the **crypto ipsec client ezvpn** command can be assigned to only one interface. If you attempt to assign it to more than one interface, an error message is displayed. You must use the **no** form of this command to remove the configuration from the first interface before assigning it to the second interface.
- The **crypto ipsec client ezvpn** command should be assigned to the outside interface of the NAT or PAT translation. This command cannot be used on the inside NAT or PAT interface. On some platforms, the inside and outside interfaces are fixed.

  For example, on Cisco uBR905 and Cisco uBR925 cable access routers, the outside interface is always the cable interface. On Cisco 1700 series routers, the FastEthernet interface defaults to being the inside interface, so attempting to use the **crypto ipsec client ezvpn** command on the FastEthernet interface displays an error message.

Note You must first use the global configuration version of the **crypto ipsec client ezvpn** command to create a Cisco Easy VPN Remote configuration before assigning it to an interface.

Examples

The following example shows a Cisco Easy VPN Remote configuration named “telecommuter-client” being assigned to the cable interface on a Cisco uBR905/uBR925 cable access router:

```
Router# configure terminal
Router(config)# interface c0
Router(config-if)# crypto ipsec client ezvpn telecommuter-client
Router(config-if)# exit
```

The following example first shows an attempt to delete the Cisco Easy VPN Remote configuration named “telecommuter-client,” but the configuration cannot be deleted because it is still assigned to an interface. The configuration is then removed from the interface and deleted.

```
Router# configure terminal
Router(config)# no crypto ipsec client ezvpn telecommuter-client
Error: crypto map in use by interface; cannot delete
```

```
Router(config)# interface e1
Router(config-if)# no crypto ipsec client ezvpn telecommuter-client
Router(config-if)# exit
Router(config)# no crypto ipsec client ezvpn telecommuter-client
```

Related Commands

Command	Description
crypto ipsec client ezvpn (global)	Creates and modifies a Cisco Easy VPN Remote configuration.
interface	Configures an interface type.

crypto ipsec client ezvpn connect

To connect to a specified IPSec Virtual Private Network (VPN) tunnel in a manual configuration, use the **crypto ipsec client ezvpn connect** command in privileged EXEC mode. To disable, use the **no** form of this command.

crypto ipsec client ezvpn connect *name*

no crypto ipsec client ezvpn connect *name*

Syntax Description

name	Identifies the IPSec VPN tunnel with a unique, arbitrary name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)YJ	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

This command is used with the **connect** [**auto** | **manual** | **acl**] subcommand. After the manual setting is designated, the Cisco Easy VPN remote waits for a command or application programming interface (API) call before attempting to establish the Cisco Easy VPN remote connection.

If the configuration is manual, the tunnel is connected only after the **crypto ipsec client ezvpn connect** *name* command is entered in privileged EXEC mode, and after the **connect** [**auto**] | **manual** subcommand is entered.

Examples

The following example shows how to connect an IPSec VPN tunnel named ISP-tunnel on a Cisco uBR905/uBR925 cable access router:

```
Router# crypto ipsec client ezvpn connect ISP-tunnel
```

Related Commands

Command	Description
connect	Manually establishes and terminates an IPSec VPN tunnel on demand.
crypto ipsec client ezvpn (global)	Creates and modifies a Cisco Easy VPN remote configuration.

crypto ipsec client ezvpn xauth

To respond to a pending Virtual Private Network (VPN) authorization request, use the **crypto ipsec client ezvpn xauth** command in privileged EXEC mode.

crypto ipsec client ezvpn xauth *name*

Syntax Description

name	Identifies the IP Security (IPSec) VPN tunnel with a unique, arbitrary name. This name is required.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)YA	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(8)YJ	This command was enhanced to specify an IPSec VPN tunnel for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(8)YJ	This command was enhanced to specify an IPSec VPN tunnel for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

If the tunnel name is not specified, the authorization request is made on the active tunnel. If there is more than one active tunnel, the command fails with an error requesting that you specify the tunnel name.

When making a VPN connection, individual users might also be required to provide authorization information, such as a username or password. When the remote end requires this information, the router displays a message on the console of the router instructing the user to enter the **crypto ipsec client ezvpn xauth** command. The user then uses command-line interface (CLI) to enter this command and to provide the information requested by the prompts that follow after the command has been entered.

Note If the user does not respond to the authentication notification, the message is repeated every 10 seconds.

Examples

The following example shows an example of the user being prompted to enter the **crypto ipsec client ezvpn xauth** command. The user then enters the requested information and continues.

```
Router#
20:27:39: EZVPN: Pending XAuth Request, Please enter the following command:
20:27:39: EZVPN: crypto ipsec client ezvpn xauth

Router> crypto ipsec client ezvpn xauth
Enter Username and Password: userid
Password: ************
```

Related Commands

Command	Description
crypto ipsec client ezvpn (interface)	Assigns a Cisco Easy VPN Remote configuration to an interface.

crypto ipsec df-bit (global)

To set the DF bit for the encapsulating header in tunnel mode to all interfaces, use the **crypto ipsec df-bit** command in global configuration mode.

crypto ipsec df-bit {**clear** | **set** | **copy**}

Syntax Description

clear	Outer IP header will have the DF bit cleared, and the router may fragment the packet to add the IP Security (IPSec) encapsulation.
set	Outer IP header will have the DF bit set; however, the router may fragment the packet if the original packet had the DF bit cleared.
copy	The router will look in the original packet for the outer DF bit setting. The **copy** keyword is the default setting.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

Use the **crypto ipsec df-bit** command in global configuration mode to configure your router to specify the DF bit in an encapsulated header.

You may want use the **clear** setting for the DF bit when encapsulating tunnel mode IPSec traffic so you can send packets larger than the available maximum transmission unit (MTU) size or if you do not know what the available MTU size is.

If this command is enabled without a specified setting, the router will use the **copy** setting as default.

Examples

The following example shows how to clear the DF bit on all interfaces:

```
crypto ipsec df-bit clear
```

crypto ipsec df-bit (interface)

To set the DF bit for the encapsulating header in tunnel mode to a specific interface, use the **crypto ipsec df-bit** command in interface configuration mode.

crypto ipsec df-bit {**clear** | **set** | **copy**}

Syntax Description

clear	Outer IP header will have the DF bit cleared, and the router may fragment the packet to add the IP Security (IPSec) encapsulation.
set	Outer IP header will have the DF bit set; however, the router may fragment the packet if the original packet had the DF bit cleared.
copy	The router will look in the original packet for the outer DF bit setting. The **copy** keyword is the default setting.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

Use the **crypto ipsec df-bit** command in interface configuration mode to configure your router to specify the DF bit in an encapsulated header. This command overrides any existing DF bit global settings.

You may want use the **clear** setting for the DF bit when encapsulating tunnel mode IPSec traffic so you can send packets larger than the available maximum transmission unit (MTU) size or if you do not know what the available MTU size is.

If this command is enabled without a specified setting, the router will use the **copy** setting as default.

Examples

In following example, the router is configured to globally clear the setting for the DF bit and copy the DF bit on the interface named Ethernet0. Thus, all interfaces *except* Ethernet0 will allow the router to send packets larger than the available MTU size; Ethernet0 will allow the router to fragment the packet.

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key Delaware address 192.168.10.66
crypto isakmp key Key-What-Key address 192.168.11.19
!
!
crypto ipsec transform-set BearMama ah-md5-hmac esp-des

crypto ipsec df-bit clear
!
!
```

```
crypto map armadillo 1 ipsec-isakmp
set peer 192.168.10.66
set transform-set BearMama
match address 101
!
crypto map basilisk 1 ipsec-isakmp
set peer 192.168.11.19
set transform-set BearMama
match address 102

!
!
interface Ethernet0
 ip address 192.168.10.38 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map armadillo
 crypto ipsec df-bit copy
!
interface Ethernet1
 ip address 192.168.11.75 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map basilisk
!
interface Serial0
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 no ip mroute-cache
```

crypto ipsec fragmentation (global)

To enable prefragmentation for IP Security (IPSec) Virtual Private Networks (VPNs) on a global basis, use the **crypto ipsec fragmentation** command in global configuration mode. To disable a manually configured command, use the **no** form of this command.

crypto ipsec fragmentation {**before-encryption** | **after-encryption**}

no crypto ipsec fragmentation {**before-encryption** | **after-encryption**}

Syntax Description

before-encryption	Enables prefragmentation for IPSec VPNs.
after-encryption	Disables prefragmentation for IPSec VPNs.

Defaults

If no other prefragmentation for IPSec VPNs commands are in the configuration, the router will revert to the default global configuration.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use the **before-encryption** keyword to enable prefragmentation for IPSec VPNs; use the **after-encryption** keyword to disable prefragmentation for IPSec VPNs. This command allows an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA). If it is predetermined that the packet will exceed the maximum transmission unit (MTU) of the output interface, the packet is fragmented before encryption.

Note This command does not show up in the a running configuration if the default global command is enabled. It shows in the running configuration only when you explicitly enable the command on an interface.

Examples

The following example shows how to globally enable prefragmentation for IPSec VPNs:

```
crypto ipsec fragmentation before-encryption
```

crypto ipsec fragmentation (interface)

To enable prefragmentation for IP Security (IPSec) Virtual Private Networks (VPNs) on an interface, use the **crypto ipsec fragmentation** command in interface configuration mode. To disable a manually configured command, use the **no** form of this command.

crypto ipsec fragmentation {**before-encryption** | **after-encryption**}

no crypto ipsec fragmentation {**before-encryption** | **after-encryption**}

Syntax Description

before-encryption	Enables prefragmentation for IPSec VPNs.
after-encryption	Disables prefragmentation for IPSec VPNs.

Defaults

If no other prefragmentation for IPSec VPNs commands are in the configuration, the router will revert to the default global configuration.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use the **before-encryption** keyword to enable prefragmentation for IPSec VPNs per interface; use the **after-encryption** keyword to disable prefragmentation for IPSec VPNs. This command allows an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA). If it is predetermined that the packet will exceed the maximum transmission unit (MTU) of output interface, the packet is fragmented before encryption.

Examples

The following example shows how to enable prefragmentation for IPSec VPNs on an interface and then how to display the output of the show running configuration command:

Note This command shows in the running configuration only when you explicitly enable it on the interface.

```
Router(config-if)# crypto ipsec fragmentation before-encryption
Router(config-if)# exit

Router# show running-config

crypto isakmp policy 10
 authentication pre-share
crypto isakmp key abcd123 address 209.165.202.130
!
```

```
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
!
crypto map bar 10 ipsec-isakmp
 set peer 209.165.202.130
 set transform-set fooprime
 match address 102
```

crypto ipsec optional

To enable IP Security (IPSec) passive mode, use the **crypto ipsec optional** command in global configuration mode. To disable IPSec passive mode, use the **no** form of this command.

crypto ipsec optional

no crypto ipsec optional

Syntax Description

This command has no arguments or keywords.

Defaults

IPSec passive mode is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **crypto ipsec optional** command to implement an intermediate mode (IPSec passive mode) that allows a router to accept unencrypted and encrypted data. IPSec passive mode is valuable for users who wish to migrate existing networks to IPSec because all routers will continue to interact with routers that encrypt data (that is, that have been upgraded with IPSec) and also with routers that have yet to be upgraded.

After this feature is disabled, all active connections that are sending unencrypted packets are cleared, and a message that reminds the user to enter the **write memory** command is sent.

Note Because a router in IPSec passive mode is insecure, ensure that no routers are accidentally left in this mode after upgrading a network.

Examples

The following example shows how to enable IPSec passive mode:

```
crypto map xauthmap 10 ipsec-isakmp
 set peer 209.165.202.145
 set transform-set xauthtransform
 match address 192
!
crypto ipsec optional
!
interface Ethernet1/0
 ip address 209.165.202.147 255.255.255.224
 crypto map xauthmap
!
access-list 192 permit ip host 209.165.202.147 host 209.165.202.145
```

crypto ipsec optional retry

To adjust the amount of time that a packet can be routed in the clear (unencrypted), use the **crypto ipsec optional retry** command in global configuration mode. To return to the default setting (5 minutes), use the **no** form of this command.

crypto ipsec optional retry *seconds*

no crypto ipsec optional retry *seconds*

Syntax Description

seconds	Time a connection can exist before another attempt is made to establish an encrypted IP Security (IPSec) session. The default value is 5 minutes.

Defaults

5 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

You must enable the **crypto ipsec optional** command, which enables IPSec passive mode, before you can use this command.

Examples

The following example shows how to enable IPSec passive mode:

```
crypto map xauthmap 10 ipsec-isakmp
 set peer 209.165.202.145
 set transform-set xauthtransform
 match address 192
!
crypto ipsec optional
crypto ipsec optional retry 60
!
interface Ethernet1/0
 ip address 209.165.202.147 255.255.255.224
 crypto map xauthmap
!
access-list 192 permit ip host 209.165.202.147 host 209.165.202.145
```

Related Commands

Command	Description
crypto ipsec optional	Enables IPSec passive mode.

crypto ipsec profile

To define the IPSecurity (IPSec) parameters that are to be used for IPSec encryption between two IPSec routers, use the **crypto ipsec profile** command in global configuration mode. To delete an IPSec profile, use the **no** form of this command.

crypto ipsec profile *name*

no crypto ipsec profile *name*

Syntax Description

name	Profile name.

Defaults

An IPSec profile is not defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

An IPSec profile abstracts the IPSec policy settings into a single profile that can be used in other parts of the Cisco IOS configuration.

The IPSec profile shares most of the same commands with the crypto map configuration, but only a subset of the commands are valid in an IPSec profile. Only commands that pertain to an IPSec policy can be issued under an IPSec profile; you cannot specify the IPSec peer address or the access control list (ACL) to match the packets that are to be encrypted.

The following valid commands can be configured under an IPSec profile:

- **set-transform-set**—Specifies a list of transform sets in order of priority.
- **set pfs**—Specifies perfect forward secrecy (PFS) settings.
- **set security-association**—Defines security association parameters.
- **set-identity**—Specifies identity restrictions.

After enabling this command, the only parameter that *must* be defined under the profile is the transform set via the **set transform-set** command.

For more information on transform sets, refer to the section “Defining Transform Sets” in the chapter “Configuring IPSec Network Security” in the *Cisco IOS Security Configuration Guide*.

Examples

The following example shows how to configure a crypto map that uses an IPSec profile:

```
crypto ipsec transform-set cat-transforms esp-des esp-sha-hmac
 mode transport
!
crypto ipsec profile cat-profile
```

```
 set transform-set cat-transforms
 set pfs group2
!
interface Tunnel1
 ip address 192.168.1.1 255.255.255.252
 tunnel source FastEthernet2/0
 tunnel destination 10.13.7.67
 tunnel protection ipsec profile cat-profile
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set.
set pfs	Specifies that IP Security should ask for PFS when requesting new security associations for a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
tunnel protection	Associates a tunnel interface with an IPSec profile.

crypto ipsec security-association lifetime

To change global lifetime values used when negotiating IPSec security associations, use the **crypto ipsec security-association lifetime** command in global configuration mode. To reset a lifetime to the default value, use the **no** form of this command.

crypto ipsec security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes*}

no crypto ipsec security-association lifetime {**seconds** | **kilobytes**}

Syntax Description

seconds *seconds*	Specifies the number of seconds a security association will live before expiring. The default is 3600 seconds (one hour).
kilobytes *kilobytes*	Specifies the volume of traffic (in kilobytes) that can pass between IPSec peers using a given security association before that security association expires. The default is 4,608,000 kilobytes.

Defaults

3600 seconds (one hour) and 4,608,000 kilobytes (10 megabits per second for one hour).

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry does not have lifetime values configured, when the router requests new security associations during security association negotiation, it will specify its global lifetime value in the request to the peer; it will use this value as the lifetime of the new security associations. When the router receives a negotiation request from the peer, it will use the smaller of the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The security association expires after the first of these lifetimes is reached.

If you change a global lifetime, the change is only applied when the crypto map entry does not have a lifetime value specified. The change will not be applied to existing security associations, but will be used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command. Refer to the **clear crypto sa** command for more details.

To change the global timed lifetime, use the **crypto ipsec security-association lifetime seconds** form of the command. The timed lifetime causes the security association to time out after the specified number of seconds have passed.

To change the global traffic-volume lifetime, use the **crypto ipsec security-association lifetime kilobytes** form of the command. The traffic-volume lifetime causes the security association to time out after the specified amount of traffic (in kilobytes) has been protected by the security associations' key.

Shorter lifetimes can make it harder to mount a successful key recovery attack, since the attacker has less data encrypted under the same key to work with. However, shorter lifetimes require more CPU processing time for establishing new security associations.

The lifetime values are ignored for manually established security associations (security associations installed using an **ipsec-manual** crypto map entry).

How These Lifetimes Work

The security association (and corresponding keys) will expire according to whichever occurs sooner, either after the number of seconds has passed (specified by the **seconds** keyword) or after the amount of traffic in kilobytes has passed (specified by the **kilobytes** keyword).

A new security association is negotiated *before* the lifetime threshold of the existing security association is reached, to ensure that a new security association is ready for use when the old one expires. The new security association is negotiated either 30 seconds before the **seconds** lifetime expires or when the volume of traffic through the tunnel reaches 256 kilobytes less than the **kilobytes** lifetime (whichever occurs first).

If no traffic has passed through the tunnel during the entire life of the security association, a new security association is not negotiated when the lifetime expires. Instead, a new security association will be negotiated only when IPSec sees another packet that should be protected.

Examples

The following example shortens both lifetimes, because the administrator feels there is a higher risk that the keys could be compromised. The timed lifetime is shortened to 2700 seconds (45 minutes), and the traffic-volume lifetime is shortened to 2,304,000 kilobytes (10 megabits per second for one half hour).

```
crypto ipsec security-association lifetime seconds 2700
crypto ipsec security-association lifetime kilobytes 2304000
```

Related Commands

Command	Description
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations.
show crypto ipsec security-association lifetime	Displays the security-association lifetime value configured for a particular crypto map entry.

crypto ipsec transform-set

To define a transform set—an acceptable combination of security protocols and algorithms—use the **crypto ipsec transform-set** command in global configuration mode. To delete a transform set, use the **no** form of this command.

crypto ipsec transform-set *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]

no crypto ipsec transform-set *transform-set-name*

Syntax Description

transform-set-name	Name of the transform set to create (or modify).
transform1 *transform2* *transform3* *transform4*	Type of transform set. You may specify up to four "transforms": one Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication, and one compression. These transforms define the IP Security (IPSec) security protocols and algorithms. Accepted transform values are described in Table 14.

Defaults

No default behavior or values

Command Modes

Global configuration

This command invokes the crypto transform configuration mode.

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(13)T	The following transform set options were added: **esp-aes**, **esp-aes 192**, and **esp-aes 256**.
12.3(7)T	The **esp-seal** transform set option was added.

Usage Guidelines

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPSec-protected traffic. During the IPSec security association (SA) negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

You can configure multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPSec SA negotiation to protect the data flows specified by the access list of that crypto map entry. During the negotiation, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and will be applied to the protected traffic as part of the IPSec SAs of both peers.

When Internet Key Exchange (IKE) is not used to establish SAs, a single transform set must be used. The transform set is not negotiated.

Before a transform set can be included in a crypto map entry, it must be defined using this command.

A transform set specifies one or two IPSec security protocols (either AH, ESP, or both) and specifies which algorithms to use with the selected security protocol. The AH and ESP IPSec security protocols are described in the section "IPSec Protocols: AH and ESP."

To define a transform set, you specify one to four "transforms"—each transform represents an IPSec security protocol (AH or ESP) plus the algorithm you want to use. When the particular transform set is used during negotiations for IPSec SAs, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

In a transform set you can specify the AH protocol, the ESP protocol, or both. If you specify an ESP protocol in a transform set, you can specify just an ESP encryption transform set or both an ESP encryption transform set and an ESP authentication transform set.

Table 14 lists the acceptable transform set combination selections for the AH and ESP protocols.

Table 14 Allowed Transform Combinations

Transform Type	Transform	Description
AH Transform (*Pick only one.*)	ah-md5-hmac	AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm
	ah-sha-hmac	AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm
ESP Encryption Transform (*Pick only one.*)	esp-aes	ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithim
	esp-aes 192	ESP with the 192-bit AES encryption algorithim
	esp-aes 256	ESP with the 256-bit AES encryption algorithim
	esp-des	ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm
	esp-3des	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES)
	esp-null	Null encryption algorithm
	esp-seal	ESP with the 160-bit SEAL encryption algorithm.

Table 14 Allowed Transform Combinations

Transform Type	Transform	Description
ESP Authentication Transform (*Pick only one.*)	esp-md5-hmac	ESP with the MD5 (HMAC variant) authentication algorithm
	esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm
IP Compression Transform	comp-lzs	IP compression with the Lempel-Ziv-Stac (LZS) algorithm

Examples of acceptable transform set combinations are as follows:

- **ah-md5-hmac**
- **esp-des**
- **esp-3des** and **esp-md5-hmac**
- **ah-sha-hmac** and **esp-des** and **esp-sha-hmac**
- **comp-lzs and esp-sha-hmac and esp-aes (In general, the comp-lzs transform set can be included with any other legal combination that does not already include the comp-lzs** transform.**)**
- esp-seal and esp-md5-hmac

The parser will prevent you from entering invalid combinations; for example, after you specify an AH transform set, it will not allow you to specify another AH transform set for the current transform set.

IPSec Protocols: AH and ESP

Both the AH and ESP protocols implement security services for IPSec.

AH provides data authentication and antireplay services.

ESP provides packet encryption and optional data authentication and antireplay services.

ESP encapsulates the protected data—either a full IP datagram (or only the payload)—with an ESP header and an ESP trailer. AH is embedded in the protected data; it inserts an AH header immediately after the outer IP header and before the inner IP datagram or payload. Traffic that originates and terminates at the IPSec peers can be sent in either tunnel or transport mode; all other traffic is sent in tunnel mode. Tunnel mode encapsulates and protects a full IP datagram, while transport mode encapsulates or protects the payload of an IP datagram. For more information about modes, see the **mode** (IPSec) command description.

The esp-seal Transform

There are three limitations on the use of the **esp-seal** transform set:

- The **esp-seal** transform set can be used only if no crypto accelerators are present. This limitation is present because no current crypto accelerators implement the SEAL encryption transform set, and if a crypto accelerator is present, it will handle all IPSec connections that are negotiated with IKE. If a crypto accelerator is present, the Cisco IOS software will allow the transform set to be configured, but it will warn that it will not be used as long as the crypto accelerator is enabled.
- The **esp-seal** transform set can be used only in conjunction with an authentication transform set, namely one of these: **esp-md5-hmac, esp-sha-hmac**, **ah-md5-hmac**, or **ah-sha-hmac**. This limitation is present because SEAL encryption is especially weak when it comes to protecting

against modifications of the encrypted packet. Therefore, to prevent such a weakness, an authentication transform set is required. (Authentication transform sets are designed to foil such attacks.) If you attempt to configure an IPSec transform set using SEAL but without an authentication transform set, an error is generated, and the transform set is rejected.

- The **esp-seal** transform set cannot be used with a manually keyed crypto map. This limitation is present because such a configuration would reuse the same keystream for each reboot, which would compromise security. Because of the security issue, such a configuration is prohibited. If you attempt to configure a manually keyed crypto map with a SEAL-based transform set, an error is generated, and the transform set is rejected.

Selecting Appropriate Transform Sets

The following tips may help you select transform sets that are appropriate for your situation:

- If you want to provide data confidentiality, include an ESP encryption transform set.
- If you want to ensure data authentication for the outer IP header as well as the data, include an AH transform set. (Some consider the benefits of outer IP header data integrity to be debatable.)
- If you use an ESP encryption transform set, also consider including an ESP authentication transform set or an AH transform set to provide authentication services for the transform set.
- If you want data authentication (either using ESP or AH), you can choose from the MD5 or SHA (HMAC keyed hash variants) authentication algorithms. The SHA algorithm is generally considered stronger than MD5 but is slower.
- Note that some transform sets might not be supported by the IPSec peer.

Note If a user enters an IPSec transform set that the hardware does not support, a warning message will be displayed immediately after the **crypto ipsec transform-set** command is entered.

- In cases where you need to specify an encryption transform set but do not actually encrypt packets, you can use the **esp-null** transform.

Suggested transform set combinations follow:

- **esp-3des** and **esp-sha-hmac**
- **esp-aes** and **esp-md5-hmac**

The Crypto Transform Configuration Mode

After you issue the **crypto ipsec transform-set** command, you are put into the crypto transform configuration mode. While in this mode, you can change the mode to tunnel or transport. (These are optional changes.) After you have made these changes, type **exit** to return to global configuration mode. For more information about these optional changes, see the **match address** (IPSec) and **mode** (IPSec) command descriptions.

Changing Existing Transform Sets

If one or more transform sets are specified in the **crypto ipsec transform-set** command for an existing transform set, the specified transform sets will replace the existing transform sets for that transform set.

If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change will not be applied to existing SAs but will be used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa** command.

Examples

The following example defines two transform sets. The first transform set will be used with an IPSec peer that supports the newer ESP and AH protocols. The second transform set will be used with an IPSec peer that supports only the older transforms.

```
Router (config)# crypto ipsec transform-set newer esp-3des esp-sha-hmac
Router (config)# crypto ipsec transform-set older ah-rfc-1828 esp-rfc1829
```

The following example is a sample warning message that is displayed when a user enters an IPSec transform set that the hardware does not support:

```
Router (config)# crypto ipsec transform transform-1 esp-aes 256 esp-md5
WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

The following output example shows that SEAL encryption has been correctly configured with an authentication transform set:

```
Router (config)# crypto ipsec transform-set seal esp-seal esp-sha-hmac
```

The following example is a warning message that is displayed when SEAL encryption has been configured with a crypto accelerator present:

```
Router (config)# show running-config

crypto ipsec transform-set seal esp-seal esp-sha-hmac
! Disabled because transform not supported by encryption hardware
```

The following example is an error message that is displayed when SEAL encryption has been configured without an authentication transform set:

```
Router (config)# crypto ipsec transform seal esp-seal
ERROR: Transform requires either ESP or AH authentication.
```

The following example is an error message that is displayed when SEAL encryption has been configured within a manually keyed crypto map:

```
Router (config)# crypto map green 10 ipsec-manual
%Note: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router (config-crypto-map)# set transform seal
ERROR: transform seal illegal for a manual crypto map.
```

Related Commands

Command	Description
clear crypto sa	Deletes IPSec security associations.
crypto ipsec transform-set	Defines a transform set—an acceptable combination of security protocols and algorithms.
match address	Specifies an extended access list for a crypto map entry.
mode (IPSec)	Changes the mode for a transform set.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto ipsec transform-set	Displays the configured transform sets.

crypto isakmp aggressive-mode disable

To block all Internet Security Association and Key Management Protocol (ISAKMP) aggressive mode requests to and from a device, use the **crypto isakmp aggressive-mode disable** command in global configuration mode. To disable the blocking, use the **no** form of this command.

crypto isakmp aggressive-mode disable

no crypto isakmp aggressive-mode disable

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, Cisco IOS software will attempt to process all incoming ISAKMP aggressive mode security association (SA) connections. In addition, if the device has been configured with the **crypto isakmp peer address** and the **set aggressive-mode password** or **set aggressive-mode client-endpoint** commands, the device will initiate aggressive mode if this command is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced on all Cisco IOS platforms that support IP Security (IPSec).

Usage Guidelines

If you configure this command, all aggressive mode requests to the device and all aggressive mode requests made by the device are blocked, regardless of the ISAKMP authentication type (preshared keys or Rivest, Shamir, and Adelman [RSA] signatures).

If a request is made by or to the device for aggressive mode, the following syslog notification is sent:

```
Unable to initiate or respond to Aggressive Mode while disabled
```

Note This command will prevent Easy Virtual Private Network (Easy VPN) clients from connecting if they are using preshared keys because Easy VPN clients (hardware and software) use aggressive mode.

Examples

The following example shows that all aggressive mode requests to and from a device are blocked:

```
Router (config)# crypto isakmp aggressive-mode disable
```

crypto isakmp client configuration address-pool local

To configure the IP address local pool to reference Internet Key Exchange (IKE) on your router, use the **crypto isakmp client configuration address-pool local** command in global configuration mode. To restore the default value, use the **no** form of this command.

crypto isakmp client configuration address-pool local *pool-name*

no crypto isakmp client configuration address-pool local

Syntax Description

pool-name	Specifies the name of a local address pool.

Defaults

IP address local pools do not reference IKE.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XE	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS release 12.0(7)T.

Examples

The following example references IP address local pools to IKE on your router, with “ire” as the *pool-name*:

```
crypto isakmp client configuration address-pool local ire
```

Related Commands

Command	Description
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

crypto isakmp client configuration group

To specify to which group a policy profile will be defined, use the **crypto isakmp client configuration group** command in global configuration mode. To remove this command and all associated subcommands from your configuration, use the **no** form of this command.

crypto isakmp client configuration group {*group-name* | **default**}

no crypto isakmp client configuration group

Syntax Description

group-name	Group definition that identifies which policy is enforced for users.
default	Policy that is enforced for all users who do not offer a group name that matches a *group-name* argument. The default keyword can only be configured locally.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(2)T	The **access-restrict**, **firewall are-u-there**, **group-lock**, **include-local-lan**, and **save-password** commands were added. These commands are added during Mode Configuration. In addition, this command was modified so that output for this command will show that the preshared key is either encrypted or unencrypted.
12.3(4)T	The **backup-gateway**, **max-logins**, **max-users, and pfs** commands were added.

Usage Guidelines

Use the **crypto isakmp client configuration group command to specify group policy information that needs to be defined or changed. You may wish to change the group policy on your router if you decide to connect to the client using a group ID that does not match the** *group-name* argument.

After enabling this command, which puts you in Internet Security Association Key Management Protocol (ISAKMP) **group configuration mode, you can specify characteristics for the group policy using the following commands:**

- **access-restrict—Ties a particular Virtual Private Network (VPN) group to a specific interface for access to the Cisco IOS gateway and the services it protects.**
- **acl**—Configures split tunneling.
- **backup-gateway**—Configures a server to “push down” a list of backup gateways to the client. These gateways are tried in order in the case of a failure of the previous gateway. The gateways may be specified using IP addresses or host names.
- **dns**—Specifies the primary and secondary Domain Name Service (DNS) servers for the group.

- **domain**—Specifies group domain membership.
- **firewall are-u-there—**Adds the Firewall-Are-U-There attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls.
- **group-lock—Use if preshared key authentication is used with** Internet Key Exchange (**IKE). Allows you to enter your extended authentication (Xauth) username. The group delimiter is compared against the group identifier sent during IKE aggressive mode.**
- **include-local-lan**—Configures the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client.
- **key**—Specifies the IKE preshared key when defining group policy information for Mode Configuration push.
- **max-logins**—Limits the number of simultaneous logins for users in a specific user group.
- **max-users**—Limits the number of connections to a specific server group.
- **pfs**—Configures a server to notify the client of the central-site policy regarding whether PFS is required for any IPSec SA. Because the client device does not have a user interface option to enable or disable PFS negotiation, the server will notify the client device of the central site policy via this parameter. The Diffie-Hellman (D-H) group that is proposed for PFS will be the same that was negotiated in Phase 1 of the IKE negotiation.
- **pool**—Refers to the IP local pool address used to allocate internal IP addresses to clients.
- **save-password**—Saves your Xauth password locally on your PC.
- **split-dns**—Specifies a list of domain names that must be tunneled or resolved to the private network.
- **wins**—Specifies the primary and secondary Windows Internet Naming Service (WINS) servers for the group.

Output for the **crypto isakmp client configuration group** command (using the **key** subcommand) will show that the preshared key is either encrypted or unencrypted. An output example for an unencrypted preshared key would be as follows:

```
crypto isakmp client configuration group key test
```

An output example for a type 6 encrypted preshared key would be as follows:

crypto isakmp client configuration group

```
 key 6 JK_JHZPeJV_XFZTKCQFYAAB
```

Session Monitoring and Limiting for Easy VPN Clients

It is possible to mimic the functionality provided by some RADIUS servers for limiting the number of connections to a specific server group and also for limiting the number of simultaneous logins for users in that group.

To limit the number of connections to a specific server group, use the **max-users** subcommand. To limit the number of simultaneous logins for users in the server group, use the **max-logins** subcommand.

The following example shows the RADIUS attribute-value (AV) pairs for the maximum users and maximum logins parameters:

```
ipsec:max-users=1000
ipsec:max-logins=1
```

The **max-users** and **max-logins** commands can be enabled together or individually to control the usage of resources by any groups or individuals.

If you use a RADIUS server, such as a CiscoSecure access control server (ACS), it is recommended that you enable this session control on the RADIUS server if the functionality is provided. In this way, usage can be controlled across a number of servers by one central repository. When enabling this feature on the router itself, only connections to groups on that specific device are monitored, and load-sharing scenarios are not accurately accounted for.

Examples

The following example shows how to define group policy information for Mode Configuration push. In this example, the first group name is "cisco" and the second group name is "default." Thus, the default policy will be enforced for all users who do not offer a group name that matches "cisco."

```
crypto isakmp client configuration group cisco
 key cisco
 dns 2.2.2.2 2.2.2.3
 wins 6.6.6.6
 domain cisco.com
 pool fred
 acl 199
!
crypto isakmp client configuration group default
 key cisco
 dns 2.2.2.2 2.3.2.3
 pool fred
 acl 199
```

Related Commands

Command	Description
access-restrict	Ties a particular VPN group to a specific interface for access to the Cisco IOS gateway and the services it protects.
acl	Configures split tunneling.
backup-gateway	Configures a server to "push down" a list of backup gateways to the client.
crypto isakmp keepalive	Adds the Firewall-Are-U-There attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls
dns	Specifies the primary and secondary DNS servers.
domain (isakmp-group)	Specifies the DNS domain to which a group belongs.
firewall are-u-there	Adds the Firewall-Are-U-There attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls.
group-lock	Allows you to enter your Xauth username, including the group name, when preshared key authentication is used with IKE.
include-local-lan	Configures the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client.
key (isakmp-group)	Specifies the IKE preshared key for Group-Policy attribute definition.
max-logins	Limits the number of simultaneous logins for users in a specific server group.
max-users	Limits the number of connections to a specific server group.
pool (isakmp-group)	Defines a local pool address.
save-password	Saves your Xauth password locally on your PC.
set aggressive-mode client-endpoint	Specifies the primary and secondary WINS servers.

crypto isakmp enable

To globally enable Internet Key Exchange (IKE) at your peer router, use the **crypto isakmp enable** command in global configuration mode. To disable IKE at the peer, use the **no** form of this command.

crypto isakmp enable

no crypto isakmp enable

Syntax Description

This command has no arguments or keywords.

Defaults

IKE is enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

IKE is enabled by default. IKE does not have to be enabled for individual interfaces, but is enabled globally for all interfaces at the router.

If you do not want IKE to be used in your IPSec implementation, you can disable IKE at all your IP Security peers. If you disable IKE at one peer, you must disable it at all your IPSec peers.

If you disable IKE, you will have to make these concessions at the peers:

- You must manually specify all the IPSec security associations (SAs) in the crypto maps at the peers. (Crypto map configuration is described in the chapter "Configuring IPSec Network Security" in the *Cisco IOS Security Configuration Guide*.)
- The IPSec SAs of the peers will never time out for a given IPSec session.
- During IPSec sessions between the peers, the encryption keys will never change.
- Anti-replay services will not be available between the peers.
- Certification authority (CA) support cannot be used.

Examples

The following example disables IKE at one peer. (The same command should be issued at all remote peers.)

```
no crypto isakmp enable
```

crypto isakmp identity

To define the identity used by the router when participating in the Internet Key Exchange (IKE) protocol, use the **crypto isakmp identity** command in global configuration mode. Set an Internet Security Association Key Management Protocol (ISAKMP) identity whenever you specify preshared keys. To reset the ISAKMP identity to the default value (address), use the **no** form of this command.

crypto isakmp identity {**address** | **hostname**}

no crypto isakmp identity

Syntax Description

address	Sets the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during IKE negotiations.
hostname	Sets the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.example.com).

Defaults

The IP address is used for the ISAKMP identity.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command to specify an ISAKMP identity either by IP address or by host name.

The **address** keyword is typically used when there is only one interface (and therefore only one IP address) that will be used by the peer for IKE negotiations, and the IP address is known.

The **hostname** keyword should be used if there is more than one interface on the peer that might be used for IKE negotiations, or if the interface's IP address is unknown (such as with dynamically assigned IP addresses).

As a general rule, you should set all peers' identities in the same way, either by IP address or by host name.

Examples

The following example uses preshared keys at two peers and sets both their ISAKMP identities to IP address.

At the local peer (at 10.0.0.1) the ISAKMP identity is set and the preshared key is specified.

```
crypto isakmp identity address
crypto isakmp key sharedkeystring address 192.168.1.33
```

At the remote peer (at 192.168.1.33) the ISAKMP identity is set and the same preshared key is specified.

```
crypto isakmp identity address
crypto isakmp key sharedkeystring address 10.0.0.1
```

Note In the preceding example if the **crypto isakmp identity** command had not been performed, the ISAKMP identities would have still been set to IP address, the default identity.

The following example uses preshared keys at two peers and sets both their ISAKMP identities to host name.

At the local peer the ISAKMP identity is set and the preshared key is specified.

```
crypto isakmp identity hostname
crypto isakmp key sharedkeystring hostname RemoteRouter.example.com
ip host RemoteRouter.example.com 192.168.0.1
```

At the remote peer the ISAKMP identity is set and the same preshared key is specified.

```
crypto isakmp identity hostname
crypto isakmp key sharedkeystring hostname LocalRouter.example.com
ip host LocalRouter.example.com 10.0.0.1 10.0.0.2
```

In the above example, host names are used for the peers' identities because the local peer has two interfaces that might be used during an IKE negotiation.

In the above example the IP addresses are also mapped to the host names; this mapping is not necessary if the routers' host names are already mapped in DNS.

Related Commands

Command	Description
crypto ipsec security-association lifetime	Specifies the authentication method within an IKE policy.
crypto isakmp key	Configures a preshared authentication key.

crypto isakmp invalid-spi-recovery

To initiate the Internet Key Exchange (IKE) security association (SA) to notify the receiving IP Security (IPSec) peer that there is an "Invalid SPI" error, use the **crypto isakmp invalid-spi-recovery** command in global configuration mode. To disable the notification process, use the **no** form of this command.

crypto isakmp invalid-spi-recovery

no crypto isakmp invalid-spi-recovery

Syntax Description

This command has no arguments or keywords.

Defaults

The IKE notification process is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

This command allows you to configure your router so that when an invalid security parameter index error (shown as "Invalid SPI") occurs, an IKE SA is initiated. The "IKE" module, which serves as a checkpoint in the IPSec session, recognizes the "Invalid SPI" situation. The IKE module then sends an "Invalid Error" message to the packet-receiving peer so that synchronization of the security association databases (SADBs) of the two peers can be attempted. As soon as the SADBs are resynchronized, packets are no longer dropped.

Caution Using this command to initiate an IKE SA to notify an IPSec peer of an "Invalid SPI" error can result in a denial-of-service (DoS) attack.

Examples

The following example shows that the IKE module process has been initiated to notify the receiving peer that there is an "Invalid SPI" error:

```
Router (config)# crypto isakmp invalid-spi-recovery
```

crypto isakmp keepalive

To allow the gateway to send dead peer detection (DPD) messages to the peer, use the **crypto isakmp keepalive** command in global configuration mode. To disable keepalives, use the **no** form of this command.

crypto isakmp keepalive *seconds* [*retries*] [**periodic** | **on-demand**]

no crypto isakmp keepalive *seconds* [*retries*] [**periodic** | **on-demand**]

Syntax Description

seconds	Number of seconds between DPD messages; the range is from 10 to 3600 seconds. **Note** If you do not specify a time interval, you will receive an error message.
retries	(Optional) Number of seconds between DPD retries if the DPD message fails; the range is from 2 to 60 seconds. If unspecified, the default is 2 seconds.
periodic	(Optional) DPD messages are sent at regular intervals.
on-demand	(Optional) The default behavior. DPD retries are sent on demand. **Note** Because this option is the default, the **on-demand** keyword does not appear in configuration output.

Defaults

No DPD messages are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(7)T	The **periodic** and **on-demand** keywords were added.

Usage Guidelines

Use the **crypto isakmp keepalive** command to enable the gateway to send DPD messages to the peer. DPD is a keepalives scheme that allows the router to query the liveliness of its Internet Key Exchange (IKE) peer.

Use the **periodic** keyword to configure your router so that DPD messages are "forced" at regular intervals. This forced approach results in earlier detection of dead peers than with the on-demand approach. If you do not configure the periodic option, the router defaults to the on-demand approach.

Note When the **crypto isakmp keepalive** command is configured, the Cisco IOS software negotiates the use of Cisco IOS keepalives or DPD, depending on which protocol the peer supports.

Examples

The following example shows how to configure DPD messages to be sent every 60 seconds and every 5 seconds between retries if the peer does not respond:

```
crypto isakmp keepalive 60 5
```

The following example shows that periodic DPD messages are to be sent at intervals of 10 seconds:

```
crypto isakmp keepalive 10 periodic
```

The following example shows that the above periodic behavior is being disabled:

```
crypto isakmp keepalive 10 on-demand
```

Related Commands

Command	Description
acl	Configures split tunneling.

crypto isakmp key

To configure a preshared authentication key, use the **crypto isakmp key command in** global configuration mode. To delete a preshared authentication key, use the **no** form of this command.

crypto isakmp key *keystring {***address** *peer-address [mask]* | **hostname** *hostname} [***no-xauth***]*

no crypto isakmp key *keystring {***address** *peer-address [mask]* | **hostname** *hostname}*

Syntax Description

keystring	Specifies the preshared key. Use any combination of alphanumeric characters up to 128 bytes. This preshared key must be identical at both peers.
address	Use this keyword if the remote peer Internet Security Association Key Management Protocol (ISAKMP) identity was set with its IP address. The *peer-address* argument specifies the IP address of the remote peer.
peer-address	Specifies the IP address of the remote peer.
mask	(Optional) Specifies the subnet address of the remote peer. (The argument can be used only if the remote peer ISAKMP identity was set with its IP address.)
hostname *hostname*	Fully qualified domain name (FQDN) of the peer.
no-xauth	(Optional) Use this keyword if router-to-router IP Security (IPSec) is on the same crypto map as a Virtual Private Network (VPN)-client-to-Cisco-IOS IPSec. This keyword prevents the router from prompting the peer for extended authentication (Xauth) information (username and password).

Defaults

There is no default preshared authentication key.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.1(1)T	The *mask* argument was added.
12.2(4)T	The **no-xauth** keyword was added.
12.3(2)T	This command was modified so that output shows that the preshared key is either encrypted or unencrypted.

Usage Guidelines

You must use this command to configure a key whenever you specify preshared keys in an Internet Key Exchange (IKE) policy; you must enable this command at both peers.

If an IKE policy includes preshared keys as the authentication method, these preshared keys must be configured at both peers—otherwise the policy cannot be used (the policy will not be submitted for matching by the IKE process). The **crypto isakmp key** command is the second task required to configure the preshared keys at the peers. (The first task is accomplished using the **crypto isakmp identity** command.)

Use the **address** keyword if the remote peer ISAKMP identity was set with its IP address.

With the **address** keyword, you can also use the *mask* argument to indicate the remote peer ISAKMP identity will be established using the preshared key only. If the *mask* argument is used, preshared keys are no longer restricted between two users.

Note If you specify *mask*, you must use a subnet address. (The subnet address 0.0.0.0 is not recommended because it encourages group preshared keys, which allow all peers to have the same group key, thereby reducing the security of your user authentication.)

Preshared keys no longer work when the hostname keyword is sent as the identity; thus, the hostname keyword as the identity in preshared key authentication is no longer supported. According to the way preshared key authentication is designed in IKE main mode, the preshared keys *must* be based on the IP address of the peers. Although a user can still send the hostname as identity in preshared key authentication, the key is searched on the IP address of the peer; if the key is not found (based on the IP address), the negotiation will fail.

If **crypto isakmp identity hostname** is configured as identity, the preshared key *must* be configured with the peer's IP address for the process to work.

Use the **no-xauth** keyword to prevent the router from prompting the peer for Xauth information (username and password). This keyword disables Xauth for static IPSec peers. The **no-xauth** keyword should be enabled when configuring the preshared key for router-to-router IPSec—not VPN-client-to-Cisco-IOS IPSec.

Output for the **crypto isakmp key** command will show that the preshared key is either encrypted or unencrypted. An output example for an unencrypted preshared key would be as follows:

```
crypto isakmp key test123 address 10.1.0.1
```

An output example for a type 6 encrypted preshared key would be as follows:

```
crypto isakmp key 6 RHZE[JACMUI\bcbTdELISAAB address 10.1.0.1
```

Examples

In the following example, the remote peer "RemoteRouter" specifies an ISAKMP identity by address:

```
crypto isakmp identity address
```

Now, the preshared key must be specified at each peer.

In the following example, the local peer specifies the preshared key and designates the remote peer by its IP address and a mask:

```
crypto isakmp key sharedkeystring address 172.21.230.33  255.255.255.255
```

Related Commands

Command	Description
crypto ipsec security-association lifetime	Specifies the authentication method within an IKE policy.
crypto isakmp identity	Defines the identity the router uses when participating in the IKE protocol.
ip host	Defines a static host name-to-address mapping in the host cache.

crypto isakmp peer

To enable an IP Security (IPSec) peer for Internet Key Exchange (IKE) querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode, use the **crypto isakmp peer** command in global configuration mode. To disable this functionality, use the **no** form of this command.

crypto isakmp peer {**ip-address** *ip-address* | **fqdn** *fqdn*} {**vrf** *fvrf-name*}

no crypto isakmp peer {**ip-address** *ip-address* | **fqdn** *fqdn*} {**vrf** *fvrf-name*}

Syntax Description

ip-address *ip-address*	IP address of the peer router.
fqdn *fqdn*	Fully qualified domain name (FQDN) of the peer router.
vrf *fvrf-name*	Virtual routing and forwarding (VRF) routing table through which the peer is reachable.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(15)T	The **vrf** keyword and *fvrf-name* argument were added.

Usage Guidelines

After enabling this command, you can use the **set aggressive-mode client-endpoint** and **set aggressive-mode password** commands to specify RADIUS tunnel attributes in the Internet Security Association and Key Management Protocol (ISAKMP) peer policy for IPSec peers.

Instead of keeping your preshared keys on the hub router, you can scale your preshared keys by storing and retrieving them from an AAA server. The preshared keys are stored in the AAA server as Internet Engineering Task Force (IETF) RADIUS tunnel attributes and are retrieved when a user tries to "speak" to the hub router. The hub router retrieves the preshared key from the AAA server and the spokes (the users) initiate aggressive mode to the hub by using the preshared key that is specified in the ISAKMP peer policy as a RADIUS tunnel attribute.

Examples

The following example shows how to initiate aggressive mode using RADIUS tunnel attributes:

```
crypto isakmp peer ip-address 209.165.200.230 vrf vpn1
 set aggressive-mode client-endpoint user-fqdn user@cisco.com
 set aggressive-mode password cisco123
```

Related Commands

Command	Description
crypto map isakmp authorization list	Enables IKE querying of AAA for tunnel attributes in aggressive mode.
set aggressive-mode client-endpoint	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.
set aggressive-mode password	Specifies the Tunnel-Password attribute within an ISAKMP peer configuration.

crypto isakmp policy

To define an Internet Key Exchange policy, use the **crypto isakmp policy** command in global configuration mode. IKE policies define a set of parameters to be used during the IKE negotiation. To delete an IKE policy, use the **no** form of this command.

crypto isakmp policy *priority*

no crypto isakmp policy

Syntax Description

priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 10,000, with 1 being the highest priority and 10,000 the lowest.

Defaults

There is a default policy, which always has the lowest priority. This default policy contains default values for the encryption, hash, authentication, Diffie-Hellman group, and lifetime parameters. (The parameter defaults are listed below in the "Usage Guidelines" section.)

When you create an IKE policy, if you do not specify a value for a particular parameter, the default for that parameter will be used.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command to specify the parameters to be used during an IKE negotiation. (These parameters are used to create the IKE security association [SA].)

This command invokes the Internet Security Association Key Management Protocol policy configuration (config-isakmp) command mode. While in the ISAKMP policy configuration command mode, the following commands are available to specify the parameters in the policy:

- **encryption (IKE policy)**; default = 56-bit DES-CBC
- **hash (IKE policy)**; default = SHA-1
- **crypto ipsec security-association lifetime**; default = RSA signatures
- **group (IKE policy)**; default = 768-bit Diffie-Hellman
- **lifetime (IKE policy)**; default = 86,400 seconds (one day)

If you do not specify one of these commands for a policy, the default value will be used for that parameter.

To exit the config-isakmp command mode, type **exit**.

You can configure multiple IKE policies on each peer participating in IPSec. When the IKE negotiation begins, it tries to find a common policy configured on both peers, starting with the highest priority policies as specified on the remote peer.

Examples

The following example configures two policies for the peer:

```
crypto isakmp policy 15
 hash md5
 authentication rsa-sig
 group 2
 lifetime 5000
crypto isakmp policy 20
 authentication pre-share
 lifetime 10000
```

The above configuration results in the following policies:

```
Router# show crypto isakmp policy

Protection suite priority 15
    encryption algorithm:DES - Data Encryption Standard (56 bit keys)
    hash algorithm:Message Digest 5
    authentication method:Rivest-Shamir-Adleman Signature
    Diffie-Hellman Group:#2 (1024 bit)
    lifetime:5000 seconds, no volume limit
Protection suite priority 20
    encryption algorithm:DES - Data Encryption Standard (56 bit keys)
    hash algorithm:Secure Hash Standard
    authentication method:preshared Key
    Diffie-Hellman Group:#1 (768 bit)
    lifetime:10000 seconds, no volume limit
Default protection suite
    encryption algorithm:DES - Data Encryption Standard (56 bit keys)
    hash algorithm:Secure Hash Standard
    authentication method:Rivest-Shamir-Adleman Signature
    Diffie-Hellman Group:#1 (768 bit)
    lifetime:86400 seconds, no volume limit
```

Related Commands

Command	Description
crypto ipsec security-association lifetime	Specifies the authentication method within an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

crypto isakmp profile

To define an Internet Security Association and Key Management Protocol (ISAKMP) profile and to audit IP Security (IPSec) user sessions, use the **crypto isakmp profile** command in global configuration mode. To delete a crypto ISAKMP profile, use the **no** form of this command.

crypto isakmp profile *profile-name* [**accounting** *aaalist*]

no crypto isakmp profile *profile-name* [**accounting** *aaalist*]

Syntax Description

profile-name	Name of the user profile. To associate a user profile with the RADIUS server, the user profile name must be identified.
accounting *aaalist*	(Optional) Name of a client accounting list.

Defaults

No default behaviors or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Defining an ISAKMP Profile

An ISAKMP profile can be viewed as a repository of Phase 1 and Phase 1.5 commands for a set of peers. The Phase 1 configuration includes commands to configure such things as keepalive, identity matching, and the authorization list. The Phase 1.5 configuration includes commands to configure such things as extended authentication (Xauth) and mode configuration.

The peers are mapped to an ISAKMP profile when their identities are matched (as given in the identification [ID] payload of the Internet Key Exchange [IKE]) against the identities defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid. Also, there must be at least one **match identity** command defined in the ISAKMP profile for it to be complete.

Auditing IPSec User Sessions

Use this command to audit multiple user sessions that are terminating on the IPSec gateway.

Note The **crypto isakmp profile** command and the **crypto map (global IPSec)** command are mutually exclusive. If a profile is present (the **crypto isakmp profile** command has been used), with no accounting configured but with the global command present (the **crypto isakmp profile** command without the **accounting** keyword), accounting will occur using the attributes in the global command.

Examples

The following example shows how to define an ISAKMP profile and match the peer identities:

```
crypto isakmp profile vpnprofile
 match identity address 10.76.11.53
```

The following accounting example shows that an ISAKMP profile is configured:

```
aaa new-model
!
!
aaa authentication login cisco-client group radius
aaa authorization network cisco-client group radius
aaa accounting network acc start-stop broadcast group radius
aaa session-id common
!
crypto isakmp profile cisco
vrf cisco
match identity group cclient
 client authentication list cisco-client
 isakmp authorization list cisco-client
 client configuration address respond
 accounting acc
!
crypto dynamic-map dynamic 1
 set transform-set aswan
 set isakmp-profile cisco
 reverse-route
!
!
radius-server host 172.1.1.4 auth-port 1645 acct-port 1646
radius-server key nsite
```

Related Commands

Command	Description
crypto map (global IPSec)	Enters crypto map configuration mode and creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, or configures a client accounting list.
debug crypto isakmp	Displays messages about IKE events.
match identity	Matches an identity from a peer in an ISAKMP profile.

crypto isamkp nat keepalive

To allow an IP Security (IPSec) node to send Network Address Translation (NAT) keepalive packets, use the **crypto isakmp nat keepalive** command in global configuration mode. To disable NAT keepalive packets, use the **no** form of this command.

crypto isakmp nat keepalive *seconds*

no crypto isakmp nat keepalive

Syntax Description

seconds	Number of seconds between keepalive packets; the range is between 5 and 3600 seconds.

Defaults

NAT keepalive packets are not sent.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The **crypto isakmp nat keepalive** command allows users to keep the dynamic NAT mapping alive during a connection between two peers. A NAT keepalive beat is sent if IPSec does not send or receive a packet within a specified time period.

If this command is enabled, users should ensure that the idle value is shorter than than the NAT mapping expiration time.

Examples

The following example shows how to enable NAT keepalives to be sent every 20 seconds:

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key 1234 address 209.165.202.130
crypto isakmp nat keepalive 20
!
crypto ipsec transform-set t2 esp-des esp-sha-hmac
no crypto engine accelerator
!
crypto map test2 10 ipsec-isakmp
 set peer 209.165.202.130
 set transform-set t2
 match address 101
```

crypto key decrypt rsa

To delete the encrypted RSA key and leave only the unencrypted key on the running router, use the **crypto key decrypt rsa** command in global configuration mode.

crypto key decrypt [**write**] **rsa** [**name** *key-name*] **passphrase** *passphrase*

Syntax Description

write	(Optional) Clear text (unencrypted) key is immediately written to NvRAM. If the **write** keyword is not issued, the configuration must be manually written to NvRAM; otherwise, the key will remain encrypted the next time the router is reloaded.
name *key-name*	(Optional) Name of the RSA key pair that is to be decrypted.
passphrase *passphrase*	Passphrase that is used to decrypt the RSA key. The passphrase must match the passphrase that was specified via the **crypto key encrypt rsa** command.

Defaults

The private key running on the router is encrypted.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **crypto key decrypt rsa** command to store the decrypted private key in NvRAM the next time NvRAM is written (which is immediately if the **write** keyword is issed).

Examples

The following example shows how to decrypt the RSA key “pki1-72a.cisco.com”:

```
Router(config)# crypto key decrypt write rsa name pki1-72a.cisco.com passphrase cisco1234
```

Related Commands

Command	Description
crypto key encrypt rsa	Encrypts the RSA private key.
show crypto key mypubkey rsa	Displays the RSA public keys of your router.

crypto key encrypt rsa

To encrypt the RSA private key, use the **crypto key encrypt rsa** command in global configuration mode.

crypto key encrypt [**write**] **rsa** [**name** *key-name*] **passphrase** *passphrase*

Syntax Description

write	(Optional) Router configuration is immediately written to NVRAM. If the **write** keyword is not issued, the configuration must be manually written to NvRAM; otherwise, the encrypted key will be lost next time the router is reloaded.
name *key-name*	(Optional) Name of the RSA key pair that is to be encrypted. If a key name is not specified, the default key name, *routername.domainname*, is used.
passphrase *passphrase*	Passphrase that is used to encrypt the RSA key. To access the RSA key pair, the passphrase must be specified.

Defaults

RSA keys are not encrypted.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

The private key is encrypted (protected) via the specified passphrase. After the key is protected, it may continue to be used by the router; that is Internet Key Exchange (IKE) tunnels and encrypted key export attempts should continue to work because the key remains "unlocked."

To lock the key, which can be used to disable the router, issue the **crypto key lock rsa** privileged EXEC command. (When you lock the encrypted key, all functions which use the locked key are disabled.)

Examples

The following example shows how to encrypt the RSA key "pki1-72a.cisco.com." Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the RSA key is encrypted and unlocked.

```
Router(config)# crypto key encrypt rsa name pki1-72a.cisco.com passphrase cisco1234
Router(config)# exit
Router# show crypto key mypubkey rsa
```

```
% Key pair was generated at:00:15:32 GMT Jun 25 2003
Key name:pki1-72a.cisco.com
Usage:General Purpose Key
*** The key is protected and UNLOCKED. ***
Key is not exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E0CC9A 1D23B52C
CD00910C ABD392AE BA6D0E3F FC47A0EF 8AFEE340 0EC1E62B D40E7DCC
23C4D09E
03018B98 E0C07B42 3CFD1A32 2A3A13C0 1FF919C5 8DE9565F 1F020301 0001
% Key pair was generated at:00:15:33 GMT Jun 25 2003
Key name:pki1-72a.cisco.com.server
Usage:Encryption Key
Key is exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D3491E 2A21D383
854D7DA8 58AFBDAC 4E11A7DD E6C40AC6 66473A9F 0C845120 7C0C6EC8 1FFF5757
3A41CE04 FDCB40A4 B9C68B4F BC7D624B 470339A3 DE739D3E F7DDB549 91CD4DA4
DF190D26 7033958C 8A61787B D40D28B8 29BCD0ED 4E6275C0 6D020301 0001
Router#
```

Related Commands

Command	Description
crypto key decrypt rsa	Deletes the encrypted RSA key and leaves only the unencrypted key on the running router.
crypto key lock rsa	Locks the RSA private key in a router.
show crypto key mypubkey rsa	Displays the RSA public keys of your router.

crypto key export pem

To export Rivest, Shamir, and Adelman (RSA) keys in privacy-enhanced mail (PEM)-formatted files, use the **crypto key export pem** command in global configuration mode.

crypto key export rsa *key-label* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase*

Syntax Description

rsa *key-label*	Name of the RSA key pair that will be exported. The *key-label* argument must match the key pair name that was specified via the **crypto key generate rsa** command.
terminal	RSA key pair will be displayed in PEM format on the console terminal.
url *url*	URL of the file system where your router should export the RSA key pair.
3des	Export the RSA key pair using the Triple Data Encryption Standard (3DES) encryption algorithm.
des	Export the RSA key pair using the DES encryption algorithm.
passphrase	Passphrase that is used to encrypt the PEM file for import. **Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **crypto key export pem** command allows you to export RSA key pairs in PEM-formatted files. The PEM files can then be imported back into a Cisco IOS router or other public key infrastructure (PKI) applications.

Note Before you can export a RSA key pair in a PEM file, ensure that the RSA key pair is exportable. To generate an exportable RSA key pair, issue the **crypto key generate rsa** command and specify the **exportable** keyword.

Examples

The following example shows how to generate, export, bring the key back (import), and verify the status of the RSA key pair "mycs":

```
! Generate the key pair
!
Router(config)# crypto key generate rsa general-purpose label mycs exportable
```

```
The name for the keys will be: mycs
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]
!
! Archive the key pair to a remote location, and use a good password.
!
Router(config)# crypto key export rsa mycs pem url nvram: 3des PASSWORD
% Key name: mycs
Usage: General Purpose Key
Exporting public key...
Destination filename [mycs.pub]?
Writing file to nvram:mycs.pub
Exporting private key...
Destination filename [mycs.prv]?
Writing file to nvram:mycs.prv
!
! Import the key as a different name.
!
Router(config)# crypto key import rsa mycs2 pem url nvram:mycs PASSWORD
% Importing public key or certificate PEM file...
Source filename [mycs.pub]?
Reading file from nvram:mycs.pub
% Importing private key PEM file...
Source filename [mycs.prv]?
Reading file from nvram:mycs.prv% Key pair import succeeded.
!
! After the key has been imported, it is no longer exportable.
!
! Verify the status of the key.
!
Router# show crypto key mypubkey rsa

% Key pair was generated at: 18:04:56 GMT Jun 6 2003
Key name: mycs
Usage: General Purpose Key
Key is exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
  9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
  A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
  A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
  C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
% Key pair was generated at: 18:17:25 GMT Jun 6 2003
Key name: mycs2
Usage: General Purpose Key
Key is not exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
  9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
  A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
  A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
  C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
```

Related Commands

Command	Description
crypto key generate rsa	Generates RSA key pairs.
crypto key import pem	Imports RSA keys in PEM-formatted files.

crypto key generate rsa (CA)

To generate RSA key pairs, use the **crypto key generate rsa** command in global configuration mode.

crypto key generate rsa [**usage-keys** | **general-keys**] [*key-pair-label*]

Syntax Description

usage-keys	(Optional) Specifies that two special-usage key pairs, instead of one general-purpose key pair, should be generated.
general-keys	(Optional) Specifies that the general-purpose key pair should be generated.
key-pair-label	(Optional) Specifies the name of the key pair that router will use. (If this argument is enabled, you *must* specify either **usage-keys** or **general-keys**.)

Defaults

Rivest, Shamir, and Adelman (RSA) key pairs do not exist.

If *key-pair-label* is not specified, the fully qualified domain name (FQDN) of the router is used, and general-purpose keys are generated.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(8)T	The **general-keys** keyword and the *key-pair-label* argument were added.

Usage Guidelines

Use this command to generate RSA key pairs for your Cisco device (such as a router).

RSA keys are generated in pairs—one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys.

Note Before issuing this command, ensure that your router has a host name and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a host name and IP domain name. (This situation is not true when you only generate a named key pair.)

This command is not saved in the router configuration; however, the keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device).

There are two mutually exclusive styles of RSA key pairs: special-usage keys and general-purpose keys. When you generate RSA key pairs, you will be prompted to select either generate special-usage keys or general-purpose keys.

Special-Usage Keys

If you generate special-usage keys, two pairs of RSA keys will be generated. One pair will be used with any Internet Key Exchange (IKE) policy that specifies RSA signatures as the authentication method, and the other pair used with any IKE policy that specifies RSA-encrypted nonces as the authentication method. (You configure RSA signatures or RSA-encrypted nonces in your IKE policies as described in the *Cisco IOS Security Configuration Guide*.)

A certification authority (CA) is used only with IKE policies specifying RSA signatures, not with IKE policies specifying RSA-encrypted nonces. (However, you could specify more than one IKE policy and have RSA signatures specified in one policy and RSA-encrypted nonces in another policy.)

If you plan to have both types of RSA authentication methods in your IKE policies, you might prefer to generate special-usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special-usage keys, one key is used for both purposes, increasing that key's exposure.)

General-Purpose Keys

If you generate general-purpose keys, only one pair of RSA keys will be generated. This pair will be used with IKE policies specifying either RSA signatures or RSA-encrypted nonces. Therefore, a general-purpose key pair might be used more frequently than a special-usage key pair.

Named Key Pairs

If you generate a named key pair using the *key-pair-label* argument, you must also specify the **usage-keys** keyword or the **general-keys** keyword. Named key pairs allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate.

Modulus Length

When you generate RSA keys, you will be prompted to enter a modulus length. A longer modulus could offer stronger security but takes longer to generate (see Table 15 for sample times) and takes longer to use. (The Cisco IOS software does not support a modulus greater than 2048 bits.) A length of less than 512 is normally not recommended. (In certain situations, the shorter modulus may not function properly with IKE, so Cisco recommends using a minimum modulus of 1024.)

Table 15 Sample Times Required to Generate RSA Keys

	Modulus Length			
Router	**360 bits**	**512 bits**	**1024 bits**	**2048 bits (maximum)**
Cisco 2500	11 seconds	20 seconds	4 minutes, 38 seconds	longer than 1 hour
Cisco 4700	less than 1 second	1 second	4 seconds	50 seconds

Examples

The following example generates special-usage RSA keys:

```
Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com

Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].

Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
```

```
Generating RSA keys.... [OK].
```

The following example generates general-purpose RSA keys. (You cannot generate both special-usage and general-purpose keys; you can generate only one or the other.)

```
Router(config)# crypto key generate rsa
The name for the keys will be: myrouter.example.com

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates the general-purpose RSA key pair “exampleCAkeys”:

```
crypto key generate rsa general-purpose exampleCAkeys
crypto ca trustpoint exampleCAkeys
 enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

Related Commands

Command	Description
show crypto ca timers	Specifies which key pair to associate with the certificate.

crypto key generate rsa (IKE)

To generate Rivest, Shamir, and Adelman (RSA) key pairs, use the **crypto key generate rsa** command in global configuration mode.

crypto key generate rsa {**general-keys** | **usage-keys**} [**label** *key-label*] **exportable** [**modulus** *modulus-size*]

Syntax Description

general-keys	Specifies that the general-purpose key pair should be generated.
usage-keys	Specifies that two RSA special-usage key pairs should be generated (that is, one encryption pair and one signature pair) instead of one general-purpose key pair.
label *key-label*	(Optional) Name that is used for an RSA key pair when they are being exported.
exportable	Specifies that the RSA key pair can be exported to another Cisco device, such as a router.
modulus *modulus-size*	(Optional) IP size of the key modulus in a range from 350 to 2048. If you do not enter the modulus keyword and specify a size, you will be prompted.

Defaults

RSA key pairs do not exist. If the **usage-keys** keyword is not used, general-purpose keys will be generated.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(15)T	The **usage-keys** and **exportable** keywords were added.

Usage Guidelines

Use this command to generate RSA key pairs for your Cisco device (such as a router).

RSA keys are generated in pairs—one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys.

Note Before issuing this command, ensure that your router has a host name and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a host name and IP domain name.

This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device).

There are two mutually exclusive types of RSA key pairs: special-usage keys and general-purpose keys. When you generate RSA key pairs, you can indicate whether to generate special-usage keys or general-purpose keys.

Special-Usage Keys

If you generate special-usage keys, two pairs of RSA keys will be generated. One pair will be used with any Internet Key Exchange (IKE) policy that specifies RSA signatures as the authentication method, and the other pair will be used with any IKE policy that specifies RSA encrypted keys as the authentication method.

If you plan to have both types of RSA authentication methods in your IKE policies, you may prefer to generate special-usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special-usage keys, one key is used for both authentication methods, increasing the exposure of that key.)

General-Purpose Keys

If you generate general-purpose keys, only one pair of RSA keys will be generated. This pair will be used with IKE policies specifying either RSA signatures or RSA encrypted keys. Therefore, a general-purpose key pair might get used more frequently than a special-usage key pair.

Modulus Length

When you generate RSA keys, you will be prompted to enter a modulus length. A longer modulus could offer stronger security but takes longer to generate (see Table 16 for sample times) and takes longer to use. A length of less than 512 is normally not recommended. (In certain situations, the shorter modulus may not function properly with IKE, so it is recommended that you use a minimum modulus of 1024.)

Table 16 Sample Times Required for Generating RSA Keys

	Modulus Length			
Router	**360 Bits**	**512 Bits**	**1024 Bits**	**2048 Bits**
Cisco 2500	11 seconds	20 seconds	4 minutes, 38 seconds	longer than 1 hour
Cisco 4700	less than 1 second	1 second	4 seconds	50 seconds

Examples

The following example generates special-usage RSA keys:

```
Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com

Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].

Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates general-purpose RSA keys:

Note You cannot generate both special-usage and general-purpose keys; you can generate only one or the other.

```
Router(config)# crypto key generate rsa
```

```
The name for the keys will be: myrouter.example.com

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

Related Commands

Command	Description
debug crypto engine	Displays debug messages about crypto engines.
hostname	Specifies or modifies the host name for the network server.
ip domain-name	Defines a default domain name to complete unqualified host names (names without a dotted-decimal domain name).
show crypto key mypubkey rsa	Displays the RSA public keys of your router.

crypto key import pem

To import Rivest, Shamir, and Adelman (RSA) keys in privacy-enhanced mail (PEM)-formatted files, use the **crypto key import pem** command in global configuration mode.

crypto key import rsa *key-label* **pem** [**usage-keys**] {**terminal** | **url** *url*} [**exportable**] *passphrase*

Syntax Description

rsa *key-label*	Name of the RSA key pair that will be imported. The *key-label* argument must match the key pair name that was specified via the **crypto key generate rsa** command.
usage-keys	(Optional) Specifies that two RSA special usage key pairs will be imported (that is, one encryption pair and one signature pair), instead of one general-purpose key pair.
terminal	Certificates and RSA key pairs will be manually imported to the console terminal.
url *url*	URL of the file system where your router should import certificates and RSA key pairs.
exportable	(Optional) Specifies that imported RSA key pair can be exported again to another Cisco device such as a router.
passphrase	Passphrase that is used to encrypt the PEM file for import. **Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **crypto key import pem** command allows you to import RSA key pairs in PEM-formatted files. The files can be previously exported from another Cisco IOS router or generated by other public key infrastructure (PKI) applications.

Examples

The following example shows how to generate, export, bring the key back (import), and verify the status of the RSA key pair "mycs":

```
! Generate the key pair
!
Router(config)# crypto key generate rsa general-purpose label mycs exportable
The name for the keys will be: mycs
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]
!
! Archive the key pair to a remote location, and use a good password.
!
Router(config)# crypto key export rsa mycs pem url nvram: 3des PASSWORD
% Key name: mycs
Usage: General Purpose Key
Exporting public key...
Destination filename [mycs.pub]?
Writing file to nvram:mycs.pub
Exporting private key...
Destination filename [mycs.prv]?
Writing file to nvram:mycs.prv
!
! Import the key as a different name.
!
Router(config)# crypto key import rsa mycs2 pem url nvram:mycs PASSWORD
% Importing public key or certificate PEM file...
Source filename [mycs.pub]?
Reading file from nvram:mycs.pub
% Importing private key PEM file...
Source filename [mycs.prv]?
Reading file from nvram:mycs.prv% Key pair import succeeded.
!
! After the key has been imported, it is no longer exportable.
!
! Verify the status of the key.
!
Router# show crypto key mypubkey rsa

% Key pair was generated at: 18:04:56 GMT Jun 6 2003
Key name: mycs
Usage: General Purpose Key
Key is exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
  9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
  A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
  A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
  C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
% Key pair was generated at: 18:17:25 GMT Jun 6 2003
Key name: mycs2
Usage: General Purpose Key
Key is not exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
  9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
  A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
  A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
  C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
```

Related Commands

Command	Description
crypto key export pem	Exports RSA keys in PEM-formatted files.
crypto key generate rsa	Generates RSA key pairs.

crypto key lock rsa

To lock the RSA private key in a router, use the **crypto key lock rsa** command in privileged EXEC mode.

crypto key lock rsa [**name** *key-name*] **passphrase** *passphrase*

Syntax Description

name *key-name*	(Optional) Name of the RSA key pair that is to be locked. The name must match the name that was specified via the **crypto key encrypt rsa** command.
passphrase *passphrase*	Passphrase that is used to lock the RSA key. The passphrase must match the passphrase that was specified via the **crypto key encrypt rsa** command.

Defaults

RSA keys are encrypted, but not locked.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When the **crypto key lock rsa** command is issued, the unencrypted copy of the key is deleted. Because the private key is not available, all RSA operations will fail.

This command affects only the "run-time" access to the key; that is, it does not affect the key that is stored in NVRAM.

Examples

The following example shows how to lock the key "pki1-72a.cisco.com." Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the key is protected (encrypted) and locked.

```
Router# crypto key lock rsa name pki1-72a.cisco.com passphrase cisco1234
!
Router# show crypto key mypubkey rsa

% Key pair was generated at:20:29:41 GMT Jun 20 2003
Key name:pki1-72a.cisco.com
Usage:General Purpose Key
*** The key is protected and LOCKED. ***
Key is exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D7808D C5FF14AC
0D2B55AC 5D199F2F 7CB4B355 C555E07B 6D0DECBE 4519B1F0 75B12D6F 902D6E9F
B6FDAD8D 654EF851 5701D5D7 EDA047ED 9A2A619D 5639DF18 EB020301 0001
```

Related Commands

Command	Description
crypto key encrypt rsa	Encrypts the RSA private key.
crypto key unlock rsa	Unlocks the RSA private key in a router.
show crypto key mypubkey rsa	Displays the RSA public keys of your router.

crypto key pubkey-chain rsa

To enter public key configuration mode (so you can manually specify other devices' RSA public keys), use the **crypto key pubkey-chain rsa** command in global configuration mode.

crypto key pubkey-chain rsa

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command to enter public key chain configuration mode. Use this command when you need to manually specify other IPSec peers' RSA public keys. You need to specify other peers' keys when you configure RSA encrypted nonces as the authentication method in an Internet Key Exchange policy at your peer router.

Examples

The following example specifies the RSA public keys of two other IPSec peers. The remote peers use their IP address as their identity.

```
Router(config)# crypto key pubkey-chain rsa
Router(config-pubkey-chain)# addressed-key 10.5.5.1
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# addressed-key 10.1.1.2
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 0738BC7A 2BC3E9F0 679B00FE 53987BCC
Router(config-pubkey)# 01030201 42DD06AF E228D24C 458AD228
Router(config-pubkey)# 58BB5DDD F4836401 2A2D7163 219F882E
Router(config-pubkey)# 64CE69D4 B583748A 241BED0F 6E7F2F16
Router(config-pubkey)# 0DE0986E DF02031F 4B0B0912 F68200C4
Router(config-pubkey)# C625C389 0BFF3321 A2598935 C1B1
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# exit
Router(config)#
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer you will manually configure.
addressed-key	Specifies the RSA public key of the peer you will manually configure.
key-string (IKE)	Specifies the RSA public key of a remote peer.
named-key	Specifies which peer RSA public key you will manually configure.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

crypto key unlock rsa

To unlock the RSA private key in a router, use the **crypto key unlock rsa** command in privileged EXEC mode.

crypto key unlock rsa [**name** *key-name*] **passphrase** *passphrase*

Syntax Description

name *key-name*	(Optional) Name of the RSA key pair that is to be unlocked. The name must match the name that was specified via the **crypto key encrypt rsa** command.
passphrase *passphrase*	Passphrase that is used to unlock the RSA key. The passphrase must match the passphrase that was specified via the **crypto key encrypt rsa** command.

Defaults

The encrypted private key is locked.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When a router with an encrypted RSA key (via the **crypto key encrypt rsa** command) initially boots up, the key does not exist in plain text and is therefore considered to be locked. Because the private key is not available, all RSA operations will fail. After you unlock the private key, RSA operations will function again.

This command affects only the “run-time” access to the key; that is, it does not affect the key that is stored in NVRAM.

Examples

The following example shows how to unlock the key “pki1-72a.cisco.com”:

```
Router# crypto key unlock rsa name pki1-72a.cisco.com passphrase cisco1234
```

Related Commands

Command	Description
crypto key encrypt rsa	Encrypts the RSA private key.
crypto key lock rsa	Locks the RSA private key in a router.
show crypto key mypubkey rsa	Displays the RSA public keys of your router.

crypto key zeroize rsa

To delete all RSA keys from your router, use the **crypto key zeroize rsa** command in global configuration mode.

crypto key zeroize rsa [*key-pair-label*]

Syntax Description

key-pair-label	(Optional) Specifies the name of the key pair that router will delete.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(8)T	The *key-pair-label* argument was added.

Usage Guidelines

This command deletes all Rivest, Shamir, and Adelman (RSA) keys that were previously generated by your router unless you include the *key-pair-label* argument, which will delete only the specified RSA key pair. If you issue this command, you must also perform two additional tasks for each trustpoint that is associated with the key pair that was deleted:

- Ask the certification authority (CA) administrator to revoke your router's certificates at the CA; you must supply the challenge password you created when you originally obtained the router's certificates using the **crypto ca enroll** command.
- Manually remove the router's certificates from the configuration by removing the configured trustpoint (using the **no crypto ca trustpoint** *name* command.)

Note This command cannot be undone (after you save your configuration), and after RSA keys have been deleted, you cannot use certificates or the CA or participate in certificate exchanges with other IP Security (IPSec) peers unless you reconfigure CA interoperability by regenerating RSA keys, getting the CA's certificate, and requesting your own certificate again.

This command is not saved to the configuration.

Examples

The following example deletes the general-purpose RSA key pair that was previously generated for the router. After deleting the RSA key pair, the administrator contacts the CA administrator and requests that the certificate of the router be revoked. The administrator then deletes the certificate of the router from the configuration.

```
crypto key zeroize rsa
crypto ca certificate chain
 no certificate
```

Related Commands

Command	Description
certificate	Adds certificates manually.
crypto ca certificate chain	Enters the certificate chain configuration mode.
crypto ca trustpoint	Declares the CA that your router should use.
show crypto ca timers	Specifies which key pair to associate with the certificate.

crypto keyring

To define a crypto keyring to be used during Internet Key Exchange (IKE) authentication, use the **crypto keyring** command in global configuration mode. To remove the keyring, use the **no** form of this command.

crypto keyring *keyring-name* [**vrf** *fvrf-name*]

no crypto keyring *keyring-name* [**vrf** *fvrf-name*]

Syntax Description

keyring-name	Name of the crypto keyring.
vrf *fvrf-name*	(Optional) Front door virtual routing and forwarding (FVRF) name to which the keyring will be referenced. The *fvrf-name* must match the FVRF name that was defined during virtual routing and forwarding (VRF) configuration.

Defaults

All the Internet Security Association and Key Management Protocol (ISAKMP) keys that were defined in the global configuration are part of the default global keyring.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

A keyring is a repository of preshared and Rivest, Shamir, and Adelman (RSA) public keys. The keyring is used in the isakmp profile configuration mode. The ISAKMP profile successfully completes authentication of peers if the peer keys are defined in the keyring that is attached to this profile.

Examples

The following example shows that a keyring and its usage have been defined:

```
crypto keyring vpnkeys
  pre-shared-key address 10.72.23.11 key vpnsecret
crypto isakmp profile vpnprofile
  keyring vpnkeys
```

crypto map (global IPSec)

To enter crypto map configuration mode and create or modify a crypto map entry, to create a crypto profile that provides a template for configuration of dynamically created crypto maps, or to configure a client accounting list, use the **crypto map** command in global configuration mode. To delete a crypto map entry, profile, or set, use the **no** form of this command.

crypto map *map-name seq-num* [**ipsec-manual**]

crypto map *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]

crypto map *map-name* [**client-accounting-list** *aaalist*]

no crypto map *map-name seq-num*

Note Issue the **crypto map** *map-name seq-num* command without a keyword to modify an existing crypto map entry.

Syntax Description

map-name	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
seq-num	Sequence number you assign to the crypto map entry. See additional explanation for using this argument in the "Usage Guidelines" section.
ipsec-manual	(Optional) Indicates that Internet Key Exchange (IKE) will not be used to establish the IP Security (IPSec) security associations (SAs) for protecting the traffic specified by this crypto map entry.
ipsec-isakmp	(Optional) Indicates that IKE will be used to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
dynamic	(Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. If you use this keyword, none of the crypto map configuration commands will be available.
dynamic-map-name	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.
discover	(Optional) Enables peer discovery. By default, peer discovery is not enabled.
profile	(Optional) Designates a crypto map as a configuration template. The security configurations of this crypto map will be cloned as new crypto maps are created dynamically on demand.
profile-name	(Optional) Name of the crypto profile being created.
client-accounting-list	(Optional) Designates a client accounting list.
aaalist	(Optional) List name.

Defaults

No crypto maps exist.

Peer discovery is not enabled.

Command Modes Global configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3 T	The following keywords and arguments were added: • **ipsec-manual** • **ipsec-isakmp** • **dynamic** • *dynamic-map-name*
12.0(5)T	The **discover** keyword was added to support Tunnel Endpoint Discovery (TED).
12.2(4)T	The **profile** *profile-name* keyword and argument combination was introduced to allow the generation of a crypto map profile that is cloned to create dynamically created crypto maps on demand.
12.2(11)T	Support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(15)T	The **client-accounting-list** keyword and *aaalist* argument were added.

Usage Guidelines Use this command to create a new crypto map entry, to create a crypto map profile, or to modify an existing crypto map entry or profile.

After a crypto map entry has been created, you cannot change the parameters specified at the global configuration level because these parameters determine which of the configuration commands are valid at the crypto map level. For example, after a map entry has been created using the **ipsec-isakmp** keyword, you cannot change it to the option specified by the **ipsec-manual** keyword; you must delete and reenter the map entry.

After you define crypto map entries, you can assign the crypto map set to interfaces using the **crypto map** (interface IPSec) command.

Crypto Map Functions

Crypto maps provide two functions: filtering and classifying traffic to be protected and defining the policy to be applied to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPSec crypto maps define the following:

- What traffic should be protected
- To which IPSec peers the protected traffic can be forwarded—these are the peers with which an SA can be established
- Which transform sets are acceptable for use with the protected traffic
- How keys and security associations should be used or managed (or what the keys are, if IKE is not used)

Multiple Crypto Map Entries with the Same Map Name Form a Crypto Map Set

A crypto map set is a collection of crypto map entries, each with a different *seq-num* argument but the same *map-name* argument. Therefore, for a given interface, you could have certain traffic forwarded to one IPSec peer with specified security applied to that traffic and other traffic forwarded to the same or a different IPSec peer with different IPSec security applied. To accomplish differential forwarding you would create two crypto maps, each with the same *map-name* argument, but each with a different *seq-num* argument. Crypto profiles must have unique names within a crypto map set.

Sequence Numbers

The number you assign to the *seq-num* argument should not be arbitrary. This number is used to rank multiple crypto map entries within a crypto map set. Within a crypto map set, a crypto map entry with a lower *seq-num* is evaluated before a map entry with a higher *seq-num*; that is, the map entry with the lower number has a higher priority.

For example, consider a crypto map set that contains three crypto map entries: mymap 10, mymap 20, and mymap 30. The crypto map set named "mymap" is applied to serial interface 0. When traffic passes through serial interface 0, the traffic is evaluated first for mymap 10. If the traffic matches any access list permit statement entry in the extended access list in mymap 10, the traffic will be processed according to the information defined in mymap 10 (including establishing IPSec SAs when necessary). If the traffic does not match the mymap 10 access list, the traffic will be evaluated for mymap 20, and then mymap 30, until the traffic matches a permit entry in a map entry. (If the traffic does not match a permit entry in any crypto map entry, it will be forwarded without any IPSec security.)

Dynamic Crypto Maps

Refer to the "Usage Guidelines" section of the **crypto dynamic-map** command for a discussion on dynamic crypto maps.

Crypto map entries that reference dynamic map sets should be the lowest priority map entries, allowing inbound SA negotiation requests to try to match the static maps first. Only after the request does not match any of the static maps, do you want it to be evaluated against the dynamic map set.

To make a crypto map entry referencing a dynamic crypto map set the lowest priority map entry, give the map entry the highest *seq-num* of all the map entries in a crypto map set.

Create dynamic crypto map entries using the **crypto dynamic-map** command. After you create a dynamic crypto map set, add the dynamic crypto map set to a static crypto map set with the **crypto map** (global IPSec) command using the **dynamic** keyword.

TED

TED is an enhancement to the IPSec feature. Defining a dynamic crypto map allows you to dynamically determine an IPSec peer; however, only the receiving router has this ability. With TED, the initiating router can dynamically determine an IPSec peer for secure IPSec communications.

Dynamic TED helps to simplify IPSec configuration on the individual routers within a large network. Each node has a simple configuration that defines the local network that the router is protecting and the IPSec transforms that are required.

Note TED helps only in discovering peers; otherwise, TED does not function any differently from normal IPSec. Thus, TED does not improve the scalability of IPSec (in terms of performance or the number of peers or tunnels).

Crypto Map Profiles

Crypto map profiles are created using the **profile** *profile-name* keyword and argument combination. Crypto map profiles are used as configuration templates for dynamically creating crypto maps on demand for use with the Layer 2 Transport Protocol (L2TP) Security feature. The relevant SAs the crypto map profile will be cloned and used to protect IP traffic on the L2TP tunnel.

Note The **set peer** and **match address** commands are ignored by crypto profiles and should not be configured in the crypto map definition.

Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the SAs:

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
```

The following example shows the minimum required crypto map configuration when the SAs are manually established:

```
crypto transform-set someset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
 match address 102
 set transform-set someset
 set peer 10.0.0.5
 set session-key inbound ah 256 98765432109876549876543210987654
 set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc
 set session-key inbound esp 256 cipher 0123456789012345
 set session-key outbound esp 256 cipher abcdefabcdefabcd
```

The following example configures an IPSec crypto map set that includes a reference to a dynamic crypto map set.

Crypto map “mymap 10” allows SAs to be established between the router and either (or both) of two remote IPSec peers for traffic matching access list 101. Crypto map “mymap 20” allows either of two transform sets to be negotiated with the remote peer for traffic matching access list 102.

Crypto map entry “mymap 30” references the dynamic crypto map set “mydynamicmap,” which can be used to process inbound SA negotiation requests that do not match “mymap” entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in “mydynamicmap,” for a flow permitted by the access list 103, IPSec will accept the request and set up SAs with the remote peer without previously knowing about the remote peer. If the request is accepted, the resulting SAs (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with “mydynamicmap 10” is also used as a filter. Inbound packets that match any access list permit statement in this list are dropped for not being IPSec protected. (The same is true for access lists associated with static crypto maps entries.) Outbound packets that match a permit statement without an existing corresponding IPSec SA are also dropped.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
crypto map mymap 20 ipsec-isakmp
 match address 102
```

```
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
 match address 103
 set transform-set my_t_set1 my_t_set2 my_t_set3
```

The following example configures TED on a Cisco router:

```
crypto map testtag 10 ipsec-isakmp dynamic dmap discover
```

The following example configures a crypto profile to be used as a template for dynamically created crypto maps when IPSec is used to protect an L2TP tunnel:

```
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto isakmp profile	Audits IPSec user sessions.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
debug crypto isakmp	Applies a previously defined crypto map set to an interface.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for PFS when requesting new SAs for this crypto map entry, or that IPSec requires PFS when receiving requests for new SAs.
set security-association level per-host	Specifies that separate IPSec SAs should be requested for each source/destination host pair.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec SAs.
set session-key	Specifies the IPSec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

crypto map (interface IPSec)

To apply a previously defined crypto map set to an interface, use the **crypto map** command in interface configuration mode. To remove the crypto map set from the interface, use the **no** form of this command.

crypto map *map-name* [**redundancy** *standby-group-name*[**stateful**]]

no crypto map [*map-name*] [**redundancy** *standby-group-name* [**stateful**]]

Syntax Description

map-name	Name that identifies the crypto map set. This is the name assigned when the crypto map was created. When the **no** form of the command is used, this argument is optional. Any value supplied for the argument is ignored.
redundancy	(Optional) Defines a backup IP Security (IPSec) peer. Both routers in the standby group are defined by the redundancy *standby name* and share the same virtual IP address.
standby-group-name	(Optional) Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands.
stateful	(Optional) Enables IPSec stateful failover for the crypto map.

Defaults

No crypto maps are assigned to interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.1(9)E	The **redundancy** keyword and *standby-name* argument were added.
12.2(8)T	The **redundancy** keyword and *standby-name* argument were integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.3(11)T	The **stateful** keyword was added.

Usage Guidelines

Use this command to assign a crypto map set to an interface. You must assign a crypto map set to an interface before that interface can provide IPSec services. Only one crypto map set can be assigned to an interface. If multiple crypto map entries have the same map name but a different sequence number, they are considered to be part of the same set and will all be applied to the interface. The crypto map entry that has the lowest sequence number is considered the highest priority and will be evaluated first. A single crypto map set can contain a combination of **ipsec-isakmp** and **ipsec-manual crypto map** entries.

The standby name must be configured on all devices in the standby group, and the standby address must be configured on at least one member of the group. If the standby name is removed from the router, the IPSec security associations (SAs) will be deleted. If the standby name is added again, regardless of whether the same name or a different name is used, the crypto map (using the **redundancy** option) will have to be reapplied to the interface.

Note A virtual IP address must be configured in the standby group to enable either stateless or stateful redundancy.

The **stateful** keyword enables stateful failover of IKE and IPSec sessions. Stateful Switchover (SSO) must also be configured for IPSec stateful failover to operate correctly.

Examples

The following example shows how all remote Virtual Private Network (VPN) gateways connect to the router via 192.168.0.3:

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102

Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

The crypto map on the interface binds this standby address as the local tunnel endpoint for all instances of “mymap” and, at the same time, ensures that stateless HSRP failover is facilitated between an active and standby device that belongs to the same standby group, “group1.”

Reverse route injection (RRI) is also enabled to provide the ability for only the *active* device in the HSRP group to be advertising itself to inside devices as the next hop VPN gateway to the remote proxies. If a failover occurs, routes are deleted on the former active device and created on the new active device.

The following example shows how to configure IPSec stateful failover on the crypto map “to-peer-outside”:

```
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
 match address peer-outside

interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 crypto map to-peer-outside redundancy HA-out stateful
```

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
redundancy inter-device	Configures redundancy and enters inter-device configuration mode.
show crypto map (IPSec)	Displays the crypto map configuration.
standby ip	Assigns an IP address that is to be shared among the members of the HSRP group and owned by the primary IP address.
standby name	Assigns a user-defined group name to the HSRP redundancy group.

crypto map client authentication list

To configure Internet Key Exchange extended authentication (Xauth) on your router, use the **crypto map client authentication list** command in global configuration mode. To restore the default value, use the **no** form of this command.

crypto map *map-name* **client authentication list** *list-name*

no crypto map *map-name* **client authentication list** *list-name*

Syntax Description

map-name	The name you assign to the crypto map set.
list-name	Character string used to name the list of authentication methods activated when a user logs in. The list-name must match the list-name defined during AAA configuration.

Defaults

Xauth is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

Before configuring Xauth, you should complete the following tasks:

- Set up an authentication list using AAA commands.
- Configure an IP Security transform.
- Configure a crypto map.
- Configure Internet Security Association Key Management Protocol (ISAKMP) policy.

After enabling Xauth, you should apply the crypto map on which Xauth is configured to the router interface.

Examples

The following example configures user authentication (a list of authentication methods called *xauthlist*) on an existing static crypto map called *xauthmap*:

```
crypto map xauthmap client authentication list xauthlist
```

The following example configures user authentication (a list of authentication methods called *xauthlist*) on a dynamic crypto map called *xauthdynamic* that has been applied to a static crypto map called *xauthmap*:

```
crypto map xauthmap client authentication list xauthlist
crypto map xauthmap 10 ipsec-isakmp dynamic xauthdynamic
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.
crypto ipsec transform-set	Defines a transform set, which is an acceptable combination of security protocols and algorithms, and enters crypto transform configuration mode.
crypto isakmp key	Configures a preshared authentication key.
crypto isakmp policy	Defines an IKE policy, and enters ISAKMP policy configuration mode.
crypto map (global configuration)	Creates or modify a crypto map entry, and enters the crypto map configuration mode.
interface	Enters the interface configuration mode.

crypto map client configuration address

To configure IKE Mode Configuration on your router, use the **crypto map client configuration address** command in global configuration mode. To disable IKE Mode Configuration, use the **no** form of this command.

crypto map *tag* **client configuration address** [**initiate** | **respond**]

no crypto map *tag* **client configuration address**

Syntax Description

tag	The name that identifies the crypto map.
initiate	(Optional) A keyword that indicates the router will attempt to set IP addresses for each peer.
respond	(Optional) A keyword that indicates the router will accept requests for IP addresses from any requesting peer.

Defaults

IKE Mode Configuration is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XE	This command was introduced.
12.0(7)T	This command was implemented in Cisco IOS release 12.0(7)T.

Usage Guidelines

At the time of this publication, this feature is an IETF draft with limited support. Therefore this feature was not designed to enable the configuration mode for every IKE connection by default.

Examples

The following examples configure IKE Mode Configuration on your router:

```
crypto map dyn client configuration address initiate
crypto map dyn client configuration address respond
```

Related Commands

Command	Description
crypto map (global)	Creates or modifies a crypto map entry and enters the crypto map configuration mode

crypto map isakmp authorization list

To enable Internet Key Exchange (IKE) querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode, use the **crypto map isakmp authorization list** command in global configuration mode. To restore the default value, use the **no** form of this command.

crypto map *map-name* **isakmp authorization list** *list-name*

no crypto map *map-name* **isakmp authorization list** *list-name*

Syntax Description

map-name	Name you assign to the crypto map set.
list-name	Character string used to name the list of authorization methods activated when a user logs in. The list name must match the list name defined during AAA configuration.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced

Usage Guidelines

Use the **crypto map client authorization list** command to enable key lookup from a AAA server.

Preshared keys deployed in a large-scale Virtual Private Network (VPN) without a certification authority, with dynamic IP addresses, are accessed during aggression mode of IKE negotiation through a AAA server. Thus, users have their own key, which is stored on an external AAA server. This allows for central management of the user database, linking it to an existing database, in addition to allowing every user to have their own unique, more secure pre-shared key.

Before configuring the **crypto map client authorization list** command, you should perform the following tasks:

- Set up an authorization list using AAA commands.
- Configure an IPSec transform.
- Configure a crypto map.
- Configure an Internet Security Association Key Management Protocol policy using IPSec and IKE commands.

After enabling the **crypto map client authorization list** command, you should apply the previously defined crypto map to the interface.

Examples

The following example shows how to configure the **crypto map client authorization list** command:

```
crypto map ikessaaamap isakmp authorization list ikessaaalist
```

```
crypto map ikessaaamap 10 ipsec-isakmp dynamic ikessaaadyn
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict a user's network access.
crypto ipsec transform-set	Defines a transform set, which is an acceptable combination of security protocols and algorithms, and enters crypto transform configuration mode.
crypto map (global configuration)	Creates or modifies a crypto map entry and enters the crypto map configuration mode
crypto isakmp policy	Defines an IKE policy and enters ISAKMP policy configuration mode.
crypto isakmp key	Configures a preshared authentication key.
interface	Enters interface configuration mode.

crypto map isakmp-profile

To configure an Internet Security Association and Key Management Protocol (ISAKMP) profile on a crypto map, use the **crypto map isakmp-profile** command in global configuration mode. To restore the default values on the crypto map, use the **no** form of this command.

crypto map *map-name* **isakmp-profile** *isakmp-profile-name*

no crypto map *map-name* **isakmp-profile** *isakmp-profile-name*

Syntax Description

map-name	Name assigned to the crypto map set.
isakmp-profile-name	Character string used to name the ISAKMP profile that is used during an Internet Key Exchange (IKE) Phase 1 and Phase 1.5 exchange. The *isakmp-profile-name* must match the ISAKMP profile name that was defined during the ISAKMP profile configuration.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command describes the ISAKMP profile to use to start the IKE exchange. Before configuring this command, you must set up the ISAKMP profile.

Examples

The following example shows that an ISAKMP profile is configured on a crypto map:

```
crypto map vpnmap isakmp-profile vpnprofile
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set—an acceptable combination of security protocols and algorithms.
crypto map (global)	Creates or modifies a crypto map entry.

crypto map local-address

To specify and name an identifying interface to be used by the crypto map for IPSec traffic, use the **crypto map local-address** command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

crypto map *map-name* **local-address** *interface-id*

no crypto map *map-name* **local-address**

Syntax Description

map-name	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
interface-id	The identifying interface that should be used by the router to identify itself to remote peers. If Internet Key Exchange is enabled and you are using a certification authority (CA) to obtain certificates, this should be the interface with the address specified in the CA certificates.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

If you apply the same crypto map to two interfaces and do not use this command, two separate security associations (with different local IP addresses) could be established to the same peer for similar traffic. If you are using the second interface as redundant to the first interface, it could be preferable to have a single security association (with a single local IP address) created for traffic sharing the two interfaces. Having a single security association decreases overhead and makes administration simpler.

This command allows a peer to establish a single security association (and use a single local IP address) that is shared by the two redundant interfaces.

If applying the same crypto map set to more than one interface, the default behavior is as follows:

- Each interface will have its own security association database.
- The IP address of the local interface will be used as the local address for IPSec traffic originating from/destined to that interface.

However, if you use a local-address for that crypto map set, it has multiple effects:

- Only one IPSec security association database will be established and shared for traffic through both interfaces.
- The IP address of the specified interface will be used as the local address for IPSec (and IKE) traffic originating from or destined to that interface.

One suggestion is to use a loopback interface as the referenced local address interface, because the loopback interface never goes down.

Examples

The following example assigns crypto map set "mymap" to the S0 interface and to the S1 interface. When traffic passes through either S0 or S1, the traffic will be evaluated against the all the crypto maps in the "mymap" set. When traffic through either interface matches an access list in one of the "mymap" crypto maps, a security association will be established. This same security association will then apply to both S0 and S1 traffic that matches the originally matched IPSec access list. The local address that IPSec will use on both interfaces will be the IP address of interface loopback0.

```
interface S0
 crypto map mymap

interface S1
 crypto map mymap

crypto map mymap local-address loopback0
```

Related Commands

Command	Description
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.

crypto map redundancy replay-interval

To modify the interval at which inbound and outbound replay updates are passed from an active device to a standby device, use the **crypto map redundancy replay-interval** command in global configuration mode. To return to the default functionality, use the **no** form of this command.

crypto map *map-name* **redundancy replay-interval inbound** *in-value* **outbound** *out-value*

no crypto map *map-name* **redundancy replay-interval inbound** *in-value* **outbound** *out-value*

Syntax Description

map-name	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
inbound *in-value*	Number of inbound packets that are processed before an anti-replay update is sent from the active router to the standby router.
outbound *out-value*	Number of outbound packets that are processed before an anti-replay update is sent from the active router to the standby router.

Defaults

inbound *in-value*: one update every 1,000 packets

outbound *out-value*: one update every 100,000 packets

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Note This command can be used only in conjunction with IPSec stateful failover on a crypto map.

Stateful failover enables a router to continue processing and forwarding packets after a planned or unplanned outage occurs; that is, a backup (secondary) router automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason.

The **crypto map redundancy replay-interval** command allows you to modify the interval in which an IP redundancy-enabled crypto map sends anti-replay updates from the active router to the standby router.

Examples

The following example shows how to enable replay checking for the crypto map "to-peer-outside" and enable IPSec stateful failover:

```
crypto map to-peer-outside redundancy replay-interval inbound 1000 outbound 10000
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
```

```
 match address peer-outside
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
```

crypto map to-peer-outside redundancy HA-out stateful

crypto mib ipsec flowmib history failure size

To change the size of the IP Security (IPSec) MIB failure history table, use the **crypto mib ipsec flowmib history failure size** command in global configuration mode.

crypto mib ipsec flowmib history failure size *number*

Syntax Description

number	Size of the failure history table. The default value is 200.

Defaults

The default table size is 200.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2 T.

Usage Guidelines

Use the **crypto mib ipsec flowmib history failure size** command to change the size of a failure history table. If you do not configure the size of a failure history table, the default of 200 will be implemented.

A failure history table stores the reason for tunnel failure and the time failure occurred. A failure history table can be used as a simple method to distinguish between a normal and an abnormal tunnel termination. That is, if a tunnel entry in the tunnel history table has no associated failure record, the tunnel must have terminated normally. However, every failure does not correspond to a tunnel. Supported setup failures are recorded in the failure table, but a history table is not associated because a tunnel was never set up.

Examples

In the following example, the size of a failure history table is configured to be 140:

```
Router(config)# crypto mib ipsec flowmib history failure size 140
```

Related Commands

Command	Description
crypto mib ipsec flowmib history tunnel size	Changes the size of the IPSec tunnel history table.
show crypto mib ipsec flowmib history failure size	Displays the size of the IPSec failure history table.

crypto mib ipsec flowmib history tunnel size

To change the size of the IP Security (IPSec) tunnel history table, use the **crypto mib ipsec flowmib history tunnel size** command in global configuration mode.

crypto mib ipsec flowmib history tunnel size *number*

Syntax Description

number	Size of the tunnel history table. The default value is 200.

Defaults

The default table size is 200.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2 T.

Usage Guidelines

Use the **crypto mib ipsec flowmib history tunnel size** command to change the size of a tunnel history table. If you do not configure the size of a tunnel history table, the default of 200 will be implemented.

A tunnel history table stores the attribute and statistics records, which contain the attributes and the last snapshot of the traffic statistics of a given tunnel. A tunnel history table accompanies a failure table, so you can display the complete history of a given tunnel. However, a tunnel history table does not accompany every failure table because every failure does not correspond to a tunnel. Thus, supported setup failures are recorded in the failure table, but an associated history table is not recorded because a tunnel was never set up.

As an optimization, a tunnel endpoint table can be combined with a tunnel history table. However, if a tunnel endpoint table is combined, all three tables (the failure history table, tunnel history table, and the endpoint table) must remain the same size even though the MIB allows each table to be distinct.

Examples

In the following example, the size of the tunnel history table changed to 130:

```
Router(config)# crypto mib ipsec flowmib history tunnel size 130
```

crypto pki authenticate

To authenticate the certification authority (by getting the certificate of the CA), use the **crypto pki authenticate** command in global configuration mode.

crypto pki authenticate *name*

Syntax Description

name	Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	The **crypto ca authenticate** command was introduced.
12.3(7)T	This command replaced the **crypto ca authenticate** command.

Usage Guidelines

This command is required when you initially configure CA support at your router.

This command authenticates the CA to your router by obtaining the self-signed certificate of the CA that contains the public key of the CA. Because the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator when you perform this command.

If you are using RA mode (using the **enrollment mode ra** command) when you issue the **crypto pki authenticate** command, then registration authority signing and encryption certificates will be returned from the CA as well as the CA certificate.

This command is not saved to the router configuration. However. the public keys embedded in the received CA (and RA) certificates are saved to the configuration as part of the RSA public key record (called the "RSA public key chain").

Note If the CA does not respond by a timeout period after this command is issued, the terminal control will be returned so it will not be tied up. If this happens, you must re-enter the command. Cisco IOS software will not recognize CA certificate expiration dates set for beyond the year 2049. If the validity period of the CA certificate is set to expire after the year 2049, the following error message will be displayed when authentication with the CA server is attempted:

```
error retrieving certificate :incomplete chain
```

If you receive an error message similar to this one, check the expiration date of your CA certificate. If the expiration date of your CA certificate is set after the year 2049, you must reduce the expiration date by a year or more.

Examples

In the following example, the router requests the certificate of the CA. The CA sends its certificate and the router prompts the administrator to verify the certificate of the CA by checking the CA certificate's fingerprint. The CA administrator can also view the CA certificate's fingerprint, so you should compare what the CA administrator sees to what the router displays on the screen. If the fingerprint on the router's screen matches the fingerprint viewed by the CA administrator, you should accept the certificate as valid.

```
Router(config)# crypto pki authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
```

Related Commands

Command	Description
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
show crypto pki certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto pki cert validate

To determine if a trustpoint has been successfully authenticated, a certificate has been requested and granted, and if the certificate is currently valid, use the **crypto pki cert validate** command in global configuration mode.

crypto pki cert validate *trustpoint*

Syntax Description

trustpoint	The trustpoint to be validated.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced. Also, effective with Cisco IOS Release 12.3(8)T, this command replaced the **crypto ca cert validate** command.

Usage Guidelines

The **crypto pki cert validate** command validates the router's own certificate for a given trustpoint. Use this command as a sanity check after enrollment to verify that the trustpoint is properly authenticated, a certificate has been requested and granted for the trustpoint, and that the certificate is currently valid. A certificate is valid if it is signed by the trustpoint certification authority (CA), not expired, and so on.

Examples

The following examples show the possible output from the **crypto pki cert validate** command:

```
Router(config)# crypto pki cert validate ka

Validation Failed: trustpoint not found for ka


Router(config)# crypto pki cert validate ka

Validation Failed: can't get local certificate chain


Router(config)# crypto pki cert validate ka

Certificate chain has 2 certificates.
Certificate chain for ka is valid


Router(config)# crypto pki cert validate ka

Certificate chain has 2 certificates.
Validation Error: no certs on chain
```

```
Router(config)# crypto pki cert validate ka

Certificate chain has 2 certificates.
Validation Error: unspecified error
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the certification authority that the router should use.
show crypto pki trustpoints	Displays the trustpoints that are configured in the router.

crypto pki certificate chain

To enter the certificate chain configuration mode, use the **crypto pki certificate chain** command in global configuration mode. (You need to be in certificate chain configuration mode to delete certificates.)

crypto pki certificate chain *name*

Syntax Description

name	Specifies the name of the CA. Use the same name as when you declared the CA using the **crypto pki trustpoint** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	The **crypto ca certificate chain** command was introduced.
12.3(7)T	This command replaced the **crypto ca certificate chain** command.

Usage Guidelines

This command puts you into certificate chain configuration mode. When you are in certificate chain configuration mode, you can delete certificates using the **certificate** command.

Examples

The following example deletes the router's certificate. In this example, the router had a general-purpose RSA key pair with one corresponding certificate. The show command is used to determine the serial number of the certificate to be deleted.

```
Router# show crypto pki certificates

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set

Router# configure terminal
Rrouter(config)# crypto pki certificate chain myca
Router(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
Router(config-cert-chain)# exit
```

Related Commands

Command	Description
certificate	Adds certificates manually.

crypto pki certificate map

To define certificate-based access control lists (ACLs), use the **crypto pki certificate map** command in ca-certificate-map configuration mode. To remove the certificate-based ACLs, use the **no** form of this command.

crypto pki certificate map *label sequence-number*

no crypto pki certificate map *label sequence-number*

Syntax Description

label	A user-specified label that is referenced within the **crypto pki trustpoint** command.
sequence-number	A number that orders the ACLs with the same label. ACLs with the same label are processed from lowest to highest sequence number. When an ACL is matched, processing stops with a successful result.

Defaults

No default behavior or value.

Command Modes

Ca-certificate-map configuration

Command History

Release	Modification
12.2(15)T	The **crypto ca certificate map** command was introduced.
12.3(7)T	This command replaced the **crypto ca certificate map** command.

Usage Guidelines

Issuing this command places the router in CA certificate map configuration mode where you can specify several certificate fields together with their matching criteria. The general form of these fields is as follows:

```
field-name match-criteria match-value
```

The *field-name* in the above example is one of the certificate fields. Field names are similar to the names used in the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) X.509 standard. The **name** field is a special field that matches any subject name or related name field in the certificate, such as the **alt-subject-name, subject-name**, and **unstructured-subject-name** fields.

- **alt-subject-name**—Case-insensitive string.
- **expires-on**—Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.
- **issuer-name**—Case-insensitive string.
- **name**—Case-insensitive string.
- **subject-name**—Case-insensitive string.
- **unstructured-subject-name**—Case-insensitive string.
- **valid-start**—Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.

Note The time portion is optional in both the **expires-on** date and **valid-start** field and defaults to 00:00:00 if not specified. The time is interpreted according to the time zone offset configured for the router. The string **utc** can be appended to the date and time when they are configured as Universal Time, Coordinated (UTC) rather than local time.

The *match-criteria* in the example is one of the following logical operators:

- **eq**—equal (valid for name and date fields)
- **ne**—not equal (valid for name and date fields)
- **co**—contains (valid only for name fields)
- **nc**—does not contain (valid only for name fields)
- **lt**—less than (valid only for date fields)
- **ge**—greater than or equal to (valid only for date fields)

The *match-value* is a case-insensitive string or a date.

Examples

The following example shows how to configure a certificate-based ACL that will allow any certificate issued by Cisco Systems to an entity within the cisco.com domain. The label is Cisco, and the sequence is 10.

```
crypto pki certificate map Cisco 10
 issuer-name co Cisco Systems
 unstructured-subject-name co cisco.com
```

The following example accepts any certificate issued by Cisco Systems for an entity with DIAL or organizationUnit component ou=WAN. This certificate-based ACL consists of two separate ACLs tied together with the common label Group. Because the check for DIAL has a lower sequence number, it is performed first. Note that the string "DIAL" can occur anywhere in the subjectName field of the certificate, but the string WAN must be in the organizationUnit component.

```
crypto pki certificate map Group 10
 issuer-name co Cisco Systems
 subject-name co DIAL
crypto pki certificate map Group 20
 issuer-name co Cisco Systems
 subject-name co ou=WAN
```

Case is ignored in string comparisons; therefore, DIAL in the previous example will match dial, DIAL, Dial, and so on. Also note that the component identifiers (o=, ou=, cn=, and so on) are not required unless it is desirable that the string to be matched occurs in a specific component of the name. (Refer to the ITU-T security standards for more information about certificate fields and components such as ou=.)

If a component identifier is specified in the match string, the exact string, including the component identifier, must appear in the certificate. This requirement can present a problem if more than one component identifier is included in the match string. For example, "ou=WAN,o=Cisco Systems" will not match a certificate with the string "ou=WAN,ou=Engineering,o=Cisco Systems" because the "ou=Engineering" string separates the two desired component identifiers.

To match both "ou=WAN" and "o=Cisco Systems" in a certificate while ignoring other component identifiers, you could use this certificate map:

```
crypto pki certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
```

Any space character proceeding or following the equal sign (=) character in component identifiers is ignored. Therefore “o=Cisco” in the proceeding example will match “o = Cisco,” “o= Cisco,” “o =Cisco,” and so on.

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

crypto pki certificate query (ca-trustpoint)

To specify that certificates should not be stored locally but retrieved from a certification authority (CA) trustpoint, use the **crypto pki certificate query** command in ca-trustpoint configuration mode. To cause certificates to be stored locally per trustpoint, use the **no** form of this command.

crypto pki certificate query

no crypto pki certificate query

Syntax Description

This command has no arguments or keywords.

Defaults

CA trustpoints are stored locally in the router's NVRAM.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	The **crypto ca certificate query (ca-trustpoint)** command was introduced.
12.3(7)T	This command replaced the **crypto ca certificate query (ca-trustpoint)** command.

Usage Guidelines

Normally, certain certificates are stored locally in the router's NVRAM, and each certificate uses a moderate amount of memory. To save NVRAM space, you can use this command to put the router into query mode, preventing certificates from being stored locally; instead, they are retrieved from a specified CA trustpoint when needed. This will save NVRAM space but could result in a slight performance impact.

The **crypto pki certificate query** command is a subcommand for each trustpoint; thus, this command can be disabled on a per-trustpoint basis.

Before you can configure this command, you must enable the **crypto pki trustpoint** command, which puts you in ca-trustpoint configuration mode.

Note This command deprecates the **crypto ca certificate query** command in global configuration mode. Although you can still enter the global configuration command, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to prevent certificates and certificate revocation lists (CRLs) from being stored locally on the router; instead, they are retrieved from the "ka" trustpoint when needed.

```
crypto pki trustpoint ka
 .
 .
 .
```

```
crypto pki certificate query
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

crypto pki crl request

To request that a new certificate revocation list (CRL) be obtained immediately from the certification authority, use the **crypto pki crl request** command in global configuration mode.

crypto pki crl request *name*

Syntax Description

name	Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto pki trustpoint** command.

Defaults

Normally, the router requests a new CRL only after the existing one expires.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	The **crypto ca crl request** command was introduced.
12.3(7)T	This command replaced the **crypto ca crl request** command.

Usage Guidelines

A CRL lists all the network's devices' certificates that have been revoked. Revoked certificates will not be honored by your router; therefore, any IPSec device with a revoked certificate cannot exchange IP Security traffic with your router.

The first time your router receives a certificate from a peer, it will download a CRL from the CA. Your router then checks the CRL to make sure the peer's certificate has not been revoked. (If the certificate appears on the CRL, it will not accept the certificate and will not authenticate the peer.)

A CRL can be reused with subsequent certificates until the CRL expires. If your router receives a peer's certificate after the applicable CRL has expired, it will download the new CRL.

If your router has a CRL which has not yet expired, but you suspect that the CRL's contents are out of date, use the **crypto pki crl request** command to request that the latest CRL be immediately downloaded to replace the old CRL.

This command is not saved to the configuration.

Examples

The following example immediately downloads the latest CRL to your router:

```
crypto pki crl request
```

crypto pki enroll

To obtain the certificate(s) of your router from the certification authority, use the **crypto pki enroll** command in global configuration mode. To delete a current enrollment request, use the **no** form of this command.

crypto pki enroll *name*

no crypto pki enroll *name*

Syntax Description

name	Specifies the name of the CA. Use the same name as when you declared the CA using the **crypto pki trustpoint** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	The **crypto ca enroll** command was introduced.
12.3(7)T	This command replaced the **crypto ca enroll** command.

Usage Guidelines

This command requests certificates from the CA for all of your router's RSA key pairs. This task is also known as enrolling with the CA. (Technically, enrolling and obtaining certificates are two separate events, but they both occur when this command is issued.)

Your router needs a signed certificate from the CA for each RSA key pairs of your router; if you previously generated general purpose keys, this command will obtain the one certificate corresponding to the one general purpose RSA key pair. If you previously generated special usage keys, this command will obtain two certificates corresponding to each of the special usage RSA key pairs.

If you already have a certificate for your keys you will be unable to complete this command; instead, you will be prompted to remove the existing certificate first. (You can remove existing certificates with the **no certificate** command.)

The **crypto pki enroll** command is not saved in the router configuration.

Note If your router reboots after you issue the **crypto pki enroll** command but before you receive the certificate(s), you must reissue the command.

Responding to Prompts

When you issue the **crypto pki enroll** command, you are prompted a number of times.

First, you are prompted to create a challenge password. This password can be up to 80 characters in length. This password is necessary in the event that you ever need to revoke your router's certificate(s). When you ask the CA administrator to revoke your certificate, you must supply this challenge password as a protection against fraudulent or mistaken revocation requests.

Note This password is not stored anywhere, so you need to remember this password.

If you lose the password, the CA administrator may still be able to revoke the router's certificate but will require further manual authentication of the router administrator identity.

You are also prompted to indicate whether or not your router's serial number should be included in the obtained certificate. The serial number is not used by IP Security or Internet Key Exchange but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular router. (Note that the serial number stored is the serial number of the internal board, not the one on the enclosure.) Ask your CA administrator if serial numbers should be included. If you are in doubt, include the serial number.

Normally, you would not include the IP address because the IP address binds the certificate more tightly to a specific entity. Also, if the router is moved, you would need to issue a new certificate. Finally, a router has multiple IP addresses, any of which might be used with IPSec.

If you indicate that the IP address should be included, you will then be prompted to specify the interface of the IP address. This interface should correspond to the interface that you apply your crypto map set to. If you apply crypto map sets to more than one interface, specify the interface that you name in the **crypto map local-address** command.

Examples

In the following example, a router with a general-purpose RSA key pair requests a certificate from the CA. When the router displays the certificate fingerprint, the administrator verifies this number by calling the CA administrator, who checks the number. The fingerprint is correct, so the router administrator accepts the certificate.

There can be a delay between when the router administrator sends the request and when the certificate is actually received by the router. The amount of delay depends on the CA method of operation.

```
Router(config)# crypto pki enroll myca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: <mypassword>
Re-enter password: <mypassword>

% The subject name in the certificate will be: myrouter.example.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 03433678
% Include an IP address in the subject name [yes/no]? yes
Interface: ethernet0/0
Request certificate from CA [yes/no]? yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificates' command will also show the fingerprint.
```

Some time later, the router receives the certificate from the CA and displays the following confirmation message:

```
Router(config)#   Fingerprint: 01234567 89ABCDEF FEDCBA98 75543210

%CRYPTO-6-CERTRET: Certificate received from Certificate Authority

Router(config)#
```

If necessary, the router administrator can verify the displayed Fingerprint with the CA administrator.

If there is a problem with the certificate request and the certificate is not granted, the following message is displayed on the console instead:

```
%CRYPTO-6-CERTREJ: Certificate enrollment request was rejected by Certificate Authority
```

The subject name in the certificate is automatically assigned to be the same as the RSA key pair's name. In the above example, the RSA key pair was named "myrouter.example.com." (The router assigned this name.)

Requesting certificates for a router with special usage keys would be the same as the previous example, except that two certificates would have been returned by the CA. When the router received the two certificates, the router would have displayed the same confirmation message:

```
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
```

Related Commands

Command	Description
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the router.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
show crypto pki certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto pki export pem

To export certificates and Rivest, Shamir, and Adelman (RSA) keys that are associated with a trustpoint in a privacy-enhanced mail (PEM)-formatted file, use the **crypto pki export pem** command in global configuration mode.

crypto pki export *trustpoint* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase*

Syntax Description

trustpoint	Name of the trustpoint that the associated certificate and RSA key pair will export. The *trustpoint* argument must match the name that was specified via the **crypto pki trustpoint** command.
terminal	Certificate and RSA key pair that will be displayed in PEM format on the console terminal.
url *url*	URL of the file system where your router should export the certificate and RSA key pairs.
3des	Export the trustpoint using the Triple Data Encryption Standard (3DES) encryption algorithm.
des	Export the trustpoint using the DES encryption algorithm.
passphrase	Passphrase that is used to encrypt the PEM file for import. **Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	The **crypto ca export pem** command was introduced.
12.3(7)T	This command replaced the **crypto ca export pem** command.

Usage Guidelines

The **crypto pki export pem** command allows you to export certificate and RSA key pairs in PEM-formatted files. The PEM files can then be imported back into the Cisco IOS router (via the **crypto pki import pem** command) or other public key infrastructure (PKI) applications.

Examples

The following example shows how to generate and export the RSA key pair "aaa" and certificates of the router in PEM files that are associated with the trustpoint "mycs":

```
Router(config)# crypto key generate rsa general-keys label aaa exportable
The name for the keys will be:aaa
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
!
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
!
Router(config)# crypto pki trustpoint mycs
Router(ca-trustpoint)# enrollment url http://mycs
Router(ca-trustpoint)# rsakeypair aaa
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate mycs
Certificate has the following attributes:
Fingerprint:C21514AC 12815946 09F635ED FBB6CF31
% Do you accept this certificate? [yes/no]:y
Trustpoint CA certificate accepted.
!
Router(config)# crypto pki enroll mycs
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The fully-qualified domain name in the certificate will be:Router
% The subject name in the certificate will be:bizarro.cisco.com
% Include the router serial number in the subject name? [yes/no]:n
% Include an IP address in the subject name? [no]:n
Request certificate from CA? [yes/no]:y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

Router(config)# Fingerprint: 8DA777BC 08477073 A5BE2403 812DD157

00:29:11:%CRYPTO-6-CERTRET:Certificate received from Certificate Authority

Router(config)# crypto pki export aaa pem terminal 3des cisco123

% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAa2gAwIBAgIBATANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJVUzES
<snip>
waDeNOSI3WlDa0AWq5DkVBkxwgn0TqIJXJOCttjHnWHK1LMcMVGn
-----END CERTIFICATE-----

% Key name:aaa
    Usage:General Purpose Key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type:4,ENCRYPTED
DEK-Info:DES-EDE3-CBC,ED6B210B626BC81A

Urguv0jnjwOgowWVUQ2XR5nbzzYHI2vGLunpH/IxIsJuNjRVjbAAUpGk7VnPCT87
<snip>
kLCOtxzEv7JHc72gMku9uUlrLSnFH5slzAtoC0czfU4=
-----END RSA PRIVATE KEY-----

% Certificate:
-----BEGIN CERTIFICATE-----
MIICTjCCAfigAwIBAgICIQUwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
<snip>
```

```
6xlBaIsuMxnHmr89KkKkYlU6
-----END CERTIFICATE-----
```

Related Commands

Command	Description
crypto pki import pem	Imports certificates and RSA keys to a trustpoint from PEM-formatted files.
crypto pki trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of a CA.

crypto pki export pkcs12

To export Rivest, Shamir, and Adelman (RSA) keys within a PKCS12 file at a specified location, use the **crypto pki export pkcs12** command in global configuration mode.

crypto pki export *trustpointname* **pkcs12** *destination url passphrase*

Syntax Description

trustpointname	Name of the trustpoint who issues the certificate that a user is going to export. When you export the PKCS12 file, the trustpoint name is the RSA key name.
destination url	Location of the PKCS12 file to which a user wants to import the RSA key pair.
passphrase	Passphrase that is used to encrypt the PKCS12 file for export.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	The **crypto ca export pkcs12** command was introduced.
12.3(7)T	This command replaced the **crypto ca export pkcs12** command.

Usage Guidelines

The **crypto pki export pkcs12** command creates a PKCS 12 file that contains an RSA key pair. The PKCS12 file, along with a certificate authority (CA), is exported to the location that you specify with the destination URL. If you decide not to import the file to another router, you must delete the file.

Security Measures

Keep the PKCS12 file stored in a secure place with restricted access.

An RSA keypair is more secure than a passphrase because the private key in the key pair is not known by multiple parties. When you export an RSA key pair to a PKCS#12 file, the RSA key pair now is only as secure as the passphrase.

To create a good passphrase, be sure to include numbers, as well as both lowercase and uppercase letters. Avoid publicizing the passphrase by mentioning it in e-mail or cell phone communications because the information could be accessed by an unauthorized user.

Examples

The following example exports an RSA key pair with a trustpoint name “mytp” to a Flash file:

```
Router(config)# crypto pki export mytp pkcs12 flash:myexport mycompany
```

Related Commands

Command	Description
crypto pki import pkcs12	Imports RSA keys.

crypto pki import

To import a certificate manually via TFTP or as a cut-and-paste at the terminal, use the **crypto pki import** command in global configuration mode.

crypto pki import *name* **certificate**

Syntax Description

name **certificate**	Name of the certification authority (CA). This name is the same name used when the CA was declared with the **crypto pki trustpoint** command.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	The **crypto ca import** command was introduced.
12.3(7)T	This command replaced the **crypto ca import** command.

Usage Guidelines

You must enter the **crypto pki import** command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.)

Examples

The following example shows how to import a certificate via cut-and-paste. In this example, the CA trustpoint is "MS."

```
crypto pki trustpoint MS
 enroll terminal
 crypto pki authenticate MS
!
crypto pki enroll MS
crypto pki import MS certificate
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of your CA.
enrollment terminal	Specifies manual cut-and-paste certificate enrollment.

crypto pki import pem

To import certificates and Rivest, Shamir, and Adelman (RSA) keys to a trustpoint from privacy-enhanced mail (PEM)-formatted files, use the **crypto pki import pem** command in global configuration mode.

crypto pki import *trustpoint* **pem** [**usage-keys**] {**terminal** | **url** *url*} [**exportable**] *passphrase*

Syntax Description

trustpoint	Name of the trustpoint that is associated with the imported certificates and RSA key pairs. The *trustpoint* argument must match the name that was specified via the **crypto pki trustpoint** command.
usage-keys	(Optional) Specifies that two RSA special usage key pairs will be imported (that is, one encryption pair and one signature pair), instead of one general-purpose key pair.
terminal	Certificates and RSA key pairs will be manually imported from the console terminal.
url *url*	URL of the file system where your router should import the certificates and RSA key pairs.
exportable	(Optional) Specifies that the imported RSA key pair can be exported again to another Cisco device such as a router.
passphrase	Passphrase that is used to encrypt the PEM file for import. **Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	The **crypto ca import pem** command was introduced.
12.3(7)T	This command replaced the **crypto ca import pem** command.

Usage Guidelines

The **crypto pki import pem** command allows you import certificates and RSA key pairs in PEM-formatted files. The files can be previously exported from another router or generated from other public key infrastructure (PKI) applications.

Examples

The following example shows how to import PEM files to trustpoint “ggg” via TFTP:

```
Router(config)# crypto pki import ggg pem url tftp://10.1.1.2/johndoe/msca cisco1234
```

```
% Importing CA certificate...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.ca]?
Reading file from tftp://10.1.1.2/johndoe/msca.ca
Loading johndoe/msca.ca from 10.1.1.2 (via Ethernet0):!
[OK - 1082 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.prv]?
Reading file from tftp://10.1.1.2/johndoe/msca.prv
Loading johndoe/msca.prv from 10.1.1.2 (via Ethernet0):!
[OK - 573 bytes]

% Importing  certificate PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.crt]?
Reading file from tftp://10.1.1.2/johndoe/msca.crt
Loading johndoe/msca.crt from 10.1.1.2 (via Ethernet0):!
[OK - 1289 bytes]
% PEM files import succeeded.
Router(config)#
```

Related Commands

Command	Description
crypto pki export pem	Exports certificates and RSA keys that are associated with a trustpoint in a PEM-formatted file.
crypto pki trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of a CA.

crypto pki import pkcs12

To import Rivest, Shamir, and Adelman (RSA) keys, use the **crypto pki import pkcs12** command in global configuration mode.

crypto pki import *trustpointname* **pkcs12** *source url passphrase*

Syntax Description

trustpointname	Name of the trustpoint who issues the certificate that a user is going to export or import. When importing, the trustpoint name will become the RSA key name.
source url	The location of the PKCS12 file to which a user wants to export the RSA key pair.
passphrase	Passphrase that must be entered to undo encryption when the RSA keys are imported.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	The **crypto ca import pkcs12** command was introduced.
12.3(7)T	This command replaced the **crypto ca import pkcs12** command.

Usage Guidelines

When you enter the **crypto pki import pkcs12** command, a ke pair and a trustpoint are generated. If you then decide you want to remove the key pair and trustpoint that were generated, enter the **crypto key zeroize rsa** command to zeroize the key pair and enter the **no crypto pki trustpoint** command to remove the trustpoint.

Note After you import RSA keys to a target router, you cannot export those keys from the target router to another router.

Examples

In the following example, an RSA key pair that has been associated with the trustpoint "forward" is to be imported:

```
Router(config)# crypto pki import forward pkcs12 flash:myexport mycompany
```

Related Commands

Command	Description
crypto pki export pkcs12	Exports RSA keys.

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.
crypto key zeroize rsa	Deletes all RSA keys from your router.

crypto pki profile enrollment

To define an enrollment profile, use the **crypto pki profile enrollment** command in global configuration mode. To delete all information associated with this enrollment profile, use the **no** form of this command.

crypto pki profile enrollment *label*

no crypto pki profile enrollment *label*

Syntax Description

label	Name for the enrollment profile; the enrollment profile name must match the name specified in the **enrollment profile** command.

Defaults

An enrollment profile does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(7)T	This command replaced the **crypto ca profile enrollment** command.

Usage Guidelines

Before entering this command, you must specify a named enrollment profile using the **enrollment profile** in ca-trustpoint configuration mode.

After entering the **crypto pki profile enrollment** command, you can use any of the following commands to define the profile parameters:

- **authentication command**—Specifies the HTTP command that is sent to the certification authority (CA) for authentication.
- **authentication terminal**—Specifies manual cut-and-paste certificate authentication requests.
- **authentication url**—Specifies the URL of the CA server to which to send authentication requests.
- **enrollment command**—Specifies the HTTP command that is sent to the CA for enrollment.
- **enrollment terminal**—Specifies manual cut-and-paste certificate enrollment.
- **enrollment url**—Specifies the URL of the CA server to which to send enrollment requests.
- **parameter**—Specifies parameters for an enrollment profile. This command can be used only if the **authentication command** or the **enrollment command** is used.

Note The **authentication url**, **enrollment url**, **authentication terminal**, and **enrollment terminal** commands allow you to specify different methods for certificate authentication and enrollment, such as TFTP authentication and manual enrollment.

Examples

The following example shows how to define the enrollment profile named "E" and associated profile parameters:

```
crypto pki trustpoint Entrust
  enrollment profile E
  serial

crypto pki profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the PKI trustpoint that your router should use.
enrollment profile	Specifies that an enrollment profile can be used for certificate authentication and enrollment.

crypto pki server

To enable a Cisco IOS certificate server and enter certificate server configuration mode, use the **crypto pki server** command in global configuration mode. To disable a certificate server (which is the default functionality), use the **no** form of this command.

crypto pki server *cs-label*

no crypto pki server *cs-label*

Syntax Description

cs-label	Name of the certificate server.

Defaults

A certificate server is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

A certificate server allows you to more easily deploy public key infrastructure (PKI) by defining default behavior, which limits user interface complexity. To define the functionality of the certificate server, you can use any of the following certificate server configuration mode commands:

- **database (certificate server)**—Requires a username or password to be issued when accessing a database storage location.
- **database level**—Controls what type of data is stored in the certificate enrollment database.
- **database url—**Specifies the location where all database entries for the certificate server will be written out.
- **grant automatic**—Specifies automatic certificate enrollment.

Note This command can be used for testing and building simple networks; however, it is recommended that you do not issue this command if your network is generally accessible.

- **issuer-name—**Specifies the distinguished name (DN) as the certification authority (CA) issuer name for the certificate server.
- **lifetime (certificate server)**—Specifies the lifetime of the CA or a certificate.
- **lifetime crl**—Defines the lifetime of the certificate revocation list (CRL) that is used by the certificate server.
- **shutdown**—Allows a certificate server to be disabled without removing the configuration.

Note All of these commands are optional; thus, any basic certificate server functionality that is not specified via the command-line interface (CLI) will use the default value.

Examples

The following example shows how to enable the certificate server "mycertserver":

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# database url tftp://mytftp/johndoe/mycertserver
```

The following example shows how to disable the certificate server "mycertserver":

```
Router(config)# no crypto pki server mycertserver
% This will stop the Certificate Server process and delete the server
  configuration
Are you sure you want to do this? [yes/no]: yes
% Do you also want to remove the associated trustpoint and
  signing certificate and key? [yes/no]: no
% Certificate Server Process stopped
```

Related Commands

Command	Description
crypto pki server info requests	Displays all outstanding certificate enrollment requests.
ip http server	Enables an HTTP server on your network.

crypto pki server grant

To grant all or certain simple certificate enrollment protocol (SCEP) requests, use the **crypto pki server grant** command in privileged EXEC mode.

crypto pki server *cs-label* **grant** {**all** | *req-id*}

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.
all	All certificate enrollment requests are granted.
req-id	ID associated with a specific enrollment request in the enrollment request database. Use the **crypto pki server info requests** command to display the ID.

Defaults

If this command is not issued, the certificate server keeps the requests in a pending state.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

After you enable the **crypto pki server grant** command, your certificate server will immediately grant all specified certificate requests. Certificate requests that are not granted will expire after the time that was specified using the **lifetime enrollment-request** command.

Examples

The following example shows to grant all manual enrollment requests for the certificate server “mycs”:

```
Router# crypto pki server mycs grant all
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto pki server reject	Rejects all or certain SCEP requests.

crypto pki server info crl

To display information regarding the status of the current certificate revocation list (CRL), use the **crypto pki server info crl** command in privileged EXEC mode.

crypto pki server *cs-label* **info crl**

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

CRLs are issued once every specified time period via the **lifetime crl** command. It is the responsibility of the network administrator to ensure that the CRL is available from the location that is specified via the **cdp-url** command. To access information, such as the lifetime and location of the CRL, use the **crypto pki server info crl** command.

Examples

The following example shows how to access CRL information for the certificate server "mycs":

```
Router# crypto pki server mycs info crl
```

Related Commands

Command	Description
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crypto pki server	Enables a Cisco IOS certificate server and enter certificate server configuration mode.
lifetime crl	Defines the lifetime of the CRL that is used by the certificate server.

crypto pki server info requests

To display all outstanding certificate enrollment requests, use the **crypto pki server info requests** command in privileged EXEC mode.

crypto pki server *cs-label* **info requests**

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

A certificate enrollment request functions as follows:

- The certificate server receives the enrollment request from an end user, and the following actions occur:
  - A request entry is created in the enrollment request database with the initial state. (See the **show pki server** command for a complete list of certificate enrollment request states.)
  - The certificate server refers to the command-line interface (CLI) configuration (or the default behavior any time a parameter is not specified) to determine the authorization of the request. Thereafter, the state of the enrollment request is updated in the enrollment request database.
- At each Simple Certificate Enrollment Protocol (SCEP) query for a response, the certificate server examines the current request and performs one of the following actions:
  - Responds to the end user with a “pending” or “denied” state.
  - Forwards to the request to the certification authority (CA) core, where it will generate and sign the appropriate certificate, store the certificate in the enrollment request database, and return the request to the built-in certificate server Simple Certificate Enrollment Protocol (SCEP) server, who will reply to the end user with the certificate on the next SCEP request.

If the connection of the client has closed, the certificate server will wait for client user to request another certificate.

All enrollment requests transitions through the certificate enrollment states that are defined in Table 17.

Table 17 Certificate Enrollment States

Certificate Enrollment State	Description
initial	The request has been created by the SCEP server.
authorized	The certificate server has authorized the request.
malformed	The certificate server has determined that the request is invalid for cryptographic reasons.
denied	The certificate server has denied the request for policy reasons.
pending	The enrollment request must be manually accepted by the network administrator.
granted	The CA core has generated the appropriate certificate for the certificate request.

Examples

The following example shows output for the certificate server "certsrv1," which has a pending certificate enrollment request:

```
Router# crypto pki server certsrv1 info requests

   Enrollment Request Database:
   ReqID  State      Fingerprint                      SubjectName
   --------------------------------------------------------------
   1      pending    0A71820219260E526D250ECC59857C2D serialNumber=2326115A+hostname=831.
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.

crypto pki server password generate

To generate a password for simple certificate enrollment protocol (SCEP) requests that can be used only one time, use the **crypto pki server password generate** command in privileged EXEC mode.

crypto pki server *cs-label* **password generate** [*minutes*]

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.
minutes	(Optional) Length of time, in minutes, that the password is valid. Valid times range from 1 to 1440 minutes. The default value is 60 minutes.

Defaults

If this command is not enabled, no password is created.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

SCEP, which is the only supported enrollment protocol, supports two client authentication mechanisms—manual and preshared key. Manual enrollment requires the administrator at the certification authority (CA) server to specifically authorize the enrollment requests; enrollment using preshared keys allows the administrator to preauthorize enrollment requests by generating a one-time password.

Note Only one password is valid at a time; if a second password is generated, the previous password is no longer valid.

Examples

The following example shows how to generate a one-time password that is valid for 75 minutes for the certificate server “mycs”:

```
Router# crypto pki server mycs password generate 75
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

crypto pki server reject

To reject all or certain Simple Certificate Enrollment Protocol (SCEP) requests, use the **crypto pki server reject** command in privileged EXEC mode.

crypto pki server *cs-label* **reject** {**all** | *req-id*}

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.
all	All certificate enrollment requests are rejected.
req-id	ID associated with a specific enrollment request in enrollment request database. Use the **crypto pki server info requests** command to display the ID.

Defaults

If this command is not issued, the certificate server keeps the requests in a pending state.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

After you enable the **crypto pki server reject** command, your certificate server will immediately reject all certificate requests.

SCEP, which is the only supported enrollment protocol, supports two client authentication mechanisms—manual and preshared key. Manual enrollment requires the administrator at the certification authority (CA) server to specifically authorize the enrollment requests. The administrator can become overloaded if there are numerous enrollment requests. Thus, the **crypto pki server reject** command can be reduce user interaction by automatically rejecting all or specific enrollment requests.

Examples

The following example shows how reject all manual enrollment requests for the certificate server "mycs":

```
Router# crypto pki server mycs reject all
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto pki server grant	Grants all or certain SCEP requests.
crypto pki server info requests	Displays all outstanding certificate enrollment requests.

crypto pki server remove

To remove enrollment requests that are in the certificate server Enrollment Request Database, use the **crypto pki server remove** command in privileged EXEC mode . This command does not have a **no** form.

crypto pki server *cs-label* **remove {all |** *req-id***}**

Syntax Description

cs-label	Name of the certificate server.
all	Removes all enrollment requests.
req-id	Removes the specified enrollment request.

Defaults

Enrollment requests will remain in the certificate server database.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

After the certificate server receives an enrollment request, it can leave the request in pending, reject it, or grant it. Before this command was added, the request would be left in the Enrollment Request Database for 1 hour until the client polled the certficiate server for the result of the request. This command allows you to remove individual or all requests from the database, especially useful if the client leaves and never polls the certificate server.

In addition, the use of this command also allows the server to be returned to a clean slate with respect to the keys and transaction IDs. Thus, it is a useful command to use during troubleshooting with a Simple Certificate Enrollment Protocol (SCEP) client that may be behaving badly.

Examples

The following example shows that all enrollment requests are to be removed from the certificate server:

```
Router# enable
 Router# crypto pki server server1 remove all
```

Related Commands

Command	Description
crypto pki server info request	Displays all outstanding enrollment requests.

crypto pki server request pkcs10

To manually add a certificate request to the request database, use the **crypto pki server request pkcs10** command in privileged EXEC mode.

crypto pki server *cs-label* **request pkcs10** {*url* | **terminal**} [**pem**]

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.
url	URL of the file systems from which the certificate server should retrieve the PKCS10 enrollment request and to which it should post the granted certificate. For a list of available options, see Table 18. **Note** The request file name should have a .req extension and the granted certificate file name will have a .crt extension (see the URL example in the section "Examples."
terminal	Certificate requests will be manually pasted from the console terminal, and the granted certificate will be displayed on the console.
pem	(Optional) Privacy-enhanced mail (PEM) headers are automatically added to the certificate after the certificate is granted.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use the **crypto pki server request pkcs10** command to manually add either a base64-encoded or PEM-formatted PKCS10 certificate enrollment request. This command is especially useful when the client does not have a network connection with the certificate server so that it can do Simple Certificate Enrollment Protocol (SCEP) enrollment. After the certificate is granted, the certificate will be displayed on the console terminal using base64 encoding if the **terminal** keyword is specified, or it will be sent to the file system that is specified using the *url* argument. If the **pem** keyword is specified, PEM headers are also added to the certificate.

The *url* argument allows you to specify or change the location in which the certificate server retrieves the new certificate request and posts the granted certificate. Table 18 lists available file system options.

Table 18 File System Options

Location	Description
cns:	Retrieves certificate from Cisco Networking Services (CNS): file system
flash:	Retrieves certificate from flash: file system

Table 18 File System Options

Location	Description
ftp:	Retrieves certificate from FTP: file system
http:	Retrieves certificate from HTTP: file system
https:	Retrieves certificate from Secure HTTP (HTTPS): file system
null:	Retrieves certificate from null: file system
nvram:	Retrieves certificate from NVRAM: file system
rcp:	Retrieves certificate from remote copy protocol (rcp): file system
scp:	Retrieves certificate from secure copy protocol (scp): file system
system:	Retrieves certificate from system: file system
tftp:	Retrieves certificate from TFTP: file system

Examples

The following example shows how to manually add a base64-encoded certificate request with PEM boundaries to the request database:

```
Router# crypto pki server mycs request pkcs10 terminal pem

% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE REQUEST-----
MIIBdTCB3wIBADA2MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVt
czEPMA0GA1UEAxMGdGVzdCAxMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDF
EFukc2lCFSHtDJn6HFR2n8rpdhlAYwcs0m68N3iRYHonv847h0/H6utTHVd2qEEo
rNw97jMRZk6BLhVDc05TKGHvUlBlHQWwc/BqpVI8WiHzZdskUH/DUM8kd67Vkjlb
e+FF7WrWT4FIO4vR4rF1V2p3FZ+A29UNc9Pi1s98nQIDAQABoAAwDQYJKoZIhvcN
AQEEBQADgYEAUQCGNzzNJwBOCwmEmG8XEGFSZWDmFlctm8VWvaZYMPOt+vl6iwFk
RmtD1Kg91Vw/qT5FJN8LmGUopOWIrwH4rUWON+TqtRmv2dgsdL5T4dx0sgG5E0s4
T302paxEHiHVRJpe8OD7FJgOvdsKRziCpyD4/Jfb1WnSVQZmvIYAxVQ=
-----END CERTIFICATE REQUEST-----

% Enrollment request pending, reqId=2

Router# crypto pki server mycs grant 2
% Granted certificate:
-----BEGIN CERTIFICATE-----
MIIB/TCCAWagAwIBAgIBAzANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDgyODAxMTcyOVoXDTA1MDgyODAxMTcyOVowNjELMAkGA1UEBhMCVVMx
FjAUBgNVBAoTDUNpc2NvIFN5c3RlbXMxDzANBgNVBAMTBnRlc3QgMTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEAxRBbpHNpQhUh7QyZ+hxUdp/K6XYZQGMHLNJu
vDd4kWB6J7/OO4dPx+rrUx1XdqhBKKzcPe4zEWZOgS4VQ3NOUyhh71JQZR0FsHPw
aqVSPFoh82XbJFB/w1DPJHeu1ZI5W3vhRe1q1k+BSDuL0eKxdVdqdxWfgNvVDXPT
4tbPfJ0CAwEAAaNCMEAwHwYDVR0jBBgwFoAUggWpVwokbUtGIwGZGavh6C8Bq6Uw
HQYDVR0OBBYEFFD3jZ/d960qzCGKwKNtFvq85Xt6MA0GCSqGSIb3DQEBBAUAA4GB
AAE4MqerwbM/nO8BCyZAiDzTqwLGnNvzS4H+u3JCsm0LaxY+E3d8NbSY+HruXWaR
7QyjprDGFd9bftRoqGYuiQkupU13sIHEyf3C2KnXJB6imySvAiuaQrGdSuUSIhBO
Xfh/xdWo3XL1e3vtWiYUa4X6jPUMpn74HoNfB4/gHO7g
-----END CERTIFICATE-----
```

The following example shows how to retrieve a certificate request and add it to the request database (using the *url* argument).

Note The request file name should have a .req extension and the certificate file name a .crt extension.

```
Router# crypto pki server mycs request pkcs10 tftp://172.69.1.129/router5
% Retrieving Base64 encoded or PEM formatted PKCS10 enrollment request...
Reading file from tftp://172.69.1.129/router5.req
Loading router5.req from 172.69.1.129 (via Ethernet0): !
[OK - 582 bytes]

% Enrollment request pending, reqId=1


Router# crypto pki server mycs grant 1
% Writing out the granted certificate...
!Writing file to tftp://172.69.1.129/router5.crt!
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto pki server grant	Grants all or certain SCEP requests.

crypto pki server revoke

To revoke a certificate on the basis of its serial number, use the **crypto pki server revoke** command in privileged EXEC mode.

crypto pki server *cs-label* **revoke** *certificate-serial-number*

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.
certificate-serial-number	Serial number of the certificate that is to be revoked. The serial number can be a hexadecimal number with the prefix "0x" (for example, 0x4c) or a decimal number (for example, 76).

Defaults

Certificates are revoked on the basis of their name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

When a new certificate revocation list (CRL) is issued, the certificate server obtains the previous CRL, makes the appropriate changes, and resigns the new CRL. A new CRL is issued after a certificate is revoked from the CLI. If this process negatively affects router performance, the **crypto pki server revoke** command can be used to revoke a list or range of certificates.

Note A new CRL cannot be issued unless the current CRL is revoked or changed.

Examples

The following examples show how to revoke a certificate with the serial number 76 (for example, 0x4c in hexidecimal) from the certificate server "mycs":

```
Router# crypto pki server mycs revoke 76
Router# crypto pki server mycs revoke 0x4c
```

Related Commands

Command	Description
cdp-url	Specifies that CDP should be used in the certificates that are issued by the certificate server.
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

crypto pki trustpoint

To declare the trustpoint that your router should use, use the **crypto pki trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the trustpoint, use the **no** form of this command.

crypto pki trustpoint *name*

no crypto pki trustpoint *name*

Syntax Description

name	Creates a name for the trustpoint. (If you previously declared the trustpoint and just want to update its characteristics, specify the name you previously created.)

Defaults

Your router does not recognize any trustpoints until you declare a trustpoint using this command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	The **crypto ca trustpoint** command was added.
12.2(15)T	The **match certificate** subcommand was introduced.
12.3(7)T	This command replaced the **crypto ca trustpoint** command. You can still enter the **crypto ca trusted-root** or **crypto ca trustpoint** command, but the command will be written in the configuration as "crypto pki trustpoint."

Usage Guidelines

Use the **crypto pki trustpoint** command to declare a trustpoint, which can be a self-signed root CA or a subordinate CA. Issuing the **crypto pki trustpoint** command puts you in ca-trustpoint configuration mode.

You can specify characteristics for the trustpoint using the following subcommands:

- **crl**—Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.
- **default (ca-trustpoint)**—Resets the value of ca-trustpoint configuration mode subcommands to their defaults.
- **enrollment**—Specifies enrollment parameters (optional).
- **enrollment http-proxy**—Accesses the CA by HTTP through the proxy server.
- **match certificate**—Associates a certificate-based access control list (ACL) defined with the **crypto ca certificate map** command.
- **primary**—Assigns a specified trustpoint as the primary trustpoint of the router.
- **root**—Defines the Trivial File Transfer Protocol (TFTP) to get the CA certificate and specifies both a name for the server and a name for the file that will store the CA certificate.

The following example shows how to declare the CA named “ka” and specify enrollment and CRL parameters:

```
crypto pki trustpoint ka
 enrollment url http://kahului:80
```

The following example shows a certificate-based access control list (ACL) with the label “Group” defined in a **crypto pki certificate map** command and included in the **match certificate** subcommand of the **crypto pki trustpoint** command:

```
crypto pki certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto pki trustpoint pki1
 match certificate Group
```

Related Commands

Command	Description
crl	Queries the CRL to ensure that the certificate of the peer has not been revoked.
default (ca-trustpoint)	Resets the value of a ca-trustpoint configuration subcommand to its default.
enrollment	Specifies the enrollment parameters of your CA.
enrollment http-proxy	Accesses the CA by HTTP through the proxy server.
primary	Assigns a specified trustpoint as the primary trustpoint of the router.
root	Obtains the CA certificate via TFTP.

crypto set security-association idle-time

To configure the IP Security (IPSec) security association (SA) idle timer, use the **crypto set security-association idle-time** command in global configuration mode or crypto map configuration mode. To inactivate the IPSec SA idle timer, use the **no** form of this command.

crypto set security-association idle-time *seconds*

no crypto set security-association idle-time

Syntax Description

seconds	Time, in seconds, that the idle timer will allow an inactive peer to maintain an SA. Valid values for the *seconds* argument range from 60 to 86400.

Defaults

IPSec SA idle timers are disabled.

Command Modes

Global configuration
Crypto map configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **crypto set security-association idle-time** command to configure the IPSec SA idle timer. This timer controls the amount of time that an SA will be maintained for an idle peer.

Use the **crypto ipsec security-association lifetime** command to configure global lifetimes for IPSec SAs. There are two lifetimes: a "timed" lifetime and a "traffic-volume" lifetime. A security association expires after the first of these lifetimes is reached.

The IPSec SA idle timers are different from the global lifetimes for IPSec SAs. The expiration of the global lifetimes is independent of peer activity. The IPSec SA idle timer allows SAs associated with inactive peers to be deleted before the global lifetime has expired.

If the IPSec SA idle timers are not configured with the **crypto set security-association idle-time** command, only the global lifetimes for IPSec SAs are applied. SAs are maintained until the global timers expire, regardless of peer activity.

Note If the last IPSec SA to a given peer is deleted due to idle timer expiration, the Internet Key Exchange (IKE) SA to that peer will also be deleted.

Examples

The following example configures the IPSec SA idle timer to drop SAs for inactive peers after 600 seconds:

```
crypto set security-association idle-time 600
```

Related Commands

Command	Description
clear crypto sa	Deletes IPSec SAs.
crypto ipsec security-association lifetime	Changes global lifetime values used when negotiating IPSec SAs.

crypto wui tti petitioner

To configure a device to become an easy secure device deployment (EzSDD) petitioner and enter tti-petitioner configuration mode, use the **crypto wui tti petitioner** command in global configuration mode. To disable petitioner support, use the **no** form of this command.

crypto wui tti petitioner

no crypto wui tti petitioner

Syntax Description

This command has no arguments or keywords.

Defaults

A device (with a crypto image) is configured to be an EzSDD petitioner.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

EzSDD uses Trusted Transitive Introduction (TTI) to easily deploy public key infrastructure (PKI) between two end devices. TTI, which is a communication protocol that provides a bidirectional introduction between two end entities, involves the following three entities:

- Introducer—A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
- Petitioner—A new device that is joined to the secure domain.
- Registrar—A server that authorizes the petitioner. The registrar can be a certificate server.

Note Because the petitioner is enabled by default on the device, you only have to issue the **crypto wui tti petitioner** command if you have previously disabled the petitioner or if you want to use an existing trustpoint instead of the automatically generated trustpoint.

Examples

After the EzSDD exchange is complete, the petitioner will automatically enroll with the registrar and obtain a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration at the petitioner. (Note that petitioner will not have any TTI-specific configuration in the begining except that ip http server will be turned on and the Domain Name System (DNS) server needs to be properly configured.)

```
crypto pki trustpoint tti
! Enrollment url contains the registrar CS details
 enrollment url http://pki1-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
```

```
auto-enroll 70
```

Related Commands

Command	Description
crypto wui tti registrar	Configures a device to become an EzSDD registrar and enters tti-registrar configuration mode.
trustpoint (tti-petitioner)	Specifies the trustpoint that is to be associated with the TTI exchange between the EzSDD petitioner and the EzSDD registrar.

crypto wui tti registrar

To configure a device to become an easy secure device deployment (EzSDD) registrar and enter tti-registrar configuration mode, use the **crypto wui tti registrar** command in global configuration mode. To disable registrar support, use the **no** form of this command.

crypto wui tti registrar

no crypto wui tti registrar

Syntax Description

This command has no arguments or keywords.

Defaults

The registrar is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

EzSDD uses Trusted Transitive Introduction (TTI) to easily deploy public key infrastructure (PKI) between two end devices. TTI, which is a communication protocol that provides a bidirectional introduction between two end entities, involves the following three entities:

- Introducer—A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
- Petitioner—A new device that is joined to the secure domain.
- Registrar—A server that authorizes the petitioner.

Although any device that contains a crypto image can be the registrar, it is recommended that the registrar be either a Cisco IOS certificate server registration authority (RA) or a Cisco IOS certificate server root.

Examples

The following sample output from the **show running-config** command verifies that the certificate server "cs1" was configured and associated with the TTI exchange between the registrar and petitioner:

```
crypto pki server cs1
 issuer-name CN = ioscs,L = Santa Cruz,C =US
 lifetime crl 336
 lifetime certificate 730
!
crypto pki trustpoint pki-36a
 enrollment url http://pki-36a:80
 ip-address FastEthernet0/0
 revocation-check none
!
crypto pki trustpoint cs1
```

```
 revocation-check crl
 rsakeypair cs1
!
!
crypto pki certificate chain pki-36a
 certificate 03
  308201D0 30820139 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333334 345A170D 30363031 33303039 33333434 5A303A31 38301606 092A8648
  86F70D01 09081309 31302E32 332E322E 32301E06 092A8648 86F70D01 09021611
  706B692D 3336612E 63697363 6F2E636F 6D305C30 0D06092A 864886F7 0D010101
  0500034B 00304802 4100AFFA 8F429618 112FAB9D 01F3352E 59DD3D2D AE67E31D
  370AC4DA 619735DF 9CF4EA13 64E4B563 C239C5F0 1578B773 07BED641 A18CA629
  191884B5 61B66ECF 4D110203 010001A3 30302E30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 141DA8B1 71652961 3F7D69F0 02903AC3 2BADB137
  C6300D06 092A8648 86F70D01 01040500 03818100 67BAE186 327CED31 D642CB39
  AD585731 95868683 B950DF14 3BCB155A 2B63CFAD B34B579C 79128AD9 296922E9
  4DEDFCAF A7B5A412 AB1FC081 09951CE3 08BFFDD9 9FB1B9DA E9AA42C8 D1049268
  C524E58F 11C6BA7F C750320C 03DFB6D4 CBB3E739 C8C76359 CE939A97 B51B3F7F
  3FF;A9D82 9CFDB6CF E2503A14 36D0A236 A1CCFEAE
  quit
 certificate ca 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
  13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
  55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
  BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
  E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
  49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
  727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
  71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
  B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
  00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
  3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
  9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A0
  F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
  8A7BCFB0 FB
  quit
crypto pki certificate chain cs1
 certificate ca 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
  13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
  55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
  BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
  E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
  49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
  727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
  71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
  B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
  00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
  3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
  9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A02;
  F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
  8A7BCFB0 FB
```

```
  quit
!
crypto wui tti registrar
 pki-server cs1
!
!
!
crypto isakmp policy 1
 hash md5
!
!
crypto ipsec transform-set test_transformset esp-3des
!
crypto map test_cryptomap 10 ipsec-isakmp
 set peer 10.23.1.10
 set security-association lifetime seconds 1800
 set transform-set test_transformset
 match address 170
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto wui tti petitioner	Configures a device to become an EzSDD petitioner and enters tti-petitioner configuration mode.

ctype

To preauthenticate calls on the basis of the call type, use the **ctype** command in AAA preauthentication configuration mode. To remove the **ctype** command from your configuration, use the **no** form of this command.

ctype [**if-avail** | **required**] [**accept-stop**] [**password** *password*] [**digital** | **speech** | **v.110** | **v.120**]

no ctype [**if-avail** | **required**] [**accept-stop**] [**password** *password*] [**digital** | **speech** | **v.110** | **v.120**]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as **clid** or **dnis** from being tried once preauthentication has succeeded for a call element.
password *password*	(Optional) Defines the password for the preauthentication element.
digital	(Optional) Specifies “digital” as the call type for preauthentication.
speech	(Optional) Specifies “speech” as the call type for preauthentication.
v.110	(Optional) Specifies “v.110” as the call type for preauthentication.
v.120	(Optional) Specifies “v.120” as the call type for preauthentication.

Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the AAA preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Set up the RADIUS preauthentication profile with the call type string as the username and with the password that is defined in the **ctype** command as the password. Table 19 shows the call types that you may use in the preauthentication profile.

Table 19 Preauthentication Call Types

Call Type String	ISDN Bearer Capabilities
digital	Unrestricted digital, restricted digital.
speech	Speech, 3.1 kHz audio, 7 kHz audio.
v.110	Anything with V.110 user information layer.
v.120	Anything with V.120 user information layer.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the call type:

```
aaa preauth
 group radius
 ctype required
```

Related Commands

Command	Description
clid	Preauthenticates calls on the basis of the CLID number.
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (RADIUS)	Specifies the AAA RADIUS server group to use for preauthentication.

database (certificate server)

To require a username or password to be issued when accessing a database storage location, use the **database** command in certificate server configuration mode. To return to the default value, use the **no** form of this command.

database username *username* [**password** *password*]

no database username *username* [**password** *password*]

Syntax Description

username *username*	When prompted, a username will be used to access a storage location.
password *password*	(Optional) When prompted, a password will be used to access a storage location.

Defaults

This command is not enabled.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

All information stored in the remote database is public: there are no private keys stored in the database location. Using a password helps to protect against a potential attacker who can change the contents of the .ser or .crl file. If the contents of the files are changed, the certificate server may shut down, refusing to either issue new certificates or respond to simple certificate enrollment protocol (SCEP) requests until the files are restored.

It is good security practice to protect all information exchanges with the database server using IP Security (IPSec). To protect your information, use a remote database to obtain the appropriate certificates and setup the necessary IPSec connections to protect all future access to the database server.

Examples

The following example shows how to specify the username “mystorage” when accessing the complete database that is stored on an external TFTP server:

```
Router (config)# ip http server
Router (config)# crypto pki server myserver
Router (cs-server)# database level complete
Router (cs-server)# database url tftp://mytftp
Router (cs-server)# database username mystorage
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.
database level	Controls what type of data is stored in the database.
database url	Specifies the location where all database entries for the certificate server will be written out.

database archive

To set the certification authority (CA) certificate and CA key archive format—and the password—to encrypt this CA certificate and CA key archive file, use the **database archive** command in certificate server configuration mode. To disable the autoarchive feature, use the **no** form of this command.

database archive {**pkcs12** | **pem**} **[password** *password***]**

no database archive {**pkcs12** | **pem**} **[password** *password***]**

Syntax Description

pkcs12	Export as a PKCS12 file. The default is PKCS12.
pem	Export as a privacy-enhanced mail (PEM) file.
password *password*	(Optional) Password to encrypt the CA certificate and CA key. The password must be at least eight characters. If a password is not specified, you will be prompted for the password after the **no shutdown** command has been issued for the first time. When the password is entered, it will be encrypted.

Defaults

The archive format is PKCS (that is, the CA certificate and CA key are exported into a PKCS12 file, and you will be prompted for the password when the certificate server is turned on the first time).

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Use this command to configure the autoarchive format for the CA certificate and CA key. The archive can later be used to restore your certificate server.

If autoarchiving is not explicitly turned off when the certificate server is first enabled (using the **no shutdown** command), the CA certificate and CA key will be archived automatically, applying the following rule:

- The CA key must be (1) manually generated and marked “exportable” or (2) automatically generated by the certificate server (it will be marked nonexportable).

Note It is strongly recommended that if the password is included in the configuration to suppress the prompt after the **no shutdown** command, the password should be removed from the configuration after the archiving is finished.

Examples

The following example shows that certificate server auto archiving has been enabled. The CA certificate and CA key format has been set to PEM, and the password has been set as cisco123.

```
Router (config)# crypto pki server myserver
Router (cs-server)# database archive pem password cisco123
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server.

database level

To control what type of data is stored in the certificate enrollment database, use the **database level** command in certificate server configuration mode. To return to the default functionality, use the **no** form of this command.

database level {**minimal** | **names** | **complete**}

no database level {**minimal** | **names** | **complete**}

Syntax Description

minimal	Enough information is stored only to continue issuing new certificates without conflict. This is the default functionality.
names	The serial number and subject name of each certificate are stored in the database, providing enough information for the administrator to find and revoke and particular certificate, if necessary.
complete	Each issued certificate is written to the database. If this keyword is used, you should enable the **database url** command; see "Usage Guidelines" for more information.

Defaults

minimal

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **database level** command is used to describe the database of certificates and certification authority (CA) states. After the user downgrades the database level, the old data stays the same and the new data is logged at the new level.

minimum Level

The *ca-label*.ser file is always available. It contains the previously issued certificate's serial number, which is always 1. If the .ser file is unavailable and the CA server has a self-signed certificate in the local configuration, the CA server will refuse to issue new certificates.

The file format is as follows:

```
last_serial = serial-number
```

names Level

The *serial-number*.cnm file, which is written for each issued certificate, contains the "human readable decoded subject name" of the issued certificate and the "der encoded" values. This file can also include a certificate expiration date and the current status. (The **minimum** level files are also written out.)

The file format is as follows:

```
subjectname_der = <base64 encoded der value>
subjectname_str = <human readable decode subjectname>
expiration = <expiration date>
status = valid | revoked
```

complete Level

The *serial-number*.cer file, which is written for each issued certificate, is the binary certificate without additional encoding. (The **minimum** and **names** level files are also written out.)

The **complete** level produces a large amount of information, so you may want to store all database entries on an external TFTP server via the **database url** command unless your router does one of the following:

- Issues only a small number of certificates
- Has a local file system that is designed to support a large number of write operations and has sufficient storage for the certificates that are being issued

Examples

The following example shows how configure a minimum database to be stored on the local system:

```
Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level minimum
Router#(cs-server) database url nvram:
Router#(cs-server) issuer-name CN = ipsec_cs,L = Santa Cruz,C = US
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.
database url	Specifies the location where all database entries for the certificate server will be written out.

database url

To specify the location where all database entries for the certificate server will be written out, use the **database url** command in certificate server configuration mode. To return to the default location, use the **no** form of this command.

database url *root-url*

no database url *root-url*

Syntax Description

root-url	Location where database entries will be written out. The URL can be any URL that is supported by the Cisco IOS file system (IFS).

Defaults

The default location is flash.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

After you create a certificate server via the **crypto pki server** command, use the **database url** command if you want to specify a combined list of all the certificates that have been issued and the current command revocation list (CRL). The CRL is written to the certificate enrollment database as *ca-label*.crl (where *ca-label* is the name of the certificate server).

Note Although issuing the **database url** command is not required, it is recommended. Unless your router has a local file system that is designed for a large number of write operations and has sufficient storage for the certificates that are issued, you should issue this command.

Cisco IOS File System

The router uses any file system that is supported by your version of Cisco IOS software (such as TFTP, FTP, flash, and NVRAM) to send a certificate request and to receive the issued certificate. A user may wish to enable IFS certificate enrollment when his or her certification authority (CA) does not support Simple Certificate Enrollment Protocol (SCEP).

Examples

The following example shows how to configure all database entries to be written out to a TFTP server:

```
Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level complete
Router#(cs-server) database url tftp://mytftp
```

Verifying the Database URL

To ensure that the specified URL is working correctly, configure the **database url** command before you issue the **no shutdown** command on the certificate server for the first time. If the URL is broken, you will see output as follows:

```
Router(config)# crypto pki server mycs
Router(cs-server)# database url ftp://myftpserver
Router(cs-server)# no shutdown
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: yes
Translating "myftpserver"

% Failed to generate CA certificate - 0xFFFFFFFF
% The Certificate Server has been disabled.
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.
database level	Controls what type of data is stored in the database.

deadtime (server-group configuration)

To configure deadtime within the context of RADIUS server groups, use the **deadtime** command in server group configuration mode. To set deadtime to 0, use the **no** form of this command.

deadtime *minutes*

no deadtime

Syntax Description

minutes	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).

Defaults

Deadtime is set to 0.

Command Modes

Server-group configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

Use this command to configure the deadtime value of any RADIUS server group. The value of deadtime set in the server groups will override the server that is configured globally. If deadtime is omitted from the server group configuration, the value will be inherited from the master list. If the server group is not configured, the default value (0) will apply to all servers in the group.

When the RADIUS Server Is Marked As Dead

For Cisco IOS versions prior to 12.2(13.7)T, the RADIUS server will be marked as dead if a transaction is transmitted for the configured number of retransmits and a valid response is not received from the server within the configured timeout for any of the RADIUS packet transmissions.

For Cisco IOS versions 12.2(13.7)T and later, the RADIUS server will be marked as dead if both of the following conditions are met:

1. A valid response has not been received from the RADIUS server for any outstanding transaction for at least the timeout period that is used to determine whether to retransmit to that server, and
2. Across all transactions being sent to the RADIUS server, at least the requisite number of retransmits +1 (for the initial transmission) have been sent consecutively without receiving a valid response from the server with the requisite timeout.

Examples

The following example specifies a one-minute deadtime for RADIUS server group group1 once it has failed to respond to authentication requests:

```
aaa group server radius group1
 server 1.1.1.1 auth-port 1645 acct-port 1646
 server 2.2.2.2 auth-port 2000 acct-port 2001
 deadtime 1
```

Related Commands

Command	Description
radius-server deadtime	Sets the deadtime value globally.

default (ca-trustpoint)

To reset the value of a ca-trustpoint configuration subcommand to its default, use the **default** command in ca-trustpoint configuration mode.

default *command-name*

Syntax Description

command-name	Ca-trustpoint configuration subcommand.

Defaults

No default behavior or values.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which enters ca-trustpoint configuration mode.

Use this command to reset the value of a ca-trustpoint configuration mode subcommand to its default.

Examples

The following example shows how to remove the **crl optional** command from your configuration; the default of **crl optional** is off.

```
default crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

description (identity policy)

To enter a description for an identity policy, use the **description** command in identity policy configuration mode. To remove the description, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

line-of-description	Description of the identity policy.

Defaults

A description is not entered for the identity policy.

Command Modes

Identity policy configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example shows that a default identity policy and its description (“bluemoon”) have been specified:

```
Router (config)# identity policy bluemoon
Router (config-identity-policy)# description policyABC
```

Related Commands

Command	Description
description (identity profile)	Enters a description for an identity profile.

description (identity profile)

To enter a description for an identity profile, use the **description** command in identity profile configuration mode. To remove the description of the identity profile, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

line-of-description	Description of the identity profile.

Defaults

A description is not entered for the identity profile.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	This command was previously configured in dot1x configuration mode.

Usage Guidelines

The **identity profile** command and one of its keywords (**default**, **dot1x**, or **eapoudp**) must be entered in global configuration mode before the **description** command can be used.

Examples

The following example shows that a default identity profile and its description ("ourdefaultpolicy") have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# description ourdefaultpolicy
```

Related Commands

Command	Description
description (identity policy)	Enters a description for an identity policy.
identity profile	Creates an identity profile and enters identity profile configuration mode.

description (isakmp peer)

To add the description of an Internet Key Exchange (IKE) peer, use the **description** command in ISAKMP peer configuration mode. To delete the description, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

line-of-description	Description given to an IKE peer.

Defaults

No default behavior or values

Command Modes

ISAKMP peer configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

IKE peers that "sit" behind a Network Address Translation (NAT) device cannot be uniquely identified; therefore, they have to share the same peer description.

Examples

The following example shows that the description "connection from site A" has been added for an IKE peer:

```
Router# crypto isakmp peer address 10.2.2.9
Router (config-isakmp-peer)# description connection from site A
```

Related Commands

Command	Description
clear crypto session	**Deletes crypto sessions (IPSec and IKE SAs).**
show crypto isakmp peer	Displays peer descriptions.
show crypto session	Displays status information for active crypto sessions in a router.

device (identity profile)

To statically authorize or reject individual devices, use the **device** command in identity profile configuration mode. To disable the authorization or rejection, use the **no** form of this command.

device {authorize {ip address *ip-address {***policy** *policy-name}* **| mac-address** *mac-address* **| type {cisco | ip | phone}} | not-authorize}**

no device {authorize {ip address *ip-address {***policy** *policy-name}* **| mac-address** *mac-address* **| type {cisco | ip | phone}} | not-authorize}**

Syntax Description

authorize	Configures an authorized device.
ip address	Specifies a device by its IP address.
ip-address	The IP address.
policy	Applies an associated policy with the device.
policy-name	Name of the policy.
mac-address	Specifies a device by its MAC address.
mac-address	The MAC address.
type	Specifies a device by its type.
cisco	Specifies a Cisco device.
ip	Specifies an IP device.
phone	Specifies a Cisco IP phone.
not-authorize	Configures an unauthorized device.

Defaults

A device is not statically authorized or rejected.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	The **unauthorize** keyword was changed to **not authorize**. The *cisco-device* argument was deleted. The **ip address** keyword and *ip-address* argument were added. The **ip** and **phone** keywords were added.

Usage Guidelines

The **identity profile** command and **default**, **dot1x**, or **eapoudp** keywords must be entered in global configuration mode before the **device** command can be used.

Examples

The following configuration example defines an identity profile for Extensible Authentication Protocol over UDP (EAPoUDP) to statically authorize host 192.168.1.3 with “greentree” as the associated identity policy:

```
Router(config)# identity profile eapoudp
Router(config-identity-prof)# device authorize ip-address 192.168.1.3 policy greentree
```

Related Commands

Command	Description
identity profile eapoudp	Creates an identity profile.

dialer aaa

To allow a dialer to access the authentication, authorization, and accounting (AAA) server for dialing information, use the **dialer aaa** command in interface configuration mode. To disable this function, use the **no** form of this command.

dialer aaa suffix *string* **password** *string*

no dialer aaa suffix *string* **password** *string*

Syntax Description

suffix *string*	Defines a suffix for authentication.
password *string*	Defines a nondefault password for authentication.

Defaults

This feature is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1(5)T	The **suffix** and **password** keywords were added.

Usage Guidelines

This command is required for large scale dial-out and Layer 2 Tunneling Protocol (L2TP) dial-out functionality. With this command, you can specify a suffix, a password, or both. If you do not specify a password, the default password will be "cisco."

Note Only IP addresses can be specified as usernames for the **dialer aaa suffix** command.

Examples

This example shows a user sending out packets from interface Dialer1 with a destination IP address of 1.1.1.1. The username in the access-request message is "1.1.1.1@ciscoDoD" and the password is "cisco."

```
interface dialer1
 dialer aaa
 dialer aaa suffix @ciscoDoD password cisco
```

Related Commands

Command	Description
accept dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.
dialer congestion-threshold	Specifies congestion threshold in connected links.
dialer vpdn	Enables a Dialer Profile or DDR dialer to use L2TP dial-out.

disconnect ssh

To terminate a Secure Shell (SSH) connection on your router, use the **disconnect ssh** command in privileged EXEC mode.

disconnect ssh [**vty**] *session-id*

Syntax Description

vty	(Optional) Virtual terminal for remote console access.
session-id	The session-id is the number of connection displayed in the **show ip ssh** command output.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1 T.

Usage Guidelines

The **clear line vty** *n* command, where *n* is the connection number displayed in the **show ip ssh** command output, may be used instead of the **disconnect ssh** command.

When the EXEC connection ends, whether normally or abnormally, the SSH connection also ends.

Examples

The following example terminates SSH connection number 1:

```
disconnect ssh 1
```

Related Commands

Command	Description
clear line vty	Returns a terminal line to idle state using the privileged EXEC command.

dnis (authentication)

To preauthenticate calls on the basis of the Dialed Number Identification Service (DNIS) number, use the **dnis** command in AAA preauthentication configuration mode. To remove the **dnis** command from your configuration, use the **no** form of this command.

dnis [**if-avail** | **required**] [**accept-stop**] [**password** *string*]

no dnis [**if-avail** | **required**] [**accept-stop**] [**password** *string*]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements from being tried once preauthentication has succeeded for a call element.
password *string*	(Optional) Password to use in the Access-Request packet. The default is cisco.

Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the AAA preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example enables DNIS preauthentication using a RADIUS server and the password Ascend-DNIS:

```
aaa preauth
 group radius
 dnis password Ascend-DNIS
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication mode.
group (authentication)	Selects the security server to use for AAA preauthentication.
isdn guard-timer	Sets a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.

dnis (RADIUS)

To preauthenticate calls on the basis of the DNIS (Dialed Number Identification Service) number, use the **dnis** command in AAA preauthentication configuration mode. To remove the **dnis** command from your configuration, use the **no** form of this command.

dnis [**if-avail** | **required**] [**accept-stop**] [**password** *password*]

no dnis [**if-avail** | **required**] [**accept-stop**] [**password** *password*]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as **clid** or **ctype** from being tried once preauthentication has succeeded for a call element.
password *password*	(Optional) Defines the password for the preauthentication element.

Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the authentication, authorization, and accounting (AAA) preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the DNIS number:

```
aaa preauth
 group radius
 dnis required
```

Related Commands

Command	Description
clid	Preauthenticates calls on the basis of the CLID number.
ctype	Preauthenticates calls on the basis of the call type.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (RADIUS)	Specifies the AAA RADIUS server group to use for preauthentication.

dnis bypass (AAA preauthentication configuration)

To specify a group of DNIS (Dialed Number Identification Service) numbers that will be bypassed for preauthentication, use the **dnis bypass** command in AAA preauthentication configuration mode. To remove the **dnis bypass** command from your configuration, use the **no** form of this command.

dnis bypass {*dnis-group-name*}

no dnis bypass {*dnis-group-name*}

Syntax Description

dnis-group-name	Name of the defined DNIS group.

Defaults

No DNIS numbers are bypassed for preauthentication.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

Before using this command, you must first create a DNIS group with the **dialer dnis group** command.

Examples

The following example specifies that preauthentication be performed on all DNIS numbers except for two DNIS numbers (12345 and 12346), which have been defined in the DNIS group called hawaii:

```
aaa preauth
 group radius
 dnis required
 dnis bypass hawaii

dialer dnis group hawaii
 number 12345
 number 12346
```

Related Commands

Command	Description
dialer dnis group	Creates a DNIS group.
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.

dns

To specify the primary and secondary Domain Name Service (DNS) servers, use the **dns** command in (Internet Security Association Key Management Protocol) ISAKMP group configuration mode. To remove this command from your configuration, use the **no** form of this command.

dns *primary-server secondary-server*

no dns *primary-server secondary-server*

Syntax Description

primary-server	Name of the primary DNS server.
secondary-server	Name of the secondary DNS server.

Defaults

A DNS server is not specified.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **dns** command to specify the primary and secondary DNS servers for the group.

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that needs to be defined or changed, before enabling the dns command.

Examples

The following example shows how to define a primary and secondary DNS server for the default group name:

```
crypto isakmp client configuration group default
 key cisco
 dns 2.2.2.2 2.3.2.3
 pool dog
 acl 199
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the policy profile of the group that will be defined.
domain (isakmp-group)	Specifies the DNS domain to which a group belongs.

dnsix-dmdp retries

To set the retransmit count used by the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) Message Delivery Protocol (DMDP), use the **dnsix-dmdp retries** command in global configuration mode. To restore the default number of retries, use the **no** form of this command.

dnsix-dmdp retries *count*

no dnsix-dmdp retries *count*

Syntax Description

count	Number of times DMDP will retransmit a message. It can be an integer from 0 to 200. The default is 4 retries, or until acknowledged.

Defaults

Retransmits messages up to 4 times, or until acknowledged.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example sets the number of times DMDP will attempt to retransmit a message to 150:

```
dnsix-dmdp retries 150
```

Related Commands

Command	Description
dnsix-nat authorized-redirection	Specifies the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages.
dnsix-nat primary	Specifies the IP address of the host to which DNSIX audit messages are sent.
dnsix-nat secondary	Specifies an alternate IP address for the host to which DNSIX audit messages are sent.
dnsix-nat source	Starts the audit-writing module and defines audit trail source address.
dnsix-nat transmit-count	Causes the audit-writing module to collect multiple audit messages in the buffer before sending the messages to a collection center.

dnsix-nat authorized-redirection

To specify the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages, use the **dnsix-nat authorized-redirection** command in global configuration mode. To delete an address, use the **no** form of this command.

dnsix-nat authorized-redirection *ip-address*

no dnsix-nat authorized-redirection *ip-address*

Syntax Description

ip-address	IP address of the host from which redirection requests are permitted.

Defaults

An empty list of addresses.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use multiple **dnsix-nat authorized-redirection** commands to specify a set of hosts that are authorized to change the destination for audit messages. Redirection requests are checked against the configured list, and if the address is not authorized the request is rejected and an audit message is generated. If no address is specified, no redirection messages are accepted.

Examples

The following example specifies that the address of the collection center that is authorized to change the primary and secondary addresses is 192.168.1.1:

```
dnsix-nat authorization-redirection 192.168.1.1
```

dnsix-nat primary

To specify the IP address of the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat primary** command in global configuration mode. To delete an entry, use the **no** form of this command.

dnsix-nat primary *ip-address*

no dnsix-nat primary *ip-address*

Syntax Description

ip-address	IP address for the primary collection center.

Defaults

Messages are not sent.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An IP address must be configured before audit messages can be sent.

Examples

The following example configures an IP address as the address of the host to which DNSIX audit messages are sent:

```
dnsix-nat primary 172.1.1.1
```

dnsix-nat secondary

To specify an alternate IP address for the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat secondary** command in global configuration mode. To delete an entry, use the **no** form of this command.

dnsix-nat secondary *ip-address*

no dnsix-nat secondary *ip-address*

Syntax Description

ip-address	IP address for the secondary collection center.

Defaults

No alternate IP address is known.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When the primary collection center is unreachable, audit messages are sent to the secondary collection center instead.

Examples

The following example configures an IP address as the address of an alternate host to which DNSIX audit messages are sent:

```
dnsix-nat secondary 192.168.1.1
```

dnsix-nat source

To start the audit-writing module and to define the audit trail source address, use the **dnsix-nat source** command in global configuration mode. To disable the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit trail writing module, use the **no** form of this command.

dnsix-nat source *ip-address*

no dnsix-nat source *ip-address*

Syntax Description

ip-address	Source IP address for DNSIX audit messages.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You must issue the **dnsix-nat source** command before any of the other **dnsix-nat** commands. The configured IP address is used as the source IP address for DMDP protocol packets sent to any of the collection centers.

Examples

The following example enables the audit trail writing module, and specifies that the source IP address for any generated audit messages should be the same as the primary IP address of Ethernet interface 0:

```
dnsix-nat source 192.168.2.5
interface ethernet 0
 ip address 192.168.2.5 255.255.255.0
```

dnsix-nat transmit-count

To have the audit writing module collect multiple audit messages in the buffer before sending the messages to a collection center, use the **dnsix-nat transmit-count** command in global configuration mode. To revert to the default audit message count, use the **no** form of this command.

dnsix-nat transmit-count *count*

no dnsix-nat transmit-count *count*

Syntax Description

count	Number of audit messages to buffer before transmitting to the server. It can be an integer from 1 to 200.

Defaults

One message is sent at a time.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An audit message is sent as soon as the message is generated by the IP packet-processing code. The audit writing module can, instead, buffer up to several audit messages before transmitting to a collection center.

Examples

The following example configures the system to buffer five audit messages before transmitting them to a collection center:

```
dnsix-nat transmit-count 5
```

domain (isakmp-group)

To specify the Domain Name Service (DNS) domain to which a group belongs, use the **domain** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration, use the **no** form of this command.

domain *name*

no domain *name*

Syntax Description

name	Name of the DNS domain.

Defaults

A DNS domain is not specified.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **domain** command to specify group domain membership.

You must enable the **crypto isakmp configuration group command, which specifies group policy information that has to be defined or changed, before enabling the domain command.**

Examples

The following example shows that members of the group “cisco” also belong to the domain “cisco.com”:

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
  domain cisco.com
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.
crypto isakmp keepalive	Specifies the primary and secondary DNS servers.

dot1x default

To reset the global 802.1X parameters to their default values, use the **dot1x default** command in global configuration mode.

dot1x default

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

Use the **show dot1x** privileged EXEC command to verify your current 802.1X settings.

Examples

The following example shows how to reset the global 802.1X parameters:

```
Router(config)# dot1x default
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that the device sends an EAP-request/identity frame before restarting the authentication process.
dot1x re-authentication (EtherSwitch)	Enables periodic reauthentication of the client for the Ethernet switch network module.
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x initialize

To initialize an interface, use the **dot1x initialize** command in privileged EXEC mode. This command does not have a **no** form.

dot1x initialize [interface *interface-name*]

Syntax Description

interface *interface-name*	(Optional) Specifies an interface to be initialized. If this keyword is not entered, all enterfaces are initialized.

Defaults

An interface is not initialized.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Examples

The following example shows that Ethernet 0 is to be initialized:

```
Router# dot1x initialize interface ethernet 0
```

dot1x max-req

To set the maximum number of times that a router or Ethernet switch network module can send an Extensible Authentication Protocol (EAP) request/identity frame to a client (assuming that a response is not received) before restarting the authentication process, use the **dot1x max-req** command in interface configuration or global configuration mode. To disable the number of times that were set, use the **no** form of this command.

dot1x max-req *number-of-retries*

no dot1x max-req *number-of-retries*

Syntax Description

number-of-retries	Maximum number of retries. The value is from 1 through 10. The default value is 2.

Defaults

The default number of retries is 2.

Command Modes

Interface configuration (router)
Global configuration (EtherSwitch)

Command History

Release	Modification
12.1(6)EA2	This command was introduced for the Cisco Ethernet Switch Module.
12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet switch network module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.3(2)XA	This command was introduced on the following Cisco routers: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Router support was added for the following platforms: Cisco 1751, Cisco 2610XM – Cisco 2611XM, Cisco 2620XM – Cisco 2621XM, Cisco 2650XM – Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.

Usage Guidelines

You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Examples

The following example shows that the maximum number of times that the router will send an EAP request/identity message to the client PC is 6:

```
Router (config) configure terminal
Router (config)# interface ethernet 0
Router (config-if)# dot1x max-req 6
```

The following example shows how to set the number of times that the switch sends an EAP-request/identity frame to 5 before restarting the authentication process:

```
Router (config)# dot1x max-req 5
```

Related Commands

Command	Description
dot1x port-control	Sets an 802.1X port control value.
dot1x re-authentication	Enables periodic reauthentication of the client on the 802.1X interface.
dot1x reauthentication (EtherSwitch)	Enables periodic reauthentication of the Ethernet switch network module client on the 802.1X interface.
dot1x timeout	Sets retry timeouts.
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x max-start

To set the maximum number of times that a router sends an Extensible Authentication Protocol (EAP) start frame to the client before concluding that there are no other authenticators present in the network, use the **dot1x max-start** command in interface configuration mode. To remove the maximum number-of-times setting, use the **no** form of this command.

dot1x max-start *number*

no dot1x max-start *number*

Syntax Description

number	Maximum number of times that the router sends an EAP start frame. The value is from 1 to 65535. The default is 3.

Defaults

The default maximum number setting is 3.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Examples

The following example shows that the maximum number of EAP over LAN- (EAPOL-) Start requests has been set to 5:

```
Router (config)# interface Ethernet1
 Router (config-if)# dot1x pae supplicant
 Router (config-if)# dot1x max-start 5
```

Related Commands

Command	Description
dot1x pae	Sets the PAE type.
interface	Configures an interface type.

dot1x multiple-hosts

To allow multiple hosts (clients) on an 802.1X-authorized port that has the **dot1x port-control** interface configuration command set to **auto**, use the **dot1x multiple-hosts** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x multiple-hosts

no dot1x multiple-hosts

Syntax Description

This command has no arguments or keywords.

Defaults

Multiple hosts are disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

This command enables you to attach multiple clients to a single 802.1X-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL]-logoff message is received), all attached clients are denied access to the network.

Use the **show dot1x (EtherSwitch)** privileged EXEC command with the **interface** keyword to verify your current 802.1X multiple host settings.

Examples

The following example shows how to enable 802.1X on Fast Ethernet interface 0/1 and to allow multiple hosts:

```
Router(config)# interface fastethernet0/1
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x multiple-hosts
```

Related Commands

Command	Description
dot1x default	Enables manual control of the authorization state of the port.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x pae

To set the Port Access Entity (PAE) type, use the **dot1x pae** command in interface configuration mode. To disable the PAE type that was set, use the **no** form of this command.

dot1x pae [supplicant | authenticator | both]

no dot1x pae [supplicant | authenticator | both]

Syntax Description

supplicant	(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.
authenticator	(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.
both	(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.

Defaults

PAE type is not set.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

If the **dot1x system-auth-control** command has not been configured, the **supplicant** keyword will be the only keyword available for use with this command. (That is, if the **dot1x system-auth-control** command has not been configured, you cannot configure the **interface as an authenticator**.)

Examples

The following example shows that the interface has been set to act as a supplicant:

```
Router (config)# interface Ethernet1
 Router (config-if)# dot1x pae supplicant
```

Related Commands

Command	Description
dot1x system-auth-control	Enables 802.1X SystemAuthControl (port-based authentication).
interface	Configures an interface type.

dot1x port-control

To set an 802.1X port control value, use the **dot1x port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.

dot1x port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control {auto | force-authorized | force-unauthorized}

Syntax Description

auto	Determines authentication status of the client PC by the authentication process. The port state will be set to AUTO.
force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Defaults

The default is **force-authorized**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced for the Cisco Ethernet switch network module.
12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet switch network module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.3(2)XA	This command was introduced on the following Cisco routers: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Router support was added for the following platforms: Cisco 1751, Cisco 2610XM – Cisco 2611XM, Cisco 2620XM – Cisco 2621XM, Cisco 2650XM – Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.

Usage Guidelines

For Ethernet Switch Network Modules

The following guidelines apply to Ethernet switch network modules:

The 802.1X protocol is supported on Layer 2 static-access ports.

You can use the **auto** keyword only if the port is not configured as one of these types:

- Trunk port—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
- EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
- Switch Port Analyzer (SPAN) destination port—You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port.

To globally disable 802.1X on the device, you must disable it on each port. There is no global configuration command for this task.

You can verify your settings by entering the **show dot1x** (EtherSwitch) privileged EXEC command and checking the Status column in the 802.1X Port Summary section of the display. An enabled status means that the port-control value is set to auto or to force-unauthorized.

Examples

The following example shows that the authentication status of the client PC will be determined by the authentication process:

```
Router (config)# configure terminal
Router (config)# interface ethernet 0
Router (config-if)# dot1x port-control auto
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x re-authentication	Enables periodic reauthentication of the client on the 802.1X interface.
dot1x reauthentication (EtherSwitch)	Enables periodic reauthentication of the Ethernet switch network module client on the 802.1X interface.
dot1x timeout	Sets retry timeouts.
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x re-authenticate (EtherSwitch)

To manually initiate a reauthentication of all 802.1X-enabled ports or the specified 802.1X-enabled port on a router with an Ethernet switch network module installed, use the **dot1x re-authenticate** command in privileged EXEC mode.

dot1x re-authenticate [**interface** *interface-type interface-number*]

Syntax Description

interface *interface-type interface-number*	(Optional) Specifies the slot and port number of the interface to reauthenticate.

Defaults

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

You can use this command to reauthenticate a client without waiting for the configured number of seconds between reauthentication attempts (reauthperiod) and automatic reauthentication.

Examples

The following example shows how to manually reauthenticate the device connected to Fast Ethernet interface 0/1:

```
Router# dot1x re-authenticate interface fastethernet 0/1
Starting reauthentication on FastEthernet0/1.
```

dot1x re-authenticate (privileged EXEC)

To reauthenticate all the authenticated devices that are attached to the specified interface, use the **dot1x re-authenticate** command in privileged EXEC mode. This command does not have a **no** form.

dot1x re-authenticate *interface-type interface-number*

Syntax Description

interface-type interface-name	Specifies an interface to be reauthenticated. • The *number of the interface* must be 0 or 1.

Defaults

An interface is not reauthenticated.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Examples

The following example shows that Ethernet 0 is to be reauthenticated:

```
Router# dot1x re-authenticate ethernet 0
```

Related Commands

Command	Description
clear dot1x	Clears 802.1X interface information.

dot1x reauthentication

To enable periodic reauthentication of the client PCs on the 802.1X interface, use the **dot1x reauthentication** command in interface configuration mode. To disable periodic reauthentication, use the **no** form of this command.

dot1x reauthentication

no dot1x reauthentication

Syntax Description

This command has no arguments or keywords.

Defaults

Periodic reauthentication is not set.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The reauthentication period can be set using the **dot1x timeout** command.

Examples

The following example shows that reauthentication has been set for 1800 seconds:

```
Router (config)# configure terminal
Router (config)# interface ethernet 0
Router (config-if)# dot1x reauthentication
Router (config-if)# dot1x timeout reauth-period 1800
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC (assuming that a response is not received) before concluding that the client PC does not support 802.1X.
dot1x port-control	Sets an 802.1X port control value.
dot1x timeout	Sets retry timeouts.

dot1x re-authentication (EtherSwitch)

To enable periodic reauthentication of the client for an Ethernet switch network module, use the **dot1x re-authentication** command in global configuration mode. To disable periodic reauthentication, use the **no** form of this command.

dot1x re-authentication

no dot1x re-authentication

Syntax Description

This command has no arguments or keywords.

Defaults

Periodic reauthentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

You configure the amount of time between periodic reauthentication attempts by using the **dot1x timeout re-authperiod** global configuration command.

Examples

The following example shows how to disable periodic reauthentication of the client:

```
Router(config)# no dot1x re-authentication
```

The following example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000 seconds:

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

Related Commands

Command	Description
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x system-auth-control

To enable 802.1X SystemAuthControl (port-based authentication), use the **dot1x system-auth-control** command in global configuration mode. To disable SystemAuthControl, use the **no** form of this command.

dot1x system-auth-control

no dot1x system-auth-control

Syntax Description

This command has no arguments or keywords.

Defaults

System authentication is set to disabled by default. If this command is disabled, all ports behave as if they are force authorized.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Examples

The following example shows that system authentication has been enabled:

```
Router (config)# dot1x system-auth-control
```

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
description	Enters an 802.1X description.
device	Statically authorizes or rejects individual devices.
dot1x initialize	Initializes an interface.
dot1x max-req	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC.
dot1x port-control	Sets an 802.1X port control value.
dot1x re-authenticate	Reauthenticates an 802.1X interface.
dot1x reauthentication	Enables periodic reauthentication of the client PCs on the interface.
dot1x timeout	Sets retry timeouts.
identity profile default	Creates an identity profile and enters dot1x profile configuration mode.
show dot1x	Shows details and statistics for an identity profile.
template	Specifies a virtual template from which commands may be cloned.

dot1x timeout

To set retry timeouts, use the **dot1x timeout** command in interface configuration mode. To remove the retry timeouts, use the **no** form of this command.

dot1x timeout {auth-period *seconds* **| held-period** *seconds* **| quiet-period** *seconds* **| ratelimit-period** *seconds* **| reauth-period** *seconds* **| server-timeout** *seconds* **| start-period** *seconds* **| tx-period** *seconds***}**

no dot1x timeout {auth-period *seconds* **| held-period** *seconds* **| quiet-period** *seconds* **| ratelimit-period** *seconds* **| reauth-period** *seconds* **| server-timeout** *seconds* **| start-period** *seconds* **| tx-period** *seconds***}**

Syntax Description

auth-period *seconds*	Timeout for authenticator reply. • The value is from 1 to 65535 seconds. The default is 30 seconds.
held-period *seconds*	Timeout for authentication retires. • The value is from 1 to 56535 seconds. The default is 60 seconds.
quiet-period *seconds*	Quiet period. • The value is from 1 to 65535 seconds. The default is 120 seconds.
ratelimit-period *seconds*	Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of router processing power). • The value is from 1 to 65535 seconds. By default, rate-limiting is disabled.
reauth-period *seconds*	Time after which an automatic reauthentication should be initiated. • The value is from 1 to 65535 seconds. The default is 3600 seconds.
server-timeout *seconds*	Timeout for RADIUS retries. • The value is from 1 to 65535 seconds. The default is 30 seconds. • If an 802.1X packet is sent to the server and the server does not send a response, after the period specified by **server-timeout** value, the packet will be sent again.
start-period *seconds*	Timeout for Extensible Authentication Protocol over LAN- (EAPOL-) Start retries. • The value is from 1 to 65535 seconds. The default is 30 seconds.
tx-period *seconds*	Sets the timeout for supplicant (client PC) retries. • The value is from 1 to 65535 seconds. The default is 30 seconds. • If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.

Defaults

Periodic reauthentication and periodic rate-limiting are not done.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)X	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(11)T	The **auth-period**, **held-period**, and **start-period** keywords were added.

Examples

The following example shows that various 802.1X retransmission and timeout periods have been set:

```
Router (config)# configure terminal
Router (config)# interface ethernet 0
Router (config-if)# dot1x port-control auto
Router (config-if)# dot1x reauthentication
Router (config-if)# dot1x timeout auth-period 2000
Router (config-if# dot1x timeout held-period 2400
Router (config-if)# dot1x timeout reauth-period 1800
Router (config-if)# dot1x timeout quiet-period 600
Router (config-if# dot1x timeout start-period 90
Router (config-if)# dot1x timeout tx-period 60
Router (config-if)# dot1x timeout server-timeout 60
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC (assuming that a response is not received) before concluding that the client PC does not support 802.1X.
dot1x port-control	Sets an 802.1X port control value.
dot1x reauthentication	Enables periodic reauthentication of the client PCs on the 802.1X interface.

dot1x timeout (EtherSwitch)

To set the number of retry seconds between 802.1X authentication exchanges when an Ethernet switch network module is installed in the router, use the **dot1x timeout** command in global configuration mode. To return to the default setting, use the **no** form of this command.

dot1x timeout {**quiet-period** *seconds* | **re-authperiod** *seconds* | **tx-period** *seconds*}

no dot1x timeout {**quiet-period** *seconds* | **re-authperiod** *seconds* | **tx-period** *seconds*}

Syntax Description

quiet-period *seconds*	Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds.
re-authperiod *seconds*	Specifies the number of seconds between reauthentication attempts. The range is from 1 to 4294967295. The default is 3660 seconds.
tx-period *seconds*	Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is from 1 to 65535 seconds. The default is 30 seconds.

Defaults

quiet-period: 60 seconds
re-authperiod: 3660 seconds
tx-period: 30 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

You should change the default values of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients or authentication servers.

quiet-period Keyword

During the quiet period, the Ethernet switch network module does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a smaller number than the default.

re-authperiod Keyword

The **re-authperiod** keyword affects the behavior of the the Ethernet switch network module only if you have enabled periodic reauthentication by using the **dot1x re-authentication** global configuration command.

Examples

The following example shows how to set the quiet time on the switch to 30 seconds:

```
Router(config)# dot1x timeout quiet-period 30
```

The following example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000 seconds:

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

The following example shows how to set 60 seconds as the amount of time that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request:

```
Router(config)# dot1x timeout tx-period 60
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that the device sends an EAP-request/identity frame before restarting the authentication process.
dot1x re-authentication (EtherSwitch)	Enables periodic reauthentication of the client for the Ethernet switch network module.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

eap

To specify Extensible Authentication Protocol- (EAP-) specific parameters, use the **eap** command in identity profile configuration mode. To disable the parameters that were set, use the **no** form of this command.

eap {username *name* **| password** *password***}**

no eap {username *name* **| password** *password***}**

Syntax Description

username *name*	Username that will be sent to Request-Id packets.
password *password*	Password that should be used when replying to an Message Digest 5 (MD5) challenge.

Defaults

EAP parameters are not set.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Use this command if your router is configured as a supplicant. This command provides the means for configuring the identity and the EAP MD5 password that will be used by 802.1X to authenticate.

Examples

The following example shows that the EAP username “user1” has been configured:

```
Router (config)# identity profile dot1x
 Router (config-identity-prof)# eap username user1
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

enable password

To set a local password to control access to various privilege levels, use the **enable password** command in global configuration mode. To remove the password requirement, use the **no** form of this command.

enable password [**level** *level*] {*password* | [*encryption-type*] *encrypted-password*}

no enable password [**level** *level*]

Syntax Description

level *level*	(Optional) Level for which the password applies. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or the **no** form of the command, the privilege level defaults to 15 (traditional enable privileges).
password	Password users type to enter enable mode.
encryption-type	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available is 7. If you specify *encryption-type*, the next argument you supply must be an encrypted password (a password already encrypted by a Cisco router).
encrypted-password	Encrypted password you enter, copied from another router configuration.

Defaults

No password is defined. The default is level 15.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Caution If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

Use this command with the **level** option to define a password for a specific privilege level. After you specify the level and the password, give the password to the users who need to access this level. Use the **privilege level** configuration command to specify commands accessible at various levels.

You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you copy and paste into this command a password that has already been encrypted by a Cisco router.

Caution If you specify an encryption type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If the **service password-encryption** command is set, the encrypted form of the password you create with the **enable password** command is displayed when a **more nvram:startup-config** command is entered.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
- Must not have a number as the first character.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Crtl-v when you create the password; for example, to create the password *abc?123*, do the following:
  - Enter **abc**.
  - Type **Crtl-v**.
  - Enter **?123**.

  When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter abc?123 at the password prompt.

Examples

The following example enables the password “pswd2” for privilege level 2:

```
enable password level 2 pswd2
```

The following example sets the encrypted password “1i5Rkls3LoyxzS8t9”, which has been copied from a router configuration file, for privilege level 2 using encryption type 7:

```
enable password level 2 7 $1$i5Rkls3LoyxzS8t9
```

Related Commands

Command	Description
disable	Exits privileged EXEC mode and returns to user EXEC mode.
enable	Enters privileged EXEC mode.
enable secret	Specifies an additional layer of security over the **enable password** command.
privilege	Configures a new privilege level for users and associate commands with that privilege level.
service password-encryption	Encrypts passwords.
show privilege	Displays your current level of privilege.

enable secret

To specify an additional layer of security over the **enable password** command, use the **enable secret** command in global configuration mode. To turn off the **enable secret** function, use the **no** form of this command.

enable secret [**level** *level*] {*password* | [*encryption-type*] *encrypted-password*}

no enable secret [**level** *level*]

Syntax Description

level *level*	(Optional) Level for which the password applies. You can specify up to sixteen privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or in the **no** form of the command, the privilege level defaults to 15 (traditional enable privileges). The same holds true for the **no** form of the command.
password	Password for users to enter enable mode. This password should be different from the password created with the **enable password** command.
encryption-type	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available for this command is 5. If you specify *encryption-type*, the next argument you supply must be an encrypted password (a password encrypted by a Cisco router).
encrypted-password	Encrypted password you enter, copied from another router configuration.

Defaults

No password is defined. The default level is 15.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Caution If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

Use this command to provide an additional layer of security over the enable password. The **enable secret** command provides better security by storing the enable secret password using a non-reversible cryptographic function. The added layer of security encryption provides is useful in environments where the password crosses the network or is stored on a TFTP server.

You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you paste into this command an encrypted password that you copied from a router configuration file.

Caution If you specify an encryption type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If you use the same password for the **enable password** and **enable secret** commands, you receive an error message warning that this practice is not recommended, but the password will be accepted. By using the same password, however, you undermine the additional security the **enable secret** command provides.

Note After you set a password using the **enable secret** command, a password set using the **enable password** command works only if the **enable secret** is disabled or an older version of Cisco IOS software is being used, such as when running an older rxboot image. Additionally, you cannot recover a lost password that has been encrypted by any method.

If **service password-encryption** is set, the encrypted form of the password you create here is displayed when a **more nvram:startup-config** command is entered.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters
- Must not have a number as the first character
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Crtl-v when you create the password; for example, to create the password *abc?123*, do the following:
  - Enter **abc**.
  - Type **Crtl-v**.
  - Enter **?123**.

  When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter **abc?123** at the password prompt.

Examples

The following example specifies the enable secret password of “greentree”:

```
enable secret greentree
```

After specifying an enable secret password, users must enter this password to gain access. Any passwords set through enable password will no longer work.

```
Password: greentree
```

The following example enables the encrypted password “1FaD0$Xyti5Rkls3LoyxzS8”, which has been copied from a router configuration file, for privilege level 2 using encryption type 5:

```
enable password level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

Related Commands

Command	Description
enable	Enters privileged EXEC mode.
enable password	Sets a local password to control access to various privilege levels.

encryption (IKE policy)

To specify the encryption algorithm within an Internet Key Exchange (IKE) policy, use the **encryption** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the encryption algorithm to the default value, use the **no** form of this command.

encryption {**des** | **3des** | **aes** | **aes 192** | **aes 256**}

no encryption

Syntax Description

des	56-bit Data Encryption Standard (DES)-CBC as the encryption algorithm.
3des	168-bit DES (3DES) as the encryption algorithm.
aes	128-bit Advanced Encryption Standard (AES) as the encryption algorithim.
aes 192	192-bit AES as the encryption algorithim.
aes 256	256-bit AES as the encryption algorithim.

Defaults

The 56-bit DES-CBC encryption algorithm

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.0(2)T	The **3des** option was added.
12.2(13)T	The following keywords were added: **aes**, **aes 192**, and **aes 256**.

Usage Guidelines

Use this command to specify the encryption algorithm to be used in an IKE policy.

If a user enters an IKE encryption method that the hardware does not support, a warning message will be displayed immediately after the **encryption** command is entered.

Examples

The following example configures an IKE policy with the 3DES encryption algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy
 encryption 3des
 exit
```

The following example is a sample warning message that is displayed when a user enters an IKE encryption method that the hardware does not support:

```
encryption aes 256
WARNING:encryption hardware does not support the configured
    encryption method for ISAKMP policy 1
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
group (IKE policy)	Specifies the DH group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

enrollment

To specify the enrollment parameters of a certification authority (CA), use the **enrollment** command in ca-trustpoint configuration mode. To remove any of the configured parameters, use the **no** form of this command.

enrollment [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]

no enrollment [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]

Syntax Description

mode	(Optional) Registration authority (RA) mode, if your CA system provides an RA. By default, RA mode is disabled.
retry period *minutes*	(Optional) Specifies the period in which the router will wait before sending the CA another certificate request. The default is 1 minute between retries. (Specify between 1 to 60 minutes.)
retry count *number*	(Optional) Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. The default is 10 retries. (Specify from 1 to 100 retries.)
url url	URL of the file system where your router should send certificate requests. For enrollment method options, see Table 20.
pem	(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request.

Defaults

Your router does not know the CA URL until you specify it via **url** *url*.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(13)T	The **url** *url* option was enhanced to support TFTP enrollment.
12.3(4)T	The **pem** keyword was added, and the **url** *url* option was enhanced to support an additional enrollment method—the Cisco IOS File System (IFS).

Usage Guidelines

Use the **mode** keyword to specify the mode supported by the CA. This keyword is required if your CA system provides an RA.

Use the **retry period** *minutes* option to change the retry period from the default of 1 minute between retries. After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a period of time (the retry period), the router will send another certificate request. By default, the router will send a maximum of 10 requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries (specified via the **retry count** *number* option) is exceeded.

Use the **pem** keyword to issue certificate requests (via the **crypto ca enroll** command) or receive issued certificates (via the **crypto ca import certificate** command) in PEM-formatted files.

Note When generating certificate requests in PEM format, your router does not have to have the CA certificate, which is obtained via the **crypto ca authenticate** command.

Use the **url** *url* option to specify or change the URL of the CA. Table 20 lists the available enrollment methods.

Table 20 Enrollment Methods

Enrollment Method	Description
bootflash	Enroll via bootflash: file system
cns	Enroll via Cisco Networking Services (CNS): file system
flash	Enroll via flash: file system
ftp	Enroll via FTP: file system
SCEP[1]	Enroll via Simple Certificate Enrollment Protocol (SCEP) (an HTTP URL)
null	Enroll via null: file system
nvram	Enroll via NVRAM: file system
rcp	Enroll via remote copy protocol (rcp): file system
scp	Enroll via secure copy protocol (scp): file system
system	Enroll via system: file system
TFTP[2]	Enroll via TFTP: file system

1. If you are using SCEP for enrollment, the URL must be in the form http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA.
2. If you are using TFTP for enrollment, the URL must be in the form tftp://certserver/file_specification. (The file_specification is optional. See the section "TFTP Certificate Enrollment" for additional information.)

TFTP Certificate Enrollment

TFTP enrollment is used to send the enrollment request and retrieve the certificate of the CA and the certificate of the router. If the file_specification is included in the URL, the router will append an extension onto the file specification. When the **crypto ca authenticate** command is entered, the router will retrieve the certificate of the CA from the specified TFTP server. As appropriate, the router will append the extension ".ca" to the filename or the fully qualified domain name (FQDN). (If the **url** *url* option does not include a file specification, the FQDN of the router will be used.)

Note The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to declare a CA named “ka” and specify the URL of the CA as “http://kahului:80”:

```
crypto ca trustpoint ka
 enrollment url http://kahului:80
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto ca enroll	Obtains the certificate or certificates of your router from the CA.
crypto ca trustpoint	Declares the CA that your router should use.

enrollment command

To specify the HTTP command that is sent to the certification authority (CA) for enrollment, use the **enrollment command** command in ca-profile-enroll configuration mode.

enrollment command

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

After enabling this command, you can use the **parameter** command to specify enrollment parameters for your enrollment profile.

Examples

The following example shows how to configure the enrollment profile name “E” for certificate enrollment:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.
parameter	Specifies parameters for an enrollment profile.

enrollment credential

To specify an existing trustpoint from another vendor that is to be enrolled with the Cisco IOS certificate server, use the **enrollment credential** command in ca-profile-enroll configuration mode.

enrollment credential *label*

Syntax Description

label	Name of the certification authority (CA) trustpoint of another vendor.

Defaults

No default behavior or values.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

To configure a router that is already enrolled with a CA of another vendor that is to be enrolled with a Cisco IOS certificate server, you must configure a certificate enrollment profile (via the **crypto pki profile enrollment** command). Thereafter, you should issue the **enrollment credential** command, which specifies the trustpoint of another vendor that has to be enrolled with a Cisco IOS certificate server.

Examples

The following example shows how to configure a client router and a Cisco IOS certificate server to exchange enrollment requests via a certificate enrollment profile:

```
! Define the trustpoint "msca-root" that points to the non-Cisco IOS CA and enroll and
! authenticate the client with the non-Cisco IOS CA.
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 ip-address FastEthernet2/0
 revocation-check crl
!
! Configure trustpoint "cs" for Cisco IOS CA.
crypto pki trustpoint cs
 enrollment profile cs1
 revocation-check crl
!
! Define enrollment profile "cs1," which points to Cisco IOS CA and mention (via the
! enrollment credential command) that "msca-root" is being initially enrolled with the
! Cisco IOS CA.
crypto pki profile enrollment cs1
 enrollment url  http://cs:80
 enrollment credential  msca-root!
```

```
! Configure the certificate server, and issue and the grant auto trustpoint command to
! instruct the certificate server to accept enrollment request only from clients who are
! already enrolled with trustpoint "msca-root."
crypto pki server cs
 database level minimum
 database url nvram:
 issuer-name CN=cs
 grant auto trustpoint msca-root
!
crypto pki trustpoint cs
 revocation-check crl
rsakeypair cs
!
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 revocation-check crl
```

Related Commands

Command	Description
crypto pki profile enrollment	Defines an enrollment profile.

enrollment http-proxy

To access the certification authority (CA) by HTTP through the proxy server, use the **enrollment http-proxy** command in ca-trustpoint configuration mode.

enrollment http-proxy *host-name port-num*

Syntax Description

host-name	Defines the proxy server used to get the CA.
port-num	Specifies the port number used to access the CA.

Defaults

If this command is not enabled, the CA will not be accessed via HTTP.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **enrollment http-proxy** command must be used in conjunction with the **enrollment** command, which specifies the enrollment parameters for the CA.

Examples

The following example shows how to access the CA named "ka" by HTTP through the bomborra proxy server:

```
crypto ca trustpoint ka
 enrollment url http://kahului
 enrollment http-proxy bomborra 8080
 crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of your CA.

enrollment mode ra

The **enrollment mode ra** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment profile

To specify that an enrollment profile can be used for certificate authentication and enrollment, use the **enrollment profile** command in ca-trustpoint configuration mode. To delete an enrollment profile from your configuration, use the **no** form of this command.

enrollment profile *label*

no enrollment profile *label*

Syntax Description

label	Creates a name for the enrollment profile.

Defaults

Your router does not recognize any enrollment profiles until you declare one using this command.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Before you can enable this command, you must enter the **crypto ca trustpoint** command.

The **enrollment profile** command enables your router to accept an enrollment profile, which can be configured via the **crypto ca profile enrollment** command. The enrollment profile, which consists of two templates, can be used to specify different URLs or methods for certificate authentication and enrollment.

Examples

The following example shows how to declare the enrollment profile named “E”:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.
crypto ca trustpoint	Declares the CA that your router should use.

enrollment retry count

The **enrollment retry count** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment retry period

The **enrollment retry period** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment terminal (ca-profile-enroll)

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal** command in ca-profile-enroll configuration mode. To delete a current enrollment request, use the **no** form of this command.

enrollment terminal

no enrollment terminal

Syntax Description

This command has no arguments or keywords.

Defaults

A certificate enrollment request is not specified.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

A user may manually cut-and-paste certificate authentication requests and certificates when a network connection between the router and certification authority (CA) is unavailable. After this command is enabled, the certificate request is printed on the console terminal so that it can be manually copied (cut) by the user.

Note Although most routers accept manual enrollment, the process can be tedious if a large number of routers have to be enrolled.

Examples

The following example shows how to configure the enrollment profile named "E" to perform certificate authentication via HTTP and manual certificate enrollment:

```
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment terminal
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.

enrollment terminal (ca-trustpoint)

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal** command in ca-trustpoint configuration mode. To delete a current enrollment request, use the **no** form of this command.

enrollment terminal [**pem**]

no enrollment terminal [**pem**]

Syntax Description

pem	(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request.

Defaults

No default behavior or values

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(4)T	The **pem** keyword was added.

Usage Guidelines

A user may want to manually cut-and-paste certificate requests and certificates when he or she does not have a network connection between the router and certification authority (CA). When this command is enabled, the router displays the certificate request on the console terminal, allowing the user to enter the issued certificate on the terminal.

The pem Keyword

Use the **pem** keyword to issue certificate requests (via the **crypto ca enroll** command) or receive issued certificates (via the **crypto ca import certificate** command) in PEM-formatted files through the console terminal. If the CA server does not support simple certificate enrollment protocol (SCEP), the certificate request can be presented to the CA server manually.

Note When generating certificate requests in PEM format, your router does not have to have the CA certificate, which is obtained via the **crypto ca authenticate** command.

Examples

The following example shows how to manually specify certificate enrollment via cut-and-paste. In this example, the CA trustpoint is "MS."

```
crypto ca trustpoint MS
 enrollment terminal
 crypto ca authenticate MS
!
crypto ca enroll MS
```

```
crypto ca import MS certificate
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto ca enroll	Obtains the certificate(s) of your router from the certification authority.
crypto ca import	Imports a certificate manually via TFTP or cut-and-paste at the terminal.
crypto ca trustpoint	Declares the CA that your router should use.

enrollment url (ca-identity)

The **enrollment url (ca-identity)** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment url (ca-profile-enroll)

To specify the URL of the certification authority (CA) server to which to send enrollment requests, use the **enrollment url** command in ca-profile-enroll configuration mode. To delete the enrollment URL from your enrollment profile, use the **no** form of this command.

enrollment url *url*

no enrollment url *url*

Syntax Description

url	URL of the CA server to which your router should send certificate requests. If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, the *url* argument must be in the form http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA. If you are using TFTP for enrollment, the *url* argument must be in the form tftp://certserver/file_specification. (If the URL does not include a file specification, the fully qualified domain name [FQDN] of the router will be used.)

Defaults

Your router does not recognize the CA URL until you specify it using this command.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

This command allows the user to specify a different URL or a different method for authenticating a certificate and enrolling a certificate; for example, manual authentication and TFTP enrollment.

Examples

The following example shows how to enable certificate enrollment via HTTP for the profile name “E”:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
```

```
parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.

eou allow

To allow additional Extensible Authentication Protocol over UDP (EAPoUDP) options, use the **eou allow** command in global configuration mode. To disable the options that have been set, use the **no** form of this command.

eou allow {clientless | ip-station-id}

no eou allow {clientless | ip-station-id}

Syntax Description

clientless	Allows authentication of clientless hosts (systems that do not run Cisco Trust Agent).
ip-station-id	Allows an IP address in the station-id field.

Defaults

No additional EAPoUDP options are allowed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **eou allow** command used with the **clientless** keyword requires that a user group be configured on the Cisco Access Control Server (ACS) using the same username and password that are specified using the **eou clientless** command.

Examples

The following example shows that clientless hosts are allowed:

```
Router (config)# eou allow clientless
```

Related Commands

Command	Description
eou clientless	Sets user group credentials for clientless hosts.

eou clientless

To set user group credentials for clientless hosts, use the **eou clientless** command in global configuration mode. To remove the user group credentials, use the **no** form of this command.

eou clientless {password *password* **| username** *username***}**

no eou clientless {password | username}

Syntax Description

password password	Sets a password.
username *username*	Sets a username.

Defaults

Username and password values are clientless.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

For this command to be effective, the **eou allow** command must also be enabled.

Examples

The following example shows that a clientless host with the username “user1” has been configured:

```
Router (config)# eou clientless username user1
```

The following example shows that a clientless host with the password “user123” has been configured:

```
Router (config)# eou clientless password user123
```

Related Commands

Command	Description
eou allow	Allows additional EAPoUDP options.

eou default

To set global Extensible Authentication Protocol over UDP (EAPoUDP) parameters to the default values, use the **eou default** command in global or interface configuration mode.

eou default

Syntax Description

This command has no arguments or keywords.

Defaults

The EAPoUDP parameters are set to their default values.

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Using this command, you can reset existing values to their default values.

Examples

The following configuration example shows that EAPoUDP parameters have been set to their default values:

```
Router (config)# eou default
```

eou initialize

To manually initialize Extensible Authentication Protocol over UDP (EAPoUDP) state machines, use the **eou initialize** command in global configuration mode. This command has no **no** form.

eou initialize {all | authentication {clientless | eap | static} | interface *interface-name* **| ip** *ip-address* **| mac** *mac-address* **| posturetoken** *string***}**

Syntax Description

all	Initiates reauthentication of all EAPoUDP clients. This keyword is the default.
authentication	Specifies the authentication type.
clientless	Clientless authentication type.
eap	EAP authentication type.
static	Static authentication type.
interface *interface-name*	Specifies a specific interface.
ip *ip-address*	Specifies a specific IP address.
mac *mac-address*	Specifies a specific MAC address.
posturetoken *string*	Specifies a specific posture token.

Defaults

No default behaviour or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

If this command is used, existing EAPoUDP state machines will be reset.

Examples

The following example shows that all EAPoUDP state machines have been reauthenticated:

```
Router (config)# eou initialize
```

Related Commands

Command	Description
eou revalidate	Revalidates an EAPoUDP association.

eou logging

To enable Extensible Authentication Protocol over UDP (EAPoUDP) system logging events, use the **eou logging** command in global configuration mode. To remove EAPoUDP logging, use the **no** form of this command.

eou logging

no eou logging

Syntax Description

This command has no arguments or keywords.

Defaults

Logging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example shows that EAPoUDP logging has been enabled:

```
Router (config)# eou logging
```

The following is sample EAPoUDP logging output:

```
Apr  9 10:04:09.824: %EOU-6-SESSION: IP=10.0.0.1| HOST=DETECTED| Interface=FastEthernet0/0
*Apr  9 10:04:09.900: %EOU-6-CTA: IP=10.0.0.1| CiscoTrustAgent=DETECTED
*Apr  9 10:06:19.576: %EOU-6-POLICY: IP=10.0.0.1| TOKEN=Healthy
*Apr  9 10:06:19.576: %EOU-6-POLICY: IP=10.0.0.1| ACLNAME=#ACSACL#-IP-HealthyACL-40921e54
*Apr  9 10:06:19.576: %EOU-6-POSTURE: IP=10.0.0.1| HOST=AUTHORIZED|
Interface=FastEthernet0/0.420
*Apr  9 10:06:19.580: %EOU-6-AUTHTYPE: IP=10.0.0.1| AuthType=EAP
*Apr  9 10:06:04.424: %EOU-6-SESSION: IP=192.43.2.1| HOST=REMOVED|
Interface=FastEthernet0/0.420
```

eou max-retry

To set the number of maximum retry attempts for Extensible Authentication Protocol over UDP (EAPoUDP), use the **eou max-retry** command in global or interface configuration mode. To remove the number of retries that were entered, use the **no** form of this command.

eou max-retry *number-of-retries*

no eou max-retry *number-of-retries*

Syntax Description

number-of-retries	Number of maximum retries that may be attempted. The value ranges from 1 through 3. The default is 3.

Defaults

The default number of retries is 3.

Command Modes

Global configuration
Interface Configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Examples

The following example shows that the maximum number of retries for an EAPoUDP session has been set for 2:

```
Router (config)# eou max-retry 2
```

Related Commands

Command	Description
show eou	Displays information about EAPoUDP global values or EAPoUDP session cache entries.

eou port

To set the UDP port for Extensible Authentication Protocol over UDP (EAPoUDP), use the **eou port** command in global configuration mode. This command has no **no** form.

eou port *port-number*

Syntax Description

port-number	Number of the port. The value ranges from 1 through 65535. The default value is 27186.

Defaults

The default *port-number* value is 27186.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Ensure that the port you set does not conflict with other UDP applications.

Examples

The following example shows that the port for an EAPoUDP session has been set to 200:

```
Router (config)# eou port 200
```

Related Commands

Command	Description
show eou	Displays information about EAPoUDP.

eou rate-limit

To set the number of simultaneous posture validations for Extensible Authentication Protocol over UDP (EAPoUDP), use the **eou rate-limit** command in global configuration mode. This command has no **no** form.

eou rate-limit *number-of-validations*

Syntax Description

number-of-validations	Number of clients that can be simultaneously validated. The value ranges from 1 through 200. The default value is 20.

Defaults

No default behaviors or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

If you set the rate limit to 0 (zero), rate limiting will be turned off.

If the rate limit is set to 100 and there are 101 clients, validation will not occur until one drops off.

To return to the default value, use the **eou default** command.

Examples

The following example shows that the number of posture validations has been set to 100:

```
Router (config)# eou rate-limit 100
```

Related Commands

Command	Description
eou default	Sets global EAPoUDP parameters to the default values.
show eou	Displays information about EAPoUDP.

eou revalidate

To revalidate an Extensible Authentication Protocol over UDP (EAPoUDP) association, use the **eou revalidate** command in privileged EXEC mode. To disable the revalidation, use the **no** form of this command.

eou revalidate {all | authentication {clientless | eap | static} | interface *interface-name* **| ip** *ip-address* **| mac** *mac-address* **| posturetoken** *string***}**

no eou revalidate {all | authentication {clientless | eap | static} | interface *interface-name* **| ip** *ip-address* **| mac** *mac-address* **| posturetoken** *string***}**

Syntax Description

all	Enables revalidation of all EAPoUDP clients. This keyword option is the default.
authentication	Specifies the authentication type.
clientless	Clientless authentication type.
eap	EAP authentication type.
static	Static authentication type.
interface *interface-name*	Name of the interface. (See Table 21 for the types of interface that may be shown.)
ip *ip-address*	IP address of the client.
mac *mac-address*	The 48-bit hardware address of the client.
posturetoken *string*	Name of the posture token.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

If you use this command, existing EAPoUDP sessions will be revalidated.

Table 21 lists the interface types that may be used with the **interface** keyword.

Table 21 Description of Interface Types

Interface Type	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	Code division multiple access Internet exchange (CDMA Ix) interface

Table 21 Description of Interface Types (continued)

Interface Type	Description
CTunnel	Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface
Dialer	Dialer interface
Ethernet	IEEE 802.3 standard interface
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink-group interface
Null	Null interface
Serial	Serial interface
Tunnel	Tunnel interface
Vif	Pragmatic General Multicast (PGM) Multicase Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following example shows that all EAPoUDP clients are to be revalidated:

```
Router# eou revalidate all
```

Related Commands

Command	Description
eou initialize	Manually initializes EAPoUDP state machines.

eou timeout

To set the Extensible Authentication Protocol over UDP (EAPoUDP) timeout values, use the **eou timeout** command in global or interface configuration mode. To remove the value that was set, use the **no** form of this command.

eou timeout {aaa *seconds* **| hold-period** *seconds* **| retransmit** *seconds* **| revalidation** *seconds* **| status query** *seconds***}**

no timeout {aaa *seconds* **| hold-period** *seconds* **| retransmit** *seconds* **| revalidation** *seconds* **| status query** *seconds***}**

Syntax Description

aaa *seconds*	Authentication, authorization, and accounting (AAA) timeout period, in seconds. The value range is from 1 through 60. Default=60.
hold-period *seconds*	Hold period following failed authentication, in seconds. The value range is from 60 through 86400. Default=180.
retransmit *seconds*	Retransmit period, in seconds. The value range is from 1 through 60. Default=3.
revalidation *seconds*	Revalidation period, in seconds. The value range is from 300 through 86400. Default=36000.
status query *seconds*	Status query period after revalidation, in seconds. The value range is from 30 through 1800. Default=300.

Defaults

No default behavior or values

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Examples

The following example shows that the status query period after revalidation is set to 30:

```
Router (config)# eou timeout status query 30
```

Related Commands

Command	Description
show eou	Displays information about EAPoUDP global values.

evaluate

To nest a reflexive access list within an access list, use the **evaluate** command in access-list configuration mode. To remove a nested reflexive access list from the access list, use the **no** form of this command.

evaluate *name*

no evaluate *name*

Syntax Description

name	The name of the reflexive access list that you want evaluated for IP traffic entering your internal network. This is the name defined in the **permit** (reflexive) command.

Defaults

Reflexive access lists are not evaluated.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command is used to achieve reflexive filtering, a form of session filtering.

Before this command will work, you must define the reflexive access list using the **permit** (reflexive) command.

This command nests a reflexive access list within an extended named IP access list.

If you are configuring reflexive access lists for an external interface, the extended named IP access list should be one which is applied to inbound traffic. If you are configuring reflexive access lists for an internal interface, the extended named IP access list should be one which is applied to outbound traffic. (In other words, use the access list opposite of the one used to define the reflexive access list.)

This command allows IP traffic entering your internal network to be evaluated against the reflexive access list. Use this command as an entry (condition statement) in the IP access list; the entry "points" to the reflexive access list to be evaluated.

As with all access list entries, the order of entries is important. Normally, when a packet is evaluated against entries in an access list, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With a reflexive access list nested in an extended access list, the extended access list entries are evaluated sequentially up to the nested entry, then the reflexive access list entries are evaluated sequentially, and then the remaining entries in the extended access list are evaluated sequentially. As usual, after a packet matches *any* of these entries, no more entries will be evaluated.

Examples

The following example shows reflexive filtering at an external interface. This example defines an extended named IP access list *inboundfilters*, and applies it to inbound traffic at the interface. The access list definition permits all Border Gateway Protocol and Enhanced Interior Gateway Routing Protocol traffic, denies all Internet Control Message Protocol traffic, and causes all Transmission Control Protocol traffic to be evaluated against the reflexive access list *tcptraffic*.

If the reflexive access list *tcptraffic* has an entry that matches an inbound packet, the packet will be permitted into the network. *tcptraffic* only has entries that permit inbound traffic for existing TCP sessions.

```
interface Serial 1
 description Access to the Internet via this interface
 ip access-group inboundfilters in
!
ip access-list extended inboundfilters
 permit bgp any any
 permit eigrp any any
 deny icmp any any
 evaluate tcptraffic
```

Related Commands

Command	Description
ip access-list	Defines an IP access list by name.
ip reflexive-list timeout	Specifies the length of time that reflexive access list entries will continue to exist when no packets in the session are detected.
permit (reflexive)	Creates a reflexive access list and enables its temporary entries to be automatically generated.

firewall are-u-there

To add the Firewall-Are-U-There attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls, use the **firewall are-u-there** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To disable the Firewall-Are-U-There attribute, use the **no** form of this command.

firewall are-u-there

no firewall are-u-there

Syntax Description

This command has no arguments or keywords.

Defaults

The server will not send the Firewall-Are-U-There attribute to the client.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

The Firewall-Are-U-There attribute is sent by the Black Ice and Zone Alarm personal firewalls if they are prompted by the server. If connections to the Virtual Private Network (VPN) are for protected devices only, that is, if a PC is running one of these personal firewalls, you should add the attribute to the server group. Devices that do not have a personal firewall will not respond with their capabilities, and their connections will be dropped.

The Firewall-Are-U-There attribute is configured on a Cisco IOS router or in the RADIUS profile.

To configure the Firewall-Are-U-There attribute, use the **firewall are-u-there** command.

An example of an attribute-value (AV) pair for the Firewall-Are-U-There attribute is as follows:

ipsec:firewall=1

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **firewall are-u-there** command.

Note

- The Firewall-Are-U-There attribute can be applied only by a RADIUS user.
- The attribute can be applied on a per-user basis after the user has been authenticated.
- The attribute can override any similar group attributes.
- User-based attributes are available only if RADIUS is used as the database.

Examples

The following example shows that the Firewall-Are-U-There attribute has been configured:

```
crypto isakmp client configuration group group1
 firewall are-u-there
```

Syntax Description

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

fqdn (ca-trustpoint)

To specify a fully qualified domain name (FQDN) that will be included as "unstructuredName" in the certificate request, use the **fqdn** command in ca-trustpoint configuration mode. To remove the FQDN, use the **no** form of this command.

fqdn {*name* **| none}**

no fqdn {*name* **| none}**

Syntax Description

name	FQDN that will be included as "unstructuredName" in the certificate request.
none	Router FQDN will not be included in the certificate request.

Defaults

The FQDN is not configured. The router FQDN will be included as "unstructuredName" in the certificate request.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Before you can issue this command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode. The **fqdn** command is a subcommand that allows you to specify a certificate enrollment parameter. Use the **fqdn** command to include a different FQDN from that of the router in the certificate request or to specify that a FQDN should not be included in the certificate request.

Examples

The following example shows that the FQDN "jack.cisco.com" will be included in the certificate request instead of the router FQDN:

```
crypto ca trustpoint root
 enrollment url http://10.3.0.7:80
 fqdn none
 subject-name CN=jack, OU=PKI, O=Cisco Systems, C=US

crypto ca trustpoint root
 enrollment url http://10.3.0.7:80
 fqdn jack.cisco.com
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

fqdn (crypto identity)

To associate the identity of the router with the host name that the peer used to authenticate itself, use the **fqdn** command in crypto identity configuration mode. To remove this command from your configuration, use the **no** form of this command.

fqdn *name*

no fqdn *name*

Syntax Description

name	Identity used to restrict access to peers with specific certificates.

Defaults

If this command is not enabled, the router can communicate with any encrypted interface that is not restricted on its IP address.

Command Modes

Crypto identity configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use the **fqdn** command to associate the identity of the router, which is defined in the **crypto identity** command, with the distinguished name (DN) in the certificate of the router. This command allows you set restrictions in the router configuration that prevent those peers with specific certificates, especially certificates with particular DNs, from having access to selected encrypted interfaces.

Note The name argument defined in the **crypto identity** command must match the *name* argument defined in the **fqdn** command. That is, the identity of the peer must be the same as the identity in the exchanged certificate.

Examples

The following example shows how to configure a crypto map that can be used only by peers that have been authenticated by hostname and if the certificate belongs to “little.com”:

```
crypto map map-to-little-com 10 ipsec-isakmp
 set peer 172.21.115.119
 set transform-set my-transformset
 match address 125
 identity to-little-com
!
crypto identity to-little-com
 fqdn little.com
```

Related Commands

Command	Description
crypto identity	Configures the identity of the router with a given list of DNs in the certificate of the router.
crypto mib ipsec flowmib history failure size	Associates the identity of the router with the DN in the certificate of the router.

grant auto

To specify automatic certificate enrollment, use the **grant auto** command in certificate server configuration mode. To disable automatic certificate enrollment, use the **no** form of this command.

grant auto

no grant auto

Syntax Description

This command has no arguments or keywords.

Defaults

Certificate enrollment is manual; that is, authorization is required.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **grant auto** command should be used only when testing and building simple networks. This command must be disabled before the network is accessible by the Internet.

Note This command can be used for testing and building simple networks; however, it is recommended that you do not issue this command if your network is generally accessible.

Examples

The following example shows how to enable automatic certificate enrollment for the certificate server "myserver":

```
Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level minimum
Router#(cs-server)# grant auto
% This will cause all certificate requests to be automatically granted.

Are you sure you want to do this? [yes/no]: yes
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

grant auto trustpoint

To specify the certification authority (CA) trustpoint of another vendor from which the Cisco IOS certificate server will automatically grant certificate enrollment requests, use the **grant auto trustpoint** command in certificate server configuration mode.

grant auto trustpoint *label*

Syntax Description

label	Name of the non-Cisco IOS CA trustpoint.

Defaults

No default behavior or values.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

After the network administrator for the server configures and authenticates a trustpoint for the CA of another vendor, the **grant auto trustpoint** command is issued to reference the newly created trustpoint and enroll the router with a Cisco IOS CA.

Note The newly created trustpoint can only be used one time (which occurs when the router is enrolled with the Cisco IOS CA). After the initial enrollment is successfully completed, the credential information will be deleted from the enrollment profile.

The Cisco IOS certificate server will automatically grant only the requests from clients who were already enrolled with the CA of another vendor. All other requests must be manually granted—unless the server is set to be in auto grant mode (via the **grant automatic** command).

Caution The **grant automatic** command can be used for testing and building simple networks and should be disabled before the network is accessible by the Internet. However, it is recommended that you do not issue this command if your network is generally accessible.

Examples

The following example shows how to configure a client router and a Cisco IOS certificate server to exchange enrollment requests via a certificate enrollment profile:

```
! Define the trustpoint "msca-root" that points to the non-Cisco IOS CA and enroll and
! authenticate the client with the non-Cisco IOS CA.
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 ip-address FastEthernet2/0
```

```
 revocation-check crl
!
! Configure trustpoint "cs" for Cisco IOS CA.
crypto pki trustpoint cs
 enrollment profile cs1
 revocation-check crl
!
! Define enrollment profile "cs1," which points to Cisco IOS CA and mention (via the
! enrollment credential command) that "msca-root" is being initially enrolled with the
! Cisco IOS CA.
crypto pki profile enrollment cs1
 enrollment url  http://cs:80
 enrollment credential  msca-root!

! Configure the certificate server, and issue the grant auto trustpoint command to
! instruct the certificate server to accept enrollment request only from clients who are
! already enrolled with trustpoint "msca-root."
crypto pki server cs
 database level minimum
 database url nvram:
 issuer-name CN=cs
 grant auto trustpoint msca-root
!
crypto pki trustpoint cs
 revocation-check crl
rsakeypair cs
!
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 revocation-check crl
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

grant none

To specify all certificate requests to be rejected, use the **grant none** command in certificate server configuration mode. To disable automatic rejection of certificate enrollment, use the **no** form of this command.

grant none

no grant none

Syntax Description

This command has no arguments or keywords.

Defaults

Certificate enrollment is manual; that is, authorization is required.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows how to automatically reject all certificate enrollment requests for the certificate server "myserver":

```
Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level minimum
Router#(cs-server)# grant none
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
grant automatic	Specifies automatic certificate enrollment.

grant ra-auto

To specify that all enrollment requests from a Registration Authority (RA) be granted automatically, use the **grant ra-auto** command in certificate server configuration mode. To disable automatic certificate enrollment, use the **no** form of this command.

grant ra-auto

no grant ra-auto

Syntax Description

This command has no arguments or keywords.

Defaults

Certificate enrollment is manual; that is, authorization is required.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When grant ra-auto mode is configured on the issuing certificate server, ensure that the RA mode certificate server is running in manual grant mode so that enrollment requests are authorized individually by the RA.

Note For the **grant ra-auto** command to work, you have to include "cn=ioscs RA" or "ou=ioscs RA" in the subject name of the RA certificate.

Examples

The following output shows that the issuing certificate server is configured to issue a certificate automatically if the request comes from an RA:

```
Router# (config) crypto pki server myserver
Router-ca (cs-server)# grant ra-auto
% This will cause all certificate requests already authorized by known RAs to be
automatically granted.

Are you sure you want to do this? [yes/no]: y
Router-ca (cs-server)#
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

group (authentication)

To specify the authentication, authorization, and accounting (AAA) TACACS+ server group to use for preauthentication, use the **group** command in AAA preauthentication configuration mode. To remove the **group** command from your configuration, use the **no** form of this command.

group {**tacacs+** *server-group*}

no group {**tacacs+** *server-group*}

Syntax Description

tacacs+	Uses a TACACS+ server for authentication.
server-group	Name of the server group to use for authentication.

Defaults

No method list is configured.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You must configure the **group** command before you configure any other AAA preauthentication command (**clid**, **ctype**, **dnis**, or **dnis bypass**).

Examples

The following example enables Dialed Number Identification Service (DNIS) preauthentication using the abc123 server group and the password aaa-DNIS:

```
aaa preauth
 group abc123
 dnis password aaa-DNIS
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication mode.
dnis (authentication)	Enables AAA preauthentication using DNIS.

group (IKE policy)

To specify the Diffie-Hellman group identifier within an Internet Key Exchange (IKE) policy, use the **group** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command.

group {**1** | **2**}

no group

Syntax Description

1	Specifies the 768-bit Diffie-Hellman group.
2	Specifies the 1024-bit Diffie-Hellman group.

Defaults

768-bit Diffie-Hellman (group 1)

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command to specify the Diffie-Hellman group to be used in an IKE policy.

Examples

The following example configures an IKE policy with the 1024-bit Diffie-Hellman group (all other parameters are set to the defaults):

```
crypto isakmp policy 15
 group 2
 exit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

group (local RADIUS server)

To enter user group configuration mode and to configure shared settings for a user group, use the **group** command in local RADIUS server configuration mode. To remove the group configuration from the local RADIUS server, use the **no** form of this command.

group *group-name*

no group *group-name*

Syntax Description

group-name	Name of user group.

Defaults

No default behavior or values

Command Modes

Local RADIUS server configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following example shows that shared settings are being configured for group “team1”:

```
group team1
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.

Command	Description
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

group (RADIUS)

To specify the authentication, authorization, and accounting (AAA) RADIUS server group to use for preauthentication, use the **group** command in AAA preauthentication configuration mode. To remove the **group** command from your configuration, use the **no** form of this command.

group *server-group*

no group *server-group*

Syntax Description

server-group	Specifies a AAA RADIUS server group.

Defaults

No default behavior or values.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You must configure a RADIUS server group with the **aaa group server radius** command in global configuration mode before using the **group** command in AAA preauthentication configuration mode.

You must configure the **group** command before you configure any other AAA preauthentication command (**clid**, **ctype**, **dnis**, or **dnis bypass**).

Examples

The following example shows the creation of a RADIUS server group called “maestro” and then specifies that DNIS preauthentication be performed using this server group:

```
aaa group server radius maestro
 server 1.1.1.1
 server 2.2.2.2
 server 3.3.3.3

aaa preauth
 group maestro
 dnis required
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
clid	Preauthenticates calls on the basis of the CLID number.
ctype	Preauthenticates calls on the basis of the call type.

Command	Description
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.

group-lock

To allow you to enter your extended authentication (Xauth) username, including the group name, when preshared key authentication is used with Internet Key Exchange (IKE), use the **group-lock** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove the group lock, use the **no** form of this command.

group-lock

no group-lock

Syntax Description

This command has no arguments or keywords.

Defaults

Group lock is not configured.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The Group-Lock attribute can be used if preshared key authentication is used with IKE. When the attribute is enabled, you may enter your extended Xauth username as name/group, name\group, name@group, or name%group. The group that is specified after the delimiter is then compared against the group identifier that is sent during IKE aggressive mode. The groups must match or the connection is rejected.

The Group-Lock attribute is configured on a Cisco IOS router or in the RADIUS profile. This attribute has local (gateway) significance only and is not passed to the client.

The username in the local or RADIUS database must be of the following format:

username[/,\,%,@]group.

To configure the Group-Lock attribute, use the **group-lock** command.

An example of an attribute-value (AV) pair for the Group-Lock attribute is as follows:

```
ipsec:group-lock=1
```

You must enable the **crypto isakmp client configuration group command, which specifies group policy information that has to be defined or changed, before enabling the group-lock command.**

Note

- The Group-Lock attribute can be applied only by a RADIUS user.
- The attribute can be applied on a per-user basis after the user has been authenticated.
- The attribute can override any similar group attributes.

- User-based attributes are available only if RADIUS is used as the database.

Examples

The following example shows that group lock is configured:

```
crypto isakmp client configuration group cisco
  group-lock
```

Syntax Description

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

hash (IKE policy)

To specify the hash algorithm within an Internet Key Exchange policy, use the **hash** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default SHA-1 hash algorithm, use the **no** form of this command.

hash {**sha** | **md5**}

no hash

Syntax Description

sha	Specifies SHA-1 (HMAC variant) as the hash algorithm.
md5	Specifies MD5 (HMAC variant) as the hash algorithm.

Defaults

The SHA-1 hash algorithm

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command to specify the hash algorithm to be used in an IKE policy.

Examples

The following example configures an IKE policy with the MD5 hash algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy 15
 hash md5
 exit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

identity

To set the identity to the crypto map, use the **identity** command in crypto map configuration mode.

identity *name*

Syntax Description

name	Identity used to permit or restrict access for a host to a crypto map.

Defaults

If this command is not enabled, the encrypted connection does not have any restrictions other than the IP address of the encrypting peer.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use the **identity** command to set the identity to the configured crypto maps. When this command is applied, only the hosts that match a configuration listed within the *name* argument can use that crypto map.

Examples

The following example shows how to configure two IP Security (IPSec) crypto maps and apply the identity to each crypto map. That is, the identity is set to “to-bigbiz” for the first crypto map and “to-little-com” for the second crypto map.

```
! The following is an IPSec crypto map (part of IPSec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
 set peer 172.21.114.196
 set transform-set my-transformset
 match address 124
 identity to-bigbiz
!
crypto identity to-bigbiz
 dn ou=BigBiz
!
!
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
 set peer 172.21.115.119
 set transform-set my-transformset
 match address 125
 identity to-little-com
!
crypto identity to-little-com
 fqdn little.com
!
```

Related Commands

Command	Description
crypto identity	Configures the identity of the router with a given list of DNs in the certificate of the router.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto mib ipsec flowmib history failure size	Associates the identity of the router with the DN in the certificate of the router.
fqdn	Associates the identity of the router with the hostname that the peer used to authenticate itself.

identity policy

To create an identity policy and to enter identity policy configuration mode, use the **identity policy** command in global configuration mode. To remove the policy, use the **no** form of this command.

identity policy *policy-name [***access-group** *group-name* | **description** *line-of-description* | **redirect** *url* | **template [virtual-template** *interface-number]]*

no identity policy *policy-name [***access-group** *name* | **description** *line-of-description* | **redirect** *url* | **template [virtual-template** *interface-number]]*

Syntax Description

policy-name	Name of the policy.
access-group *group-name*	(Optional) Access list to be applied.
description *line-of-description*	(Optional) Description of the policy.
redirect *url*	(Optional) Redirects clients to a particular URL.
template	(Optional) Virtual template interface from which commands may be cloned.
virtual-template *interface-number*	(Optional) Virtual template number. The values range from 1 through 200.

Defaults

An identity policy is not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

An identity policy has to be associated with an identity profile.

Examples

The following example shows that an access policy named “greentree” is being created. The access-group attribute is set to “allow-access.” The redirect URL is set to “http://remediate-url.com.” This access policy will be associated with a statically authorized device in the identity profile.

```
Router (config)# identity policy greentree
Router (config-identity-policy)# access-group allow-access
Router (config-identity-policy)# redirect url http://remediate-url.com
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

identity profile

To create an identity profile and to enter identity profile configuration mode, use the **identity profile** command in global configuration mode. To disable an identity profile, use the **no** form of this command.

identity profile {default | dot1x | eapoudp}

no identity profile {default | dot1x | eapoudp}

Syntax Description

default	Service type is default.
dot1x	Service type for 802.1X.
eapoudp	Service type for Extensible Authentication Protocol over UDP (EAPoUDP).

Defaults

An identity profile is not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	The **eapoudp** keyword was added.

Usage Guidelines

The **identity profile** command and **default** keyword allow you to configure static MAC addresses of a client computer that does not support 802.1X and to authorize or unauthorize them statically. After you have issued the **identity profile** command and **default** keyword and are in identity profile configuration mode, you can specify the configuration of a template that can be used to create the virtual access interface to which unauthenticated supplicants (client computers) will be mapped.

The **identity profile** command and the **dot1x** keyword are used by the supplicant and authenticator. Using the **dot1x** keyword, you can set the username, password, or other identity-related information for an 802.1X authentication.

Using the **identity profile** command and the **eapoudp** keyword, you can statically authenticate or unauthenticate a device either on the basis of the device IP address or MAC address or on the type, and the corresponding network access policy can be specified using the **identity policy** command.

Examples

The following example shows that an identity profile and its description have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# description description_entered_here
```

The following example shows that an EAP username has been entered:

```
Router (config)# identity policy dot1x
```

```
Router (config-identity-prof)# eap username user1
```

The following example shows that an EAPoUDP identity profile has been created:

```
Router (config)# identity policy eapoudp
```

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
description	Enters an 802.1X description.
device	Statically authorizes or rejects individual devices.
dot1x initialize	Initializes an interface.
dot1x max-req	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC.
dot1x max-start	Sets the maximum number of times that the router sends an EAP start frame to the client before concluding that the other end is 802.1X unaware.
dot1x pae	Sets the PAE type.
dot1x port-control	Sets an 802.1X port control value.
dot1x re-authenticate	Reauthenticates an 802.1X interface.
dot1x reauthentication	Enables periodic reauthentication of the client PCs on the interface.
dot1x system-auth-control	Enables 802.1X SystemAuthControl (port-based authentication).
dot1x timeout	Sets retry timeouts.
eap	Specifies EAP-specific parameters.
identity policy	Creates an identity policy.
show dot1x	Shows details and statistics for an identity profile.
template	Specifies a virtual template from which commands may be cloned.

identity profile eapoudp

To create an identity profile and to enter Extensible Authentication Protocol over UDP (EAPoUDP) profile configuration mode, use the **identity profile eapoudp** command in global configuration mode. To remove the policy, use the **no** form of this command.

identity profile eapoudp

no identity profile eapoudp

Syntax Description

This command has no arguments or keywords.

Defaults

No EAPoUDP identity profile exists.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Using this command, you can statically authenticate or unauthenticate a device either on the basis of the device IP address or MAC address or on the type, and the corresponding network access policy can be specified using the **identity policy** command.

Examples

The following example shows that an EAPoUDP identity profile has been created:

```
Router (config)# identity profile eapoudp
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

include-local-lan

To configure the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client, use the **include-local-lan** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To disable the attribute that allows the nonsplit-tunneling connection, use the **no** form of this command.

include-local-lan

no include-local-lan

Syntax Description

This command has no arguments or keywords.

Defaults

A nonsplit-tunneling connection is not able to access the local subnet at the same time as the client.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

If split tunneling is not in use (that is, the SPLIT_INCLUDE attribute was not negotiated), you lose not only Internet access, but also access to resources on the local subnetworks. The Include-Local-LAN attribute allows the server to push the attribute to the client, which allows for a nonsplit-tunneling connection to access the local subnetwork at the same time as the client (that is, the connection is to the subnetwork to which the client is directly attached).

The Include-Local-LAN attribute is configured on a Cisco IOS router or in the RADIUS profile.

To configure the Include-Local-LAN attribute, use the **include-local-lan** command.

An example of an attribute-value (AV) pair for the Include-Local-LAN attribute is as follows:

```
ipsec:include-local-lan=1
```

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **include-local-lan** command.

Note

- The Include-Local-LAN attribute can be applied only by a RADIUS user.
- The attribute can be applied on a per-user basis after the user has been authenticated.
- The attribute can override any similar group attributes.
- User-based attributes are available only if RADIUS is used as the database.

Examples

The following example shows that the Include-Local-LAN has been configured:

```
crypto isakmp client configuration group cisco
 include-local-lan
```

Syntax Description

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

incoming

To configure filtering for incoming IP traffic, use the **incoming** command in router IP traffic export (RITE) configuration mode. To disable filtering for incoming traffic, use the **no** form of this command.

incoming {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}

no incoming {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}

Syntax Description

access-list {*standard* | *extended* | *named*}	An existing numbered (standard or extended) or named access control list (ACL). **Note** The filter is applied only to exported traffic, not normal router traffic.
sample one-in-every *packet-number*	Exports only one packet out of every specified number of packets. Valid range for the *packet-number* argument is 2 to 2147483647 packets. By default, all traffic is exported.

Defaults

If this command is not enabled, all incoming IP traffic will be filtered via sampling.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

When configuring a network device for exporting IP traffic, you can issue the **incoming** command to filter unwanted traffic via the following methods:

- ACLs, which accept or deny an IP packet for export
- Sampling, which allows you to export one in every few packets in which you are interested. Use this option when it is not necessary to export all incoming traffic. Also, sampling is useful when a monitored ingress interface can send traffic faster than the egress interface can transmit it.

Examples

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the ACL “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
```

```
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
outgoing	Configures filtering for outgoing export traffic.

initiate-mode

To configure the Phase 1 mode of an Internet Key Exchange (IKE), use the **initiate-mode** command in ISAKMP profile configuration mode. To remove the mode that was configured, use the **no** form of this command.

initiate-mode aggressive

no initiate-mode aggressive

Syntax Description

aggressive	Aggressive mode is initiated.

Defaults

IKE initiates main mode.

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use this command if you want to initiate an IKE aggressive mode exchange instead of a main mode exchange.

Examples

The following example shows that aggressive mode has been configured:

```
crypto isakmp profile vpnprofile
 initiate-mode aggressive
```

interface (RITE)

To specify the outgoing interface for exporting traffic, use the **interface** command in router IP traffic export (RITE) configuration mode. To disable an interface, use the **no** form of this command.

interface *interface-name*

no interface *interface-name*

Syntax Description

interface-name	Name of interface in which IP packets are exported.

Defaults

If this command is not enabled, the exported IP traffic profile does not recognize an interface in which to send captured IP traffic.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

After you configure an IP traffic export profile via the **ip traffic-export profile** global configuration command, you should issue the **interface** command; otherwise, the profile will be unable to export the captured IP packets. If you do not specify the **interface** command, you will receive a warning, which states that the profile is incomplete, when you attempt to apply the profile to an interface via the **ip traffic-export apply profile** interface configuration command.

Note Currently, only Ethernet and Fast Ethernet interfaces are supported.

Examples

The following example shows how to configure the profile "corp1," which will send captured IP traffic to host "00a.8aab.90a0" at the interface "FastEthernet 0/1." This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the access control list ACL "ham_ACL."

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
ip traffic-export apply profile	Applies an IP traffic export profile to a specific interface.
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.

ip-address (ca-trustpoint)

To specify a dotted IP address or an interface that will be included as "unstructuredAddress" in the certificate request, use the **ip-address** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

ip-address {*ip-address* | *interface* | **none**]

no ip-address

Syntax Description

ip-address	Specifies a dotted IP address that will be included as "unstructuredAddress" in the certificate request.
interface	Specifies an interface, from which the router can get an IP address, that will be included as "unstructuredAddress" in the certificate request.
none	**Specifies that an IP address is not to be included in the certificate request.**

Defaults

An IP address is not configured. You will be prompted for the IP address during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Before you can issue this command, you must enable the **crypto ca | pki trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode. The **ip-address** command is a subcommand that allows you to specify a certificate enrollment parameter.

Use the **ip-address** command to include the IP address of the specified interface in the certificate request or to specify that an IP address should not be included in the certificate request.

If this command is enabled, you will not be prompted for an IP address during certificate enrollment.

Examples

The following example shows how to include the IP address of the Ethernet-0 interface in the certificate request for the trustpoint "frog":

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
```

The following example shows that an IP address is not to be included in the certificate request:

```
crypto ca trustpoint root
 enrollment url http://10.3.0.7:80
```

```
fqdn none
ip-address none
subject-name CN=subject1, OU=PKI, O=Cisco Systems, C=US
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

ip admission

To create a Layer 3 network admission control rule to be applied to the interface, use the **ip admission** command in interface configuration mode. To remove the admission control rule, use the **no** form of this command.

ip admission *admission-name*

no ip admission *admission-name*

Syntax Description

admission-name	Authentication or admission rule name.

Defaults

A network admission control rule is not applied to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The admission rule defines how you apply admission control.

Examples

The following example shows that a network admission control rule named “greentree” is to be applied to the interface:

```
Router (config-if)# ip admission greentree
```

Related Commands

Command	Description
interface	Defines an interface.

ip admission name

To create an IP network admission control rule, use the **ip admission name** command in global configuration mode. To remove the network admission control rule, use the **no** form of this command.

ip admission name *admission-name [***eapoudp** | **proxy** *{***ftp** | **http** | **telnet***}] [***list** *{acl | acl-name}]*

no ip admission name *admission-name [***eapoudp** | **proxy** *{***ftp** | **http** | **telnet***}] [***list** *{acl | acl-name}]*

Syntax Description

admission-name	Name of network admission control rule.
eapoudp	(Optional) Specifies IP network admission control using Extensible Authentication Protocol over UDP (EAPoUDP).
proxy	(Optional) Specifies authentication proxy.
ftp	Specifies that FTP is to be used to trigger the authentication proxy.
http	Specifies that HTTP is to be used to trigger authentication proxy.
telnet	Specified that Telnet is to be used to trigger authentication proxy.
list	(Optional) Associates the named rule with an access control list (ACL).
acl	Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199.
acl-name	Applies a named access list to a named admission control rule.

Defaults

An IP network admission control rule is not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The admission rule defines how you apply admission control.

You can associate the named rule with an ACL, providing control over which hosts use the admission control feature. If no standard access list is defined, the named admission rule intercepts IP traffic from all hosts whose connection-initiating packets are received at the configured interface.

The **list** keyword option allows you to apply a standard, extended (1 through 199) or named access list to a named admission control rule. IP connections that are initiated by hosts in the access list are intercepted by the admission control feature.

Examples

The following example shows that an IP admission control rule is named “greentree” and that it is associated with ACL “101.” Any IP traffic that is destined to a previously configured network (using the **access-list** command) will be subjected to antivirus state validation using EAPoUDP.

```
Router (config)# ip admission name greentree eapoudp list 101
```

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.

ip audit attack

To specify the default actions for attack signatures, use the **ip audit attack** command in global configuration mode. To set the default action for attack signatures, use the **no** form of this command.

ip audit attack {**action** [**alarm**] [**drop**] [**reset**]}

no ip audit attack

Syntax Description

action	Specifies an action for the attack signature to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the **action** keyword.
drop	(Optional) Drops the packet. Used with the **action** keyword.
reset	(Optional) Resets the TCP session. Used with the **action** keyword.

Defaults

The default action is **alarm**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **ip audit attack** global configuration command to specify the default actions for attack signatures.

Examples

In the following example, the default action for attack signatures is set to all three actions:

```
ip audit attack action alarm drop reset
```

ip audit info

To specify the default actions for info signatures, use the **ip audit info** command in global configuration mode. To set the default action for info signatures, use the **no** form of this command.

ip audit info {**action** [**alarm**] [**drop**] [**reset**]}

no ip audit info

Syntax Description

action	Sets an action for the info signature to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the **action** keyword.
drop	(Optional) Drops the packet. Used with the **action** keyword.
reset	(Optional) Resets the TCP session. Used with the **action** keyword.

Defaults

The default action is **alarm**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **ip audit info** global configuration command to specify the default actions for info signatures.

Examples

In the following example, the default action for info signatures is set to all three actions:

```
ip audit info action alarm drop reset
```

ip audit smtp

To specify the number of recipients in a mail message over which a spam attack is suspected, use the **ip audit smtp** command in global configuration mode. To set the number of recipients to the default setting, use the **no** form of this command.

ip audit smtp spam *number-of-recipients*

no ip audit smtp spam

Syntax Description

spam	Specifies a threshold beyond which the Cisco IOS Firewall IDS alarms on spam e-mail.
number-of-recipients	Integer in the range of 1 to 65535 that designates the maximum number of recipients in a mail message before a spam attack is suspected. Use with the **spam** keyword. The default is 250 recipients.

Defaults

The default number of recipients is 250.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **ip audit smtp** global configuration command to specify the number of recipients in a mail message over which a spam attack is suspected.

Examples

In the following example, the number of recipients is set to 300:

```
ip audit smtp spam 300
```

ip auth-proxy (global configuration)

To set the authentication proxy idle timeout value (the length of time an authentication cache entry, along with its associated dynamic user access control list, is managed after a period of inactivity), use the **ip auth-proxy** command in global configuration mode. To set the default value, use the **no** form of this command.

ip auth-proxy {**inactivity-timer** *min* | **absolute-timer** *min*}

no ip auth-proxy {**inactivity-timer** | **absolute-timer**}

Syntax Description

inactivity-timer *min*	Specifies the length of time in minutes that an authentication cache entry, along with its associated dynamic user access control list (ACL), is managed after a period of inactivity. Enter a value in the range 1 to 2,147,483,647. The default value is 60 minutes. **Note** This option deprecates the **auth-cache-time** *min* option.
absolute-timer *min*	Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 1 to 65,535 minutes (45 and a half days). The default value is 0 minutes.

Defaults

The default value of the **inactivity-timer** *min* option is 60 minutes.

The default value of the **absolute-timer** *min* option is 0 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	The **inactivity-timer** *min* and **absolute-timer** *min* options were added.

Usage Guidelines

Use this command to set the global idle timeout value for the authentication proxy. You must set the value of the **inactivity-timer** *min* option to a higher value than the idle timeout of any Context-Based Access Control (CBAC) protocols. Otherwise, when the authentication proxy removes the user profile along associated dynamic user ACLs, there might be some idle connections monitored by CBAC. Removing these user-specific ACLs could cause those idle connections to hang. If the CBAC idle timeout value is shorter, CBAC resets these connections when the CBAC idle timeout expires, which is before the authentication proxy removes the user profile.

The **absolute-timer** *min* option allows users to configure a window during which the authentication proxy on the enabled interface is active. Once the absolute timer expires, the authentication proxy will be disabled regardless of any activity. The global absolute timeout value can be overridden by the local (per protocol) value, which is enabled via the **ip auth-proxy name** command. The absolute timer is turned off by default, and the authentication proxy is enabled indefinitely.

Examples

The following example sets the inactivity timeout to 30 minutes:

```
ip auth-proxy inactivity-timer 30
```

Related Commands

Command	Description
ip auth-proxy name	Creates an authentication proxy rule.
show ip auth-proxy configuration	Displays the authentication proxy entries or the running authentication proxy configuration.

ip auth-proxy (interface configuration)

To apply an authentication proxy rule at a firewall interface, use the **ip auth-proxy** command in interface configuration mode. To remove the authentication proxy rules, use the **no** form of this command.

ip auth-proxy *auth-proxy-name*

no ip auth-proxy *auth-proxy-name*

Syntax Description

auth-proxy-name	Specifies the name of the authentication proxy rule to apply to the interface configuration. The authentication proxy rule is established with the **ip auth-proxy name** command.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **ip auth-proxy** command to enable the named authentication proxy rule at the firewall interface. Traffic passing through the interface from hosts with an IP address matching the standard access list and protocol type (HTTP) is intercepted for authentication if no corresponding authentication cache entry exists. If no access list is defined, the authentication proxy intercepts traffic from all hosts whose connection initiating packets are received at the configured interface.

Use the **no** form of this command with a rule name to disable the authentication proxy for a given rule on a specific interface. If a rule is not specified, the **no** form of this command disables the authentication proxy on the interface.

Examples

The following example configures interface Ethernet0 with the HQ_users rule:

```
interface e0
 ip address 172.21.127.210 255.255.255.0
 ip access-group 111 in
 ip auth-proxy HQ_users
 ip nat inside
```

Related Commands

Command	Description
ip auth-proxy name	Creates an authentication proxy rule.

ip auth-proxy auth-proxy-banner

To display a banner, such as the router name, in the authentication proxy login page, use the **ip auth-proxy auth-proxy-banner** command in global configuration mode. To disable display of the banner, use the **no** form of this command.

ip auth-proxy auth-proxy-banner {**ftp** | **http** | **telnet**} [*banner-text*]

no ip auth-proxy auth-proxy-banner {**ftp** | **http** | **telnet**}

Syntax Description

ftp	Specifies the FTP protocol.
http	Specifies the HTTP protocol.
telnet	Specifies the Telnet protocol.
banner-text	(Optional) Specifies a text string to replace the default banner, which is the name of the router. The text string should be written in the following format: "C banner-text C," where "C" is a delimiting character.

Defaults

This command is not enabled, and a banner is not displayed on the authentication proxy login page.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	The following keywords were added: **ftp**, **http**, and **telnet**.

Usage Guidelines

The **ip auth-proxy auth-proxy-banner** command allows users to configure one of two possible scenarios:

- The **ip auth-proxy auth-proxy-banner** command is enabled.

  In this scenario, the administrator has not supplied any text. Thus, a default banner that states the following: "Cisco Systems, <router's hostname> Authentication" will be displayed in the authentication proxy login page. This scenario is most commonly used.

- The **ip auth-proxy auth-proxy-banner** command with the *banner-text* argument is enabled.

  In this scenario, the administrator can supply multiline text that will be converted to HTML by the auth-proxy parser code. Thus, *only* the multiline text will displayed in the authentication proxy login page. You will *not* see the default banner, "Cisco Systems, <router's hostname> Authentication."

Note If the **ip auth-proxy auth-proxy-banner** command is not enabled, there will not be any banner configuration. Thus, nothing will be displayed to the user on authentication proxy login page except a text box to enter the username and a text box to enter the password.

Examples

The following example causes the router name to be displayed in the authentication proxy login page:

```
ip auth-proxy auth-proxy-banner ftp
```

The following example shows how to specify the custom banner “whozat” to be displayed in the authentication proxy login page:

```
ip auth-proxy auth-proxy-banner telnet CwhozatC
```

Related Commands

Command	Description
ip auth-proxy name	Creates an authentication proxy rule.

ip auth-proxy name

To create an authentication proxy rule, use the **ip auth-proxy name** command in global configuration mode. To remove the authentication proxy rules, use the **no** form of this command.

ip auth-proxy name *auth-proxy-name* {**ftp** | **http** | **telnet**} [**inactivity-timer** *min*] [**absolute-timer** *min*] [**list** {*acl* | *acl-name*}]

no ip auth-proxy name *auth-proxy-name*

Syntax Description

auth-proxy-name	Associates a name with an authentication proxy rule. Enter a name of up to 16 alphanumeric characters.
ftp	Specifies FTP to trigger the authentication proxy.
http	Specifies HTTP to trigger the authentication proxy.
telnet	Specifies Telnet to trigger the authentication proxy.
inactivity-timer *min*	(Optional) Overrides the global authentication proxy cache timer for a specific authentication proxy name, offering more control over timeout values. Enter a value in the range 1 to 2,147,483,647. The default value is equal to the value set with the **ip auth-proxy** command. **Note** This option deprecates the **auth-cache-time** *min* option.
absolute-timer *min*	(Optional) Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 1 to 65,535 minutes (45 and a half days). The default value is 0 minutes.
list {*acl* | *acl-name*}	(Optional) Specifies a standard (1–99), extended (1–199), or named IP access list to use with the authentication proxy. With this option, the authentication proxy is applied only to those hosts in the access list. If no list is specified, all connections initiating HTTP, FTP, or Telnet traffic arriving at the interface are subject to authentication.

Defaults

The default value is equal to the value set with the **ip auth-proxy auth-cache-time** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2	Support for named and extend access lists was introduced.
12.3(1)	The following keywords were introduced: • **ftp** • **telnet** • **inactivity-timer** *min* • **absolute-timer** *min*

Usage Guidelines

This command creates a named authentication proxy rule, and it allows you to associate that rule with an access control list (ACL), providing control over which hosts use the authentication proxy. The rule is applied to an interface on a router using the **ip auth-proxy** command.

Use the **inactivity-timer** *min* option to override the global the authentication proxy cache timer. This option provides control over timeout values for specific authentication proxy rules. The authentication proxy cache timer monitors the length of time (in minutes) that an authentication cache entry, along with its associated dynamic user access control list, is managed after a period of inactivity. When that period of inactivity (idle time) expires, the authentication entry and the associated dynamic access lists are deleted.

Use the **list** option to associate a set of specific IP addresses or a named ACL with the **ip auth-proxy name** command.

Use the **no** form of this command with a rule name to remove the authentication proxy rules. If no rule is specified, the **no** form of this command removes all the authentication rules on the router, and disables the proxy at all interfaces.

Note You must use the **aaa authorization auth-proxy** command together with the **ip auth-proxy name** command. Together these commands set up the authorization policy to be retrieved by the firewall. Refer to the **aaa authorization auth-proxy** command for more information.

Examples

The following example creates the HQ_users authentication proxy rule. Because an access list is not specified in the rule, all connection-initiating HTTP traffic is subjected to authentication.

```
ip auth-proxy name HQ_users http
```

The following example creates the Mfg_users authentication proxy rule and applies it to hosts specified in ACL 10:

```
access-list 10 192.168.7.0 0.0.0.255
ip auth-proxy name Mfg_users http list 10
```

The following example sets the timeout value for Mfg_users to 30 minutes:

```
access-list 15 any
ip auth-proxy name Mfg_users http inactivity-timer 30 list 15
```

The following example disables the Mfg_users rule:

```
no ip auth-proxy name Mfg_users
```

The following example disables the authentication proxy at all interfaces and removes all the rules from the router configuration:

```
no ip auth-proxy
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict network access to a user.
ip auth-proxy (global)	Sets the authentication proxy idle timeout value (the length of time an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity).

Command	Description
ip auth-proxy (interface)	Applies an authentication proxy rule at a firewall interface.
show ip auth-proxy configuration	Displays the authentication proxy entries or the running authentication proxy configuration.

ip http ezvpn

To enable the Cisco Easy VPN remote web server interface, use the **ip http ezvpn** command in global configuration mode. To disable the Cisco Easy VPN remote web server interface, use the **no** form of this command.

Cisco uBR905 and Cisco BR925 cable access routers

ip http ezvpn

no ip http ezvpn

Syntax Description

This command has no keywords or arguments.

Defaults

The Cisco Easy VPN Remote web server interface is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YJ	This command was introduced for the Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

This command enables the Cisco Easy VPN Remote web server, an onboard web server that allows users to connect an IPSec Easy VPN tunnel and to provide the required authentication information. The Cisco Easy VPN Remote web server allows the user to perform these functions without having to use the Cisco command-line interface (CLI).

Before using this command, you must first enable the Cisco web server that is onboard the cable access router by entering the **ip http server** command. Then use the **ip http ezvpn** command to enable the Cisco Easy VPN remote web server. You can then access the web server by entering the IP address for the Ethernet interface of the router in your web browser.

Note The Cisco Easy VPN Remote web interface does not work with the cable monitor web interface in Cisco IOS Release 12.2(8)YJ. To access the cable monitor web interface, you must first disable the Cisco Easy VPN remote web interface with the **no ip http ezvpn** command, and then enable the cable monitor with the **ip http cable-monitor** command.

Examples

The following example shows how to enable the Cisco Easy VPN remote web server interface:

```
Router# configure terminal
Router(config)# ip http server
Router(config)# ip http ezvpn
Router(config)# exit
```

```
Router# copy running-config startup-config
```

Related Commands

Command	Description
ip http cable-monitor	Enables and disables the Cable Monitor Web Server feature.
ip http port	Configures the TCP port number for the HTTP web server of the router.
ip http server	Enables and disables the HTTP web server of the router.

ip inspect

To apply a set of inspection rules to an interface, use the **ip inspect** command in interface configuration mode. To remove the set of rules from the interface, use the **no** form of this command.

ip inspect *inspection-name* {**in** | **out**}

no ip inspect *inspection-name* {**in** | **out**}

Syntax Description

inspection-name	Identifies which set of inspection rules to apply.
in	Applies the inspection rules to inbound traffic.
out	Applies the inspection rules to outbound traffic.

Defaults

If no set of inspection rules is applied to an interface, no traffic will be inspected by CBAC.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to apply a set of inspection rules to an interface.

Typically, if the interface connects to the external network, you apply the inspection rules to outbound traffic; alternately, if the interface connects to the internal network, you apply the inspection rules to inbound traffic.

If you apply the rules to outbound traffic, then return inbound packets will be permitted if they belong to a valid connection with existing state information. This connection must be initiated with an outbound packet.

If you apply the rules to inbound traffic, then return outbound packets will be permitted if they belong to a valid connection with existing state information. This connection must be initiated with an inbound packet.

Examples

The following example applies a set of inspection rules named “outboundrules” to an external interface’s outbound traffic. This causes inbound IP traffic to be permitted only if the traffic is part of an existing session, and to be denied if the traffic is not part of an existing session.

```
interface serial0
 ip inspect outboundrules out
```

Related Commands

Command	Description
ip inspect name	Defines a set of inspection rules.

ip inspect alert-off

To disable Context-based Access Control (CBAC) alert messages, which are displayed on the console, use the **ip inspect alert-off** command in global configuration mode. To enable CBAC alert messages, use the **no** form of this command.

ip inspect alert-off

no ip inspect alert-off

Syntax Description

This command has no arguments or keywords.

Defaults

Alert messages are displayed.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following example turns on CBAC alert messages:

```
ip inspect alert-off
```

ip inspect audit trail

To turn on Context-based Access Control (CBAC) audit trail messages, which will be displayed on the console after each CBAC session closes, use the **ip inspect audit trail** command in global configuration mode. To turn off CBAC audit trail message, use the **no** form of this command.

ip inspect audit trail

no ip inspect audit trail

Syntax Description

This command has no arguments or keywords.

Defaults

Audit trail messages are not displayed.

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

Use this command to turn on CBAC audit trail messages.

Examples

The following example turns on CBAC audit trail messages:

```
ip inspect audit trail
```

Afterward, audit trail messages such as the following are displayed:

```
%FW-6-SESS_AUDIT_TRAIL: tcp session initiator (192.168.1.13:33192) sent 22 bytes --
responder (192.168.129.11:25) sent 208 bytes
%FW-6-SESS_AUDIT_TRAIL: ftp session initiator 192.168.1.13:33194) sent 336 bytes --
responder (192.168.129.11:21) sent 325 bytes
```

These messages are examples of audit trail messages. To determine which protocol was inspected, refer to the responder's port number. The port number follows the responder's IP address.

ip inspect dns-timeout

To specify the Domain Name System (DNS) idle timeout (the length of time during which a DNS name lookup session will still be managed while there is no activity), use the **ip inspect dns-timeout** command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

ip inspect dns-timeout *seconds*

no ip inspect dns-timeout

Syntax Description

seconds	Specifies the length of time in seconds, for which a DNS name lookup session will still be managed while there is no activity. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

When the software detects a valid User Datagram Protocol packet for a new DNS name lookup session, if Context-based Access Control (CBAC) inspection is configured for UDP, the software establishes state information for the new DNS session.

If the software detects no packets for the DNS session for a time period defined by the DNS idle timeout, the software will not continue to manage state information for the session.

The DNS idle timeout applies to all DNS name lookup sessions inspected by CBAC.

The DNS idle timeout value overrides the global UDP timeout. The DNS idle timeout value also enters aggressive mode and overrides any timeouts specified for specific interfaces when you define a set of inspection rules with the **ip inspect name** command.

Examples

The following example sets the DNS idle timeout to 30 seconds:

```
ip inspect dns-timeout 30
```

The following example sets the DNS idle timeout back to the default (5 seconds):

```
no ip inspect dns-timeout
```

ip inspect hashtable

To change the size of the session hash table, use the **ip inspect hashtable** command in global configuration mode. To restore the size of the session hash table to the default, use the **no** form of this command.

ip inspect hashtable *number*

no ip inspect hashtable *number*

Syntax Description

number	Size of the hash table in terms of buckets. Possible values for the hash table are 1024, 2048, 4096, and 8192; the default value is 1024.

Defaults

1024 buckets

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **ip inspect hashtable** command to increase the size of the hash table when the number of concurrent sessions increases or to reduce the search time for the session. Collisions in a hash table result in poor hash function distribution because many entries are hashed into the same bucket for certain patterns of addresses. Even if a hash function distribution evenly dispenses the input across all of the buckets, a small hash table size will not scale well if there are a large number of sessions. As the number of sessions increase, the collisions increase, which increases the length of the linked lists, thereby, deteriorating the throughput performance.

Note You should increase the hash table size when the total number of sessions running through the context-based access control (CBAC) router is approximately twice the current hash size; decrease the hash table size when the total number of sessions is reduced to approximately half the current hash size. Essentially, try to maintain a 1:1 ratio between the number of sessions and the size of the hash table.

Examples

The following example shows how to change the size of the session hash table to 2048 buckets:

```
ip inspect hashtable 2048
```

ip inspect L2-transparent dhcp-passthrough

To allow a transparent firewall to forward Dynamic Host Control Protocol (DHCP) pass-through traffic, use the **ip inspect L2-transparent dhcp-passthrough** command in global configuration mode. To return to the default functionality, use the **no** form of this command.

ip inspect L2-transparent dhcp-passthrough

no ip inspect L2-transparent dhcp-passthrough

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not enabled; thus, DHCP packets are forwarded or denied according to the configured access control list (ACL).

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

A transparent firewall allows a Cisco IOS Firewall (a Layer 3 device) to operate as a Layer 2 firewall in bridging mode. Thus, the firewall can exist "transparently" to a network, no longer requiring users to reconfigure their statically defined network devices.

The **ip inspect L2-transparent dhcp-passthrough** command overrides the ACL for DHCP packets; that is, DHCP packets are forwarded even if the ACL is configured to deny all IP packets. Thus, this command can be used to enable a transparent firewall to forward DHCP packets across the bridge without inspection so clients on one side of the bridge can get an IP address from a DHCP server on the opposite side of the bridge.

Examples

Allowing DHCP Pass-Through Traffic

In this example, the static IP address of the client is removed, and the address is acquired via DHCP using the **ip address dhcp** command on the interface that is connected to the transparent firewall.

```
Router# show debug
ARP:
  ARP packet debugging is on
L2 Inspection:
  INSPECT L2 firewall debugging is on
  INSPECT L2 firewall DHCP debugging is on
Router#
Router#
! Configure DHCP passthrough
Router(config)# ip insp L2-transparent dhcp-passthrough
```

```
! The DHCP discover broadcast packet arrives from the client. Since this packet is a
! broadcast (255.255.255.255), it arrives in the flood path
*Mar  1 00:35:01.299:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar  1 00:35:01.299:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar  1 00:35:01.299:L2FW:udp ports src 68 dst 67
*Mar  1 00:35:01.299:L2FW:src 0.0.0.0 dst 255.255.255.255
! The DHCP pass through flag is checked and the packet is allowed
*Mar  1 00:35:01.299:L2FW:DHCP packet seen. Pass-through flag allows the packet
! The packet is a broadcast packet and therefore not sent to CBAC
*Mar  1 00:35:01.299:L2FW*:Packet is broadcast or multicast.PASS
! The DHCP server 97.0.0.23 responds to the client's request
*Mar  1 00:35:01.303:L2FW:insp_l2_flood:input is Ethernet1 output is Ethernet0
*Mar  1 00:35:01.303:L2FW*:Src 97.0.0.23 dst 255.255.255.255 protocol udp
*Mar  1 00:35:01.307:L2FW:udp ports src 67 dst 68
*Mar  1 00:35:01.307:L2FW:src 97.0.0.23 dst 255.255.255.255
*Mar  1 00:35:01.307:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar  1 00:35:01.307:L2FW*:Packet is broadcast or multicast.PASS
*Mar  1 00:35:01.311:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar  1 00:35:01.311:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar  1 00:35:01.311:L2FW:udp ports src 68 dst 67
*Mar  1 00:35:01.311:L2FW:src 0.0.0.0 dst 255.255.255.255
*Mar  1 00:35:01.315:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar  1 00:35:01.315:L2FW*:Packet is broadcast or multicast.PASS
*Mar  1 00:35:01.315:L2FW:insp_l2_flood:input is Ethernet1 output is Ethernet0
*Mar  1 00:35:01.323:L2FW*:Src 97.0.0.23 dst 255.255.255.255 protocol udp
*Mar  1 00:35:01.323:L2FW:udp ports src 67 dst 68
*Mar  1 00:35:01.323:L2FW:src 97.0.0.23 dst 255.255.255.255
*Mar  1 00:35:01.323:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar  1 00:35:01.323:L2FW*:Packet is broadcast or multicast.PASS
! The client has an IP address (97.0.0.5) and has issued a G-ARP to let everyone know it's
address
*Mar  1 00:35:01.327:IP ARP:rcvd rep src 97.0.0.5 0008.a3b6.b603, dst 97.0.0.5 BVI1
Router#
```

Denying DHCP Pass-Through Traffic

In this example, DHCP pass-through traffic is not allowed (via the **no ip inspect L2-transparent dhcp-passthrough** command). The client is denied when it attempts to acquire a DHCP address from the server.

```
! Deny DHCP pass-through traffic
Router(config)# no ip inspect L2-transparent dhcp-passthrough

! The DHCP discover broadcast packet arrives from the client
*Mar  1 00:36:40.003:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar  1 00:36:40.003:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar  1 00:36:40.003:L2FW:udp ports src 68 dst 67
*Mar  1 00:36:40.007:L2FW:src 0.0.0.0 dst 255.255.255.255
! The pass-through flag is checked
*Mar  1 00:36:40.007:L2FW:DHCP packet seen. Pass-through flag denies the packet
! The packet is dropped because the flag does not allow DHCP passthrough traffic. Thus,
! the client cannot acquire an address, and it times out
*Mar  1 00:36:40.007:L2FW:FLOOD Dropping the packet after ACL check.
```

Related Commands

Command	Description
debug ip inspect L2-transparent	Enables debugging messages for transparent firewall events.
show ip inspect	Displays Cisco IOS Firewall configuration and session information.

ip inspect max-incomplete high

To define the number of existing half-open sessions that will cause the software to start deleting half-open sessions, use the **ip inspect max-incomplete high** command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the **no** form of this command.

ip inspect max-incomplete high *number*

no ip inspect max-incomplete high

Syntax Description

number	Specifies the number of existing half-open sessions that will cause the software to start deleting half-open sessions. The default is 500 half-open sessions.

Defaults

500 half-open sessions

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

```
ip inspect max-incomplete high 900
ip inspect max-incomplete low 800
```

Related Commands

Command	Description
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ip inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ip inspect max-incomplete low

To define the number of existing half-open sessions that will cause the software to stop deleting half-open sessions, use the **ip inspect max-incomplete low** command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command.

ip inspect max-incomplete low *number*

no ip inspect max-incomplete low

Syntax Description

number	Specifies the number of existing half-open sessions that will cause the software to stop deleting half-open sessions. The default is 400 half-open sessions.

Defaults

400 half-open sessions

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

```
ip inspect max-incomplete high 900
ip inspect max-incomplete low 800
```

Related Commands

Command	Description
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ip inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ip inspect name

To define a set of inspection rules, use the **ip inspect name** command in global configuration mode. To remove the inspection rule for a protocol or to remove the entire set of inspection rules, use the **no** form of this command.

ip inspect name *inspection-name protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]

no ip inspect name [*inspection-name protocol*]

HTTP Inspection Syntax

ip inspect name *inspection-name* **http** [**urlfilter**] [**java-list** *access-list*] [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]

no ip inspect name *inspection-name protocol*

SMTP and ESMTP Inspection Syntax

ip inspect name *inspection-name* {**smtp** | **esmtp**} [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**max-data** *number*] [**timeout** *seconds*]

remote-procedure call (RPC) Inspection Syntax

ip inspect name *inspection-name* **rpc program-number** *number* [**wait-time** *minutes*] [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]

no ip inspect name *inspection-name protocol*

Fragment Inspection Syntax

ip inspect name *inspection-name* **fragment** [**max** *number* **timeout** *seconds*]

no ip inspect name *inspection-name* **fragment**

Syntax Description

inspection-name	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same *inspection-name* as the existing set of rules. **Note** The *inspection-name* cannot exceed 16 characters; otherwise, the name will be truncated to the 16-character limit.
protocol	A protocol keyword listed in Table 22 or Table 23.
alert {**on** | **off**}	(Optional) For each inspected protocol, the generation of alert messages can be set be **on** or **off**. If no option is selected, alerts are generated on the basis of the setting of the **ip inspect alert-off** command.
audit-trail {**on** | **off**}	(Optional) For each inspected protocol, **audit trail** can be set **on** or **off**. If no option is selected, an audit trail message are generated on the basis of the setting of the **ip inspect audit-trail** command.
http	Specifies the HTTP protocol for Java applet blocking.

urlfilter	(Optional) Associates URL filtering with HTTP inspection.
timeout *seconds*	(Optional) To override the global TCP or User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP) idle timeouts for the specified protocol, specify the number of seconds for a different idle timeout. This timeout overrides the global TCP, UDP, or ICMP timeouts but will not override the global Domain Name System (DNS) timeout.
java-list *access-list*	(Optional) Specifies the numbered standard access list to use to determine "friendly" sites. This keyword is available only for the HTTP protocol, for Java applet blocking. Java blocking only works with numbered standard access lists.
max-data *number*	(Optional) Specifies the maximum number of bytes (data) that can be transferred in a single Simple Mail Transport Protocol (SMTP) session. After the maximum value is exceeded, the firewall will log an alert message and close the session. Default value: 20MB
rpc program-number *number*	Specifies the program number to permit. This keyword is available only for the remote-procedure call protocol.
wait-time *minutes*	(Optional) Specifies the number of minutes to keep a small hole in the firewall to allow subsequent connections from the same source address and to the same destination address and port. The default wait-time is zero minutes. This keyword is available only for the remote-procedure call (RPC) protocol.
fragment	Specifies fragment inspection for the named rule.
max *number*	(Optional) Specifies the maximum number of unassembled packets for which state information (structures) is allocated by Cisco IOS software. Unassembled packets are packets that arrive at the router interface before the initial packet for a session. The acceptable range is 50 through 10000. The default is 256 state entries. Memory is allocated for the state structures, and setting this value to a larger number may cause memory resources to be exhausted.
timeout *seconds* (fragmentation)	(Optional) Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet. The default timeout value is one second. If this number is set to a value greater that one second, it will be automatically adjusted by the Cisco IOS software when the number of free state structures goes below certain thresholds: when the number of free states is less than 32, the timeout will be divided by 2. When the number of free states is less than 16, the timeout will be set to 1 second.

Defaults

No inspection rules are defined until you define them using this command.

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.0(5)T	Introduced configurable alert and audit trail, IP fragmentation checking, and NetShow protocol support.
12.2(11)YU	Support was added for ICMP and SIP protocols and the **urlfilter** keyword was added to the HTTP inspection syntax.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(1)	Skinny protocol support was added.
12.3(7)T	ESMTP protocol support was added.

Usage Guidelines

To define a set of inspection rules, enter this command for each protocol that you want the Cisco IOS firewall to inspect, using the same *inspection-name*. Give each set of inspection rules a unique *inspection-name*, which should not exceed the 16-character limit. Define either one or two sets of rules per interface—you can define one set to examine both inbound and outbound traffic, or you can define two sets: one for outbound traffic and one for inbound traffic.

To define a single set of inspection rules, configure inspection for all the desired application-layer protocols, and for TCP, UDP, or ICMP as desired. This combination of TCP, UDP, and application-layer protocols join together to form a single set of inspection rules with a unique name. (There are no application-layer protocols associated with ICMP.)

To remove the inspection rule for a protocol, use the **no** form of this command with the specified inspection name and protocol; to remove the entire set of inspection rules, use the **no** form of this command only; that is, do not list any inspection names or protocols.

In general, when inspection is configured for a protocol, return traffic entering the internal network will be permitted only if the packets are part of a valid, existing session for which state information is being maintained.

TCP and UDP Inspection

You can configure TCP and UDP inspection to permit TCP and UDP packets to enter the internal network through the firewall, even if the application-layer protocol is not configured to be inspected. However, TCP and UDP inspection do not recognize application-specific commands, and therefore might not permit all return packets for an application, particularly if the return packets have a different port number from the previous exiting packet.

Any application-layer protocol that is inspected will take precedence over the TCP or UDP packet inspection. For example, if inspection is configured for FTP, all control channel information will be recorded in the state table, and all FTP traffic will be permitted back through the firewall if the control channel information is valid for the state of the FTP session. The fact that TCP inspection is configured is irrelevant.

With TCP and UDP inspection, packets entering the network must exactly match an existing session: the entering packets must have the same source or destination addresses and source or destination port numbers as the exiting packet (but reversed). Otherwise, the entering packets will be blocked at the interface.

ICMP Inspection

An ICMP inspection session is on the basis of the source address of the inside host that originates the ICMP packet. Dynamic access control lists (ACLs) are created for return ICMP packets of the allowed types (echo-reply, time-exceeded, destination unreachable, and timestamp reply) for each session. There are no port numbers associated with an ICMP session, and the permitted IP address of the return packet

is wild-carded in the ACL. The wildcard address is because the IP address of the return packet cannot be known in advance for time-exceeded and destination-unreachable replies. These replies can come from intermediate devices rather than the intended destination.

Table 22 Protocol Keywords—Transport-Layer and Network-Layer Protocols

Protocol	Keyword
ICMP	icmp
TCP	**tcp**
UDP	**udp**

Application-Layer Protocol Inspection

In general, if you configure inspection for an application-layer protocol, packets for that protocol should be permitted to exit the firewall (by configuring the correct access control list), and packets for that protocol will only be allowed back in through the firewall if they belong to a valid existing session. Each protocol packet is inspected to maintain information about the session state.

Java, H.323, RPC, Session Initiation Protocol (SIP), and SMTP inspection have additional information, described in the next five sections. Table 23 lists the supported application-layer protocols.

Table 23 Protocol Keywords—Application-Layer Protocols

Protocol	Keyword
CU-SeeMe	**cuseeme**
Extended Simple Mail Transfer Protocol (ESMTP)	smtp
FTP	**ftp**
Java	**http**
H.323	**h323**
Microsoft NetShow	netshow
RealAudio	**realaudio**
RPC	**rpc**
SIP	sip
Simple Mail Transfer Protocol (SMTP)	**smtp**
Skinny Client Control Protocol (SCCP)	skinny
StreamWorks	**streamworks**
Structured Query Language*Net (SQL*Net)	**sqlnet**
TFTP	**tftp**
UNIX R commands (rlogin, rexec, rsh)	**rcmd**
VDOLive	**vdolive**

Java Inspection

Java inspection enables Java applet filtering at the firewall. Java applet filtering distinguishes between trusted and untrusted applets by relying on a list of external sites that you designate as "friendly." If an applet is from a friendly site, the firewall allows the applet through. If the applet is not from a friendly site, the applet will be blocked. Alternately, you could permit applets from all sites except sites specifically designated as "hostile."

Note Before you configure Java inspection, you must configure a numbered standard access list that defines "friendly" and "hostile" external sites. You configure this numbered standard access list to permit traffic from friendly sites, and to deny traffic from hostile sites. If you do not configure a numbered standard access list, but use a "placeholder" access list in the **ip inspect name** *inspection-name* **http** command, all Java applets will be blocked.

Caution Context-Based Access Control (CBAC) does not detect or block encapsulated Java applets. Therefore, Java applets that are wrapped or encapsulated, such as applets in .zip or .jar format, are *not* blocked at the firewall. CBAC also does not detect or block applets loaded via FTP, gopher, or HTTP on a nonstandard port.

H.323 Inspection

If you want CBAC inspection to work with NetMeeting 2.0 traffic (an H.323 application-layer protocol), you must also configure inspection for TCP, as described in the chapter "Configuring Context-Based Access Control" in the *Cisco IOS Security Configuration Guide*. This requirement exists because NetMeeting 2.0 uses an additional TCP channel not defined in the H.323 specification.

RPC Inspection

RPC inspection allows the specification of various program numbers. You can define multiple program numbers by creating multiple entries for RPC inspection, each with a different program number. If a program number is specified, all traffic for that program number will be permitted. If a program number is not specified, all traffic for that program number will be blocked. For example, if you created an RPC entry with the NFS program number, all NFS traffic will be allowed through the firewall.

SIP Inspection

You can configure SIP inspection to permit media sessions associated with SIP-signaled calls to traverse the firewall. Because SIP is frequently used to signal both incoming and outgoing calls, it is often necessary to configure SIP inspection in both directions on a firewall (both from the protected internal network and from the external network). Because inspection of traffic from the external network is not done with most protocols, it may be necessary to create an additional inspection rule to cause only SIP inspection to be performed on traffic coming from the external network.

SMTP Inspection

SMTP inspection causes SMTP commands to be inspected for illegal commands. Packets with illegal commands are modified to a "xxxx" pattern and forwarded to the server. This process causes the server to send a negative reply, forcing the client to issue a valid command. An illegal SMTP command is any command except the following:

- DATA
- HELO
- HELP

- MAIL
- NOOP
- QUIT
- RCPT
- RSET
- SAML
- SEND
- SOML
- VRFY

ESMTP Inspection

Like SMTP, ESMTP inspection also causes the commands to be inspected for illegal commands. Packets with illegal commands are modified to a “xxxx” pattern and forwarded to the server. This process causes the server to send a negative reply, forcing the client to issue a valid command. An illegal ESMTP command is any command except the following:

- AUTH
- DATA
- EHLO
- ETRN
- HELO
- HELP
- MAIL
- NOOP
- QUIT
- RCPT
- RSET
- SAML
- SEND
- SOML
- VRFY

In addition to inspecting commands, the ESMTP firewall also inspects the following extensions via deeper command inspection:

- Message Size Declaration (SIZE)
- Remote Queue Processing Declaration (ETRN)
- Binary MIME (BINARYMIME)
- Command Pipelining
- Authentication
- Delivery Status Notification (DSN)
- Enhanced Status Code (ENHANCEDSTATUSCODE)

- 8bit-MIMEtransport (8BITMIME)

Note SMTP and ESMTP cannot exist simultaneously. An attempt to configure both protocols will result in an error message.

Use of the urlfilter Keyword

If you specify the **urlfilter** keyword, the Cisco IOS firewall will interact with a URL filtering software to control web traffic for a given host or user on the basis of a specified security policy.

Note Enabling HTTP inspection with or without any option triggers the Java applet scanner, which is CPU intensive. The only way to stop the Java applet scanner is to specify the **java-list** *access-list* option. Configuring URL filtering without enabling the **java-list** *access-list* option will severely impact performance.

Use of the timeout Keyword

If you specify a timeout for any of the transport-layer or application-layer protocols, the timeout will override the global idle timeout for the interface to which the set of inspection rules is applied.

If the protocol is TCP or a TCP application-layer protocol, the timeout will override the global TCP idle timeout. If the protocol is UDP or a UDP application-layer protocol, the timeout will override the global UDP idle timeout.

If you do not specify a timeout for a protocol, the timeout value applied to a new session of that protocol will be taken from the corresponding TCP or UDP global timeout value valid at the time of session creation.

The default ICMP timeout is deliberately short (10 seconds) due to the security hole that is opened by allowing ICMP packets with a wild-carded source address back into the inside network. The timeout will occur 10 seconds after the last outgoing packet from the originating host. For example, if you send a set of 10 ping packets spaced one second apart, the timeout will expire in 20 seconds or 10 seconds after the last outgoing packet. However, the timeout is not extended for return packets. If a return packet is not seen within the timeout window, the hole will be closed and the return packet will not be allowed in. Although the default timeout can be made longer if desired, it is recommended that this value be kept relatively short.

IP Fragmentation Inspection

CBAC inspection rules can help protect hosts against certain denial-of-service attacks involving fragmented IP packets. Even though the firewall keeps an attacker from making actual connections to a given host, the attacker may still be able to disrupt services provided by that host. This is done by sending many noninitial IP fragments or by sending complete fragmented packets through a router with an ACL that filters the first fragment of a fragmented packet. These fragments can tie up resources on the target host as it tries to reassemble the incomplete packets.

Using fragmentation inspection, the firewall maintains an *interfragment state* (structure) for IP traffic. Noninitial fragments are discarded unless the corresponding initial fragment was permitted to pass through the firewall. Non-initial fragments received before the corresponding initial fragments are discarded.

Note Fragmentation inspection can have undesirable effects in certain cases, because it can result in the firewall discarding any packet whose fragments arrive out of order. There are many circumstances that can cause out-of-order delivery of legitimate fragments. Apply fragmentation inspection in situations where legitimate fragments, which are likely to arrive out of order, might have a severe performance impact.

Because routers running Cisco IOS software are used in a very large variety of networks, and because the CBAC feature is often used to isolate parts of internal networks from one another, the fragmentation inspection feature is not enabled by default. Fragmentation detection must be explicitly enabled for an inspection rule using the **ip inspect name** command. Unfragmented traffic is never discarded because it lacks a fragment state. Even when the system is under heavy attack with fragmented packets, legitimate fragmented traffic, if any, will still get some fraction of the firewall's fragment state resources, and legitimate, unfragmented traffic can flow through the firewall unimpeded.

Examples

The following example causes the software to inspect TCP sessions and UDP sessions, and to specifically allow CU-SeeMe, FTP, and RPC traffic back through the firewall for existing sessions only. For UDP traffic, audit-trail is on. For FTP traffic, the idle timeout is set to override the global TCP idle timeout. For RPC traffic, program numbers 100003, 100005, and 100021 are permitted.

```
ip inspect name myrules tcp
ip inspect name myrules udp audit-trail on
ip inspect name myrules cuseeme
ip inspect name myrules ftp timeout 120
ip inspect name myrules rpc program-number 100003
ip inspect name myrules rpc program-number 100005
ip inspect name myrules rpc program-number 100021
```

The following example adds fragment checking to software inspection of TCP and UDP sessions for the rule named "*myrules*." In this example, the firewall software will allocate 100 state structures, and the timeout value for dropping unassembled packets is set to 4 seconds. If 100 initial fragments for 100 different packets are sent through the router, all of the state structures will be used up. The initial fragment for packet 101 will be dropped. Additionally, if the number of free state structures (structures available for use by unassembled packets) drops below the threshold values, 32 or 16, the timeout value is automatically reduced to 2 or 1, respectively. Changing the timeout value frees up packet state structures more quickly.

```
ip inspect name myrules tcp
ip inspect name myrules udp audit-trail on
ip inspect name myrules cuseeme
ip inspect name myrules ftp timeout 120
ip inspect name myrules rpc program-number 100003
ip inspect name myrules rpc program-number 100005
ip inspect name myrules rpc program-number 100021
ip inspect name myrules fragment max 100 timeout 4
```

The following firewall and SIP example shows how to allow outside-initiated calls and internal calls. For outside-initiated calls, an ACL needs to be punched to allow for the traffic from the initial signaling packet from outside. Subsequent signaling and media channels will be allowed by the inspection module.

```
ip inspect name voip sip
interface FastEthernet0/0
 ip inspect voip in
!
!
interface FastEthernet0/1
 ip inspect voip in
```

```
 ip access-group 100 in
!
!
access-list 100 permit udp host <gw ip> any eq 5060
access-list 100 permit udp host <proxy ip> any eq 5060
access-list deny ip any any
```

The following example shows two configured inspections named “fw_only” and “fw_urlf”; URL filtering will work only on the traffic that is inspected by fw_urlf. Note that the **java-list** *access-list* option has been enabled, which disables java scanning.

```
ip inspect name fw_only http java-list 51 timeout 30
interface e0
 ip inspect fw_only in
!
ip inspect name fw_urlf  http urlfilter java-list 51 timeout 30
interface e1
 ip inspect fw_urlf in
```

Related Commands

Command	Description
ip inspect	Applies a set of inspection rules to an interface.
ip inspect alert-off	Disables CBAC alert messages.
ip inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.

ip inspect one-minute high

To define the rate of new unestablished sessions that will cause the software to start deleting half-open sessions, use the **ip inspect one-minute high** command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the **no** form of this command.

ip inspect one-minute high *number*

no ip inspect one-minute high

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions. The default is 500 half-open sessions.

Defaults

500 half-open sessions

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially-decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ip inspect one-minute high 1000
ip inspect one-minute low 950
```

Related Commands

Command	Description
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ip inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ip inspect one-minute low

To define the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions, use the **ip inspect one-minute low** command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command.

ip inspect one-minute low *number*

no ip inspect one-minute low

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions. The default is 400 half-open sessions.

Defaults

400 half-open sessions

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ip inspect one-minute high 1000
ip inspect one-minute low 950
```

Related Commands

Command	Description
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ip inspect tcp finwait-time

To define how long a TCP session will still be managed after the firewall detects a FIN-exchange, use the **ip inspect tcp finwait-time** command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

ip inspect tcp finwait-time *seconds*

no ip inspect tcp finwait-time

Syntax Description

seconds	Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

When the software detects a valid TCP packet that is the first in a session, and if Context-based Access Control (CBAC) inspection is configured for the packet's protocol, the software establishes state information for the new session.

Use this command to define how long TCP session state information will be maintained after the firewall detects a FIN-exchange for the session. The FIN-exchange occurs when the TCP session is ready to close.

The global value specified for this timeout applies to all TCP sessions inspected by CBAC.

The timeout set with this command is referred to as the "finwait" timeout.

Note If the -n option is used with rsh, and the commands being executed do not produce output before the "finwait" timeout, the session will be dropped and no further output will be seen.

Examples

The following example changes the "finwait" timeout to 10 seconds:

```
ip inspect tcp finwait-time 10
```

The following example changes the "finwait" timeout back to the default (5 seconds):

```
no ip inspect tcp finwait-time
```

ip inspect tcp idle-time

To specify the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity), use the **ip inspect tcp idle-time** command in global configuration mode. To reset the timeout to the default of 3600 seconds (1 hour), use the **no** form of this command.

ip inspect tcp idle-time *seconds*

no ip inspect tcp idle-time

Syntax Description

seconds	Specifies the length of time, in seconds, for which a TCP session will still be managed while there is no activity. The default is 3600 seconds (1 hour).

Defaults

3600 seconds (1 hour)

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

When the software detects a valid TCP packet that is the first in a session, and if Context-based Access Control (CBAC) inspection is configured for the packet's protocol, the software establishes state information for the new session.

If the software detects no packets for the session for a time period defined by the TCP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all TCP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ip inspect name** (global configuration) command.

Note This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the TCP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

Examples

The following example sets the global TCP idle timeout to 1800 seconds (30 minutes):

```
ip inspect tcp idle-time 1800
```

The following example sets the global TCP idle timeout back to the default of 3600 seconds (one hour):

```
no ip inspect tcp idle-time
```

ip inspect tcp max-incomplete host

To specify threshold and blocking time values for TCP host-specific denial-of-service detection and prevention, use the **ip inspect tcp max-incomplete host** command in global configuration mode. To reset the threshold and blocking time to the default values, use the **no** form of this command.

ip inspect tcp max-incomplete host *number* **block-time** *minutes*

no ip inspect tcp max-incomplete host

Syntax Description

number	Specifies how many half-open TCP sessions with the same host destination address can exist at a time, before the software starts deleting half-open sessions to the host. Use a number from 1 to 250. The default is 50 half-open sessions.
block-time	Specifies blocking of connection initiation to a host.
minutes	Specifies how long the software will continue to delete new connection requests to the host. The default is 0 minutes.

Defaults

50 half-open sessions and 0 minutes

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions with the same destination host address could indicate that a denial-of-service attack is being launched against the host. For TCP, “half-open” means that the session has not reached the established state.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (the **max-incomplete host** number), the software will delete half-open sessions according to one of the following methods:

- If the **block-time** *minutes* timeout is 0 (the default):

  The software will delete the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.

- If the **block-time** *minutes* timeout is greater than 0:

  The software will delete all existing half-open sessions for the host, and then block all new connection requests to the host. The software will continue to block all new connection requests until the **block-time** expires.

The software also sends syslog messages whenever the **max-incomplete host** number is exceeded and when blocking of connection initiations to a host starts or ends.

The global values specified for the threshold and blocking time apply to all TCP connections inspected by Context-based Access Control (CBAC).

Examples

The following example changes the **max-incomplete host** number to 40 half-open sessions, and changes the **block-time** timeout to 2 minutes (120 seconds):

```
ip inspect tcp max-incomplete host 40 block-time 120
```

The following example resets the defaults (50 half-open sessions and 0 seconds):

```
no ip inspect tcp max-incomplete host
```

Related Commands

Command	Description
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.

ip inspect tcp synwait-time

To define how long the software will wait for a TCP session to reach the established state before dropping the session, use the **ip inspect tcp synwait-time** command in global configuration mode. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

ip inspect tcp synwait-time *seconds*

no ip inspect tcp synwait-time

Syntax Description

seconds	Specifies how long, in seconds, the software will wait for a TCP session to reach the established state before dropping the session. The default is 30 seconds.

Defaults

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

Use this command to define how long Cisco IOS software will wait for a TCP session to reach the established state before dropping the session. The session is considered to have reached the established state after the session's first SYN bit is detected.

The global value specified for this timeout applies to all TCP sessions inspected by Context-based Access Control (CBAC).

Examples

The following example changes the "synwait" timeout to 20 seconds:

```
ip inspect tcp synwait-time 20
```

The following example changes the "synwait" timeout back to the default (30 seconds):

```
no ip inspect tcp synwait-time
```

ip inspect udp idle-time

To specify the User Datagram Protocol idle timeout (the length of time for which a UDP "session" will still be managed while there is no activity), use the **ip inspect udp idle-time** command in global configuration mode. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

ip inspect udp idle-time *seconds*

no ip inspect udp idle-time

Syntax Description

seconds	Specifies the length of time a UDP "session" will still be managed while there is no activity. The default is 30 seconds.

Defaults

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

When the software detects a valid UDP packet, if Context-based Access Control (CBAC) inspection is configured for the packet's protocol, the software establishes state information for a new UDP "session." Because UDP is a connectionless service, there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, it has similar source or destination addresses) and if the packet was detected soon after another similar UDP packet.

If the software detects no UDP packets for the UDP session for the a period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all UDP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ip inspect name** command.

Note This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the UDP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

Examples

The following example sets the global UDP idle timeout to 120 seconds (2 minutes):

```
ip inspect udp idle-time 120
```

The following example sets the global UDP idle timeout back to the default of 30 seconds:

```
no ip inspect udp idle-time
```

ip ips

To apply an Intrusion Prevention System (IPS) rule to an interface, use the **ip ips** command in interface configuration mode. To remove an IPS rule from an interface direction, use the **no** form of this command.

ip ips *ips-name* {**in** | **out**} [**list** *acl*]

no ip ips *ips-name* {**in** | **out**} [**list** *acl*]

Syntax Description

ips-name	Name of IPS signature definition file (SDF).
in	Applies IPS to inbound traffic.
out	Applies IPS to outbound traffic.
list *acl*	(Optional) Specifies an extended or standard access control list (ACL) to filter the traffic that will be scanned.

Defaults

By default, IPS signatures are not applied to an interface or direction.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit** command to the **ip ips** command.

Usage Guidelines

The **ip ips** command loads the SDF onto the router and builds the signature engines when IPS is applied to the first interface.

Note The router prompt disappears while the signatures are loading and the signature engines are building. It will reappear after these tasks are complete.

Depending on your platform and how many signatures are being loaded, building the signature engine can take several of minutes. It is recommended that you enable logging messages so you can monitor the engine building status.

The **ip ips** command replaces the **ip audit** command. If the **ip audit** command is part of an existing configuration, IPS will interpret it as the **ip ips** command.

Examples

The following example shows the basic configuration necessary to load the attack-drop.sdf file onto a router running Cisco IOS IPS. Note that the configuration is almost the same as when you load the default signatures onto a router, except for the **ip ips sdf location** command, which specifies the attack-drop.sdf file.

```
!
ip ips sdf location disk2:attack-drop.sdf
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
```

The following example shows how to configure the router to load and merge the attack-drop.sdf file with the default signatures. After you have merged the two files, it is recommended to copy the newly merged signatures to a separate file. The router can then be reloaded (via the **reload** command) or reinitalized to so as to recognize the newly merged file (as shown the following example)

```
!
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
!
! Merge the flash-based SDF (attack-drop.sdf) with the built-in signatures.
copy disk2:attack-drop.sdf ips-sdf
! Save the newly merged signatures to a separate file.
copy ips-sdf disk2:my-signatures.sdf
!
! Configure the router to use the new file, my-signatures.sdf
configure terminal
ip ips sdf location disk2:my-signatures.sdf
! Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.
interface gig 0/1
 no ip ips MYIPS in
!
*Apr 8 14:05:38.243:%IPS-2-DISABLED:IPS removed from all interfaces - IPS disabled
!
 ip ips MYIPS in
!
 exit
```

Related Commands

Command	Description
copy ips-sdf	Loads or saves the SDF in the router.
ip ips sdf location	Specifies the location in which the router should load the SDF.

ip ips fail closed

To instruct the router to drop all packets until the signature engine is built and ready to scan traffic, use the **ip ips fail closed** command in global configuration mode. To return to the default functionality, use the **no** form of this command.

ip ips fail closed

no ip ips fail closed

Syntax Description

This command has no arguments or keywords.

Defaults

All packets are passed without being scanned while the signature engine is being built or if the signature engine fails to build.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Cisco IOS IPS Fails to Load the SDF

By default, the router running Intrusion Prevention System (IPS) will load the built-in signatures if it fails to load the signature definition file (SDF). If this command is issued, the router will drop all packets—unless the user specifies an access control list (ACL) for packets to send to IPS.

IPS Loads the SDF but Fails to Build a Signature Engine

If the router running IPS loads the SDF but fails to build a signature engine, the router will mark the engine "not ready." If an available engine is previously loaded, the IPS will keep the available engine and discard the engine that is not ready for use. If no previous engines have been loaded or "not ready," the router will install the engine that is not ready and rely on the configuration of the **ip ips fail closed** command.

By default, packets destined for an engine marked "not ready" will be passed without being scanned. If this command is issued, the router will drop all packets that are destined for that signature engine.

Examples

The following example shows how to instruct the router to drop all packets if the SME is not yet available:

```
Router(config)# ip ips fail closed
```

ip ips name

To specify an intrusion prevention system (IPS) rule, use the **ip ips name** command in global configuration mode. To delete an IPS rule, use the **no** form of this command.

ip ips name *ips-name*

no ip ips name *ips-name*

Syntax Description

ips-name	Name for IPS rule.

Defaults

An IPS rule does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit name** command to the **ip ips name** command.

Usage Guidelines

The IPS does not load the signatures until the rule is applied to an interface via the **ip ips** command.

Note This command replaces the **ip audit name** global configuration command. If the **ip audit name** command has been issued in an existing configuration and an access control list (ACL) has been defined, IPS will apply the **ip ips name** command and the ACL parameter on all interfaces that applied the rule.

Examples

The following example shows how to configure a router running Cisco IOS IPS to load the default, built-in signatures. Note that a configuration option for specifying an SDF location is not necessary; built-in signatures reside statically in Cisco IOS.

```
!
ip ips po max-events 100
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
```

Related Commands

Command	Description
ip ips	Applies an IPS rule to an interface.
show ip ips	Displays IPS information such as configured sessions and signatures.

ip ips notify

To specify the method of event notification, use the **ip ips notify** command in global configuration mode. To disable event notification, use the **no** form of this command.

ip ips notify [**log** | **sdee**]

no ip ips notify [**log** | **sdee**]

Syntax Description

log	(Optional) Send messages in syslog format. **Note** If an option is not specified, alert messages are sent in syslog format.
sdee	(Optional) Send messages in Security Device Event Exchange (SDEE) format.

Defaults

Disabled (alert messages are not sent).

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit notify** command to the **ip ips notify** command.
12.3(11)T	Support for SDEE was introduced, and the **sdee** keyword was added; the Post Office protocol was deprecated, and the **nr-director** keyword was removed.

Usage Guidelines

SDEE is always running, but it does not receive and process events from Intrusion Prevention System (IPS) unless SDEE notification is enabled. If it is not enabled and a client sends a request, SDEE will respond with a fault response message, indicating that notification is not enabled.

To use SDEE, the HTTP server must be enabled (via the **ip http server** command). If the HTTP server is not enabled, the router cannot respond to the SDEE clients because it cannot not see the requests.

Note The **ip ips notify** command replaces the **ip audit notify** command. If the **ip audit notify** command is part of an existing configuration, the IPS will interpret it as the **ip ips notify** command.

Examples

In the following example, event notifications are specified to be sent in SDEE format:

```
ip ips notify sdee
```

Related Commands

Command	Description
ip http server	Enables the HTTP server on your system.

ip ips po local

Note Effective with Cisco IOS Release 12.3(11)T, the **ip ips po local** command is no longer available in Cisco IOS software.

To specify the local Post Office parameters used when sending event notifications to the VPN/Security Management Solution (VMS), use the **ip ips po local** command in global configuration mode. To set the local Post Office parameters to their default settings, use the **no** form of this command.

ip ips po local hostid *id-number* **orgid** *id-number*

no ip ips po local [**hostid** *id-number* **orgid** *id-number*]

Syntax Description

hostid	Specifies a VMS host ID.
id-number	Unique integer in the range 1 to 65535 used in VMS communications to identify the local host. The default host ID is 1.
orgid	Specifies a VMS organization ID.
id-number	Unique integer in the range 1 to 65535 used in VMS communications to identify the group to which the local host belongs. The default organization ID is 1.

Defaults

The default organization ID is 1. The default host ID is 1.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit po local** command to the **ip ips po local** command.
12.3(11)T	This command is no longer available in Cisco IOS software.

Usage Guidelines

Use the **ip ips po local** global configuration command to specify the local Post Office parameters used when sending event notifications to the VMS.

Examples

In the following example, the local host is assigned a host ID of 10 and an organization ID of 500:

```
ip ips po local hostid 10 orgid 500
```

ip ips po max-events

Note Effective with Cisco IOS Release 12.3(11)T, the **ip ips po max-events** command is no longer available in Cisco IOS software.

To specify the maximum number of event notifications that are placed in the router's event queue, use the **ip ips po max-events** command in global configuration mode. To set the number of recipients to the default setting, use the **no** form of this command.

ip ips po max-events *number-of-events*

no ip ips po max-events

Syntax Description

number-of-events	Integer in the range from 1 to 65535 that designates the maximum number of events allowable in the event queue. The default is 100 events.

Defaults

The default number of events is 100.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command named was changed from the **ip audit po max-events** command to the **ip ips po max-events** command.
12.3(11)T	This command is no longer available in Cisco IOS software.

Usage Guidelines

Raising the number of events past 100 may cause memory and performance impacts because each event in the event queue requires 32 KB of memory.

Examples

In the following example, the number of events in the event queue is set to 250:

```
ip ips po max-events 250
```

ip ips po protected

Note Effective with Cisco IOS Release 12.3(11)T, the **ip ips po protected** command is no longer available in Cisco IOS software.

To specify whether an address is on a protected network, use the **ip ips po protected** command in global configuration mode. To remove network addresses from the protected network list, use the **no** form of this command.

ip ips po protected *ip-addr* [**to** *ip-addr*]

no ip ips po protected [*ip-addr*]

Syntax Description

ip-addr	IP address of a network host.
to *ip-addr*	(Optional) Specifies a range of IP addresses.

Defaults

If no addresses are defined as protected, then all addresses are considered outside the protected network.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit po protected** command to the **ip ips po protected** command.
12.3(11)T	This command is no longer available in Cisco IOS software.

Usage Guidelines

You can enter a single address at a time or a range of addresses at a time. You can also make as many entries to the protected networks list as you want. When an attack is detected, the corresponding event contains a flag that denotes whether the source or destination of the packet belongs to a protected network or not.

If you specify an IP address for removal, that address is removed from the list. If you do not specify an address, then all IP addresses are removed from the list.

Examples

In the following example, a range of addresses is added to the protected network list:

```
ip ips po protected 10.1.1.0 to 10.1.1.255
```

In the following example, three individual addresses are added to the protected network list:

```
ip ips po protected 10.4.1.1
ip ips po protected 10.4.1.8
ip ips po protected 10.4.1.25
```

ip ips po remote

Note Effective with Cisco IOS Release 12.3(11)T, the **ip ips po remote** command is no longer available in Cisco IOS software.

To specify one or more set of Post Office parameters for the VPN/Security Management Solution (VMS) receiving event notifications from the router, use the **ip ips po remote** command in global configuration mode. To remove a VMS' Post Office parameters as defined by host ID, organization ID, and IP address, use the **no** form of this command.

ip ips po remote hostid *host-id* **orgid** *org-id* **rmtaddress** *ip-address* **localaddress** *ip-address* [**port** *port-number*] [**preference** *preference-number*] [**timeout** *seconds*] [**application** {**director** | **logger**}]

no ip ips po remote hostid *host-id* **orgid** *org-id* **rmtaddress** *ip-address*

Syntax Description

hostid	Specifies a VMS host ID.
host-id	Unique integer in the range from 1 to 65535 used in VMS communications to identify the local host. The default host ID is 1.
orgid	Specifies a VMS organization ID.
org-id	Unique integer in the range from 1 to 65535 used in VMS communications to identify the group in which the local host belongs. The default organization ID is 1.
rmtaddress	Specifies the IP address of the VMS.
localaddress	Specifies the IP address of the Cisco IOS Firewall Intrusion Prevention System (IPS) router.
ip-address	IP address of the VMS or Cisco IOS Firewall IPS router's interface. Use with the **rmtaddress** and **localaddress** keywords.
port	(Optional) Specifies a User Datagram Protocol port through which to send messages.
port-number	(Optional) Integer representing the UDP port on which the VMS is listening for event notifications. The default UDP port number is 45000.
preference	(Optional) Specifies a route preference for communication.
preference-number	(Optional) Integer representing the relative priority of a route to a VMS, if more than one route exists. The default preference is 1.
timeout	(Optional) Specifies a timeout value for Post Office communications.
seconds	(Optional) Integer representing the heartbeat timeout value for Post Office communications. The default timeout is 5 seconds.
application	(Optional) Specifies the type of application that is receiving the Cisco IOS Firewall IPS messages. The default application is director.
director	(Optional) Specifies that the receiving application is the VMS interface.
logger	(Optional) Specifies that the receiving application is a VMS.

Defaults

Parameter values are not set.

Command Modes Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changes from the **ip audit po remote** command to the **ip ips po remote** command.
12.3(11)T	This command is no longer available in Cisco IOS software.

Usage Guidelines A router can report to more than one VMS. In this case, use the **ip ips po remote** command to add each VMS to which the router sends notifications.

More than one route can be established to the same VMS. In this case, you must give each route a preference number that establishes the relative priority of routes. The router always attempts to use the lowest numbered route, switching automatically to the next higher number when a route fails, and then switching back when the route begins functioning again.

Note The **ip ips po remote** command replaces the **ip audit po remote** command. If the **ip audit po remote** command is found in an existing configuration, Cisco IOS IPS will interpret it as the **ip ips po remote** command.

Examples In the following example, two communication routes for the same dual-homed VMS are defined:

```
ip ips po remote hostid 30 orgid 500 rmtaddress 10.1.99.100 localaddress 10.1.99.1
preference 1
ip ips po remote hostid 30 orgid 500 rmtaddress 10.1.4.30 localaddress 10.1.4.1 preference
2
```

The router uses the first entry to establish communication with the VMS defined with host ID 30 and organization ID 500. If this route fails, then the router will switch to the secondary communications route. As soon as the first route begins functioning again, the router switches back to the primary route and closes the secondary route.

In the following example, a different VMS is assigned a longer heartbeat timeout value because of network congestion, and is designated as a logger application:

```
ip ips po remote hostid 70 orgid 500 rmtaddress 10.1.8.1 localaddress 10.1.8.100 timeout
10 application director
```

ip ips sdf location

To specify the location in which the router will load the signature definition file (SDF), use the **ip ips sdf location** command in global configuration mode. To remove an SDF location from the configuration, use the **no** form of this command.

ip ips sdf location *url*

no ip ips sdf location *url*

Syntax Description

url	Location of the SDF. Available URL options: • local flash, such as flash:sig.xml • FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml • rcp, such as rcp://myuser@rcp_server/sig.xml • TFTP server, such as tftp://tftp_server/sig.xml

Defaults

If an SDF location is not specified, the router will load the default, built-in signatures.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

When the **ip ips sdf location** command is issued, the signatures are not loaded until the router is rebooted or until the Intrusion Prevention System (IPS) is applied to an interface (via the **ip ips** command). If IPS is already applied to an interface, the signatures will not be loaded. If IPS cannot load the SDF, you will receive an error message and the router will use the built-in IPS signatures.

You can also issue the **copy ips-sdf** command to load an SDF from a specified location. Unlike the **ip ips sdf location** command, the signatures are loaded immediately after the **copy ips-sdf** command is issued.

Examples

The following example shows how to configure the router to load and merge the attack-drop.sdf file with the default signatures. After you have merged the two files, it is recommended to copy the newly merged signatures to a separate file. The router can then be reloaded (via the **reload** command) or reinitalized to so as to recognize the newly merged file (as shown the following example)

```
!
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
```

```
 speed 100
 media-type rj45
 no negotiation auto
!
!
! Merge the flash-based SDF (attack-drop.sdf) with the  built-in signatures.
copy disk2:attack-drop.sdf ips-sdf
! Save the newly merged signatures to a separate file.
copy ips-sdf disk2:my-signatures.sdf
!
! Configure the router to use the new file, my-signatures.sdf
configure terminal
ip ips sdf location disk2:my-signatures.sdf
! Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.
interface gig 0/1
no ip ips MYIPS in
!
*Apr 8 14:05:38.243:%IPS-2-DISABLED:IPS removed from all interfaces - IPS disabled
!
 ip ips MYIPS in
!
exit
```

Related Commands

Command	Description
copy ips-sdf	Loads or saves the SDF in the router.
ip ips	Applies the IPS rule to an interface.

ip ips signature

To attach a policy to a signature, use the **ip ips signature** command in global configuration mode. If the policy disabled a signature, use the **no** form of this command to reenable the signature. If the policy attached an access list to the signature, use the **no** form of this command to remove the access list.

ip ips signature *signature-id* {**delete** | **disable** | **list** *acl-list*}

no ip ips signature *signature-id*

Syntax Description

signature-id	Signature within the signature detection file (SDF).
delete	Deleted a specified signature.
disable	Disables a specified signature.
list *acl-list*	A named, standard, or ACL that is associated with the signature.

Defaults

No policy is attached to a signature.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit signature** command to the **ip ips signature** command to support SDFs.

Usage Guidelines

This command allow you to set three policies: delete a signature, disable the audit of a signature, or qualify the audit of a signature with an access list.

If you are attaching an ACL to a signature, then you also need to create an Intrusion Prevention System (IPS) rule with the **ip ips name** command and apply it to an interface with the **ip ips** command.

Note The **ip ips signature** command replaces the **ip audit signature** command. If the **ip audit signature** command is found in an existing configuration, Cisco IOS IPS will interpret it as the **ip ips signature** command.

Examples

In the following example, a signature is disabled, another signature has ACL 99 attached to it, and ACL 99 is defined:

```
ip ips signature 6150 disable
ip ips signature 1000 list 99

access-list 99 deny 10.1.10.0 0.0.0.255
access-list 99 permit any
```

ip ips signature disable

To instruct the router to scan for a given signature but not take any action if the signature is detected, use the **ip ips signature** command in global configuration mode. To reenable a signature, use the **no** form of this command.

ip ips signature *signature-id* [*sub-signature-id*] **disable** [**list** *acl-list*]

no ip ips signature *signature-id* [*sub-signature-id*] **disable** [**list** *acl-list*]

Syntax Description

signature-id [*sub-signature-id*]	Signature that is disabled.
list *acl-list*	(Optional) A named, standard, or extended access control list (ACL) to filter the traffic that will be scanned. If the packet is permitted by the ACL, the signature will be scanned and reported; if the packet is denied by the ACL, the signature is deemed disabled.

Defaults

All signatures within the signature definition file (SDF) are reported, if detected.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

You may want to disable a signature (or set of signatures) if your deployment scenario deems the signatures unnecessary.

Examples

The following example shows how to instructs the router not to report on signature 1000, if detected:

```
Router(config) ip ips signature 1000 disable
```

Related Commands

Command	Description
ip ips	Applies the IPS rule to an interface.
ip ips name	Specifies an IPS rule.

ip port-map

To establish port to application mapping (PAM), use the **ip port-map** command in global configuration mode. To delete user-defined PAM entries, use the **no** form of this command.

ip port-map *appl-name* **port** *port-num* [**list** *acl-num*]

no ip port-map *appl-name* **port** *port-num* [**list** *acl-num*]

Syntax Description

appl-name	Specifies the name of the application with which to apply the port mapping.
port	Indicates that a port number maps to the application.
port-num	Identifies a port number in the range 1 to 65535.
list	(Optional) Indicates that the port mapping information applies to a specific host or subnet.
acl-num	(Optional) Identifies the standard access control list (ACL) number used with PAM.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	Skinny Client Control protocol (SCCP) support was added.

Usage Guidelines

The **ip port-map** command associates TCP or User Datagram Protocol (UDP) port numbers with applications or services, establishing a table of default port mapping information at the firewall. This information is used to support network environments that run services using ports that are different from the registered or well-known ports associated with a service or application.

The port mapping information in the PAM table is of one of three types:

- System-defined
- User-defined
- Host-specific

System-Defined Port Mapping

Initially, PAM creates a set of system-defined entries in the mapping table using well-known or registered port mapping information set up during the system start-up. The Cisco IOS Firewall Context-Based Access Control feature requires the system-defined mapping information to function properly. System-defined mapping information cannot be deleted or changed; that is, you cannot map HTTP services to port 21 (FTP) or FTP services to port 80 (HTTP).

Table 24 lists the default system-defined services and applications in the PAM table.

Table 24 System-Defined Port Mapping

Application Name	Well-Known or Registered Port Number	Protocol Description
cuseeme	7648	CU-SeeMe Protocol
exec	512	Remote Process Execution
ftp	21	File Transfer Protocol (control port)
h323	1720	H.323 Protocol (for example, MS NetMeeting, Intel Video Phone)
http	80	Hypertext Transfer Protocol
login	513	Remote login
msrpc	135	Microsoft Remote Procedure Call
netshow	1755	Microsoft NetShow
real-audio-video	7070	RealAudio and RealVideo
sccp	2000	Skinny Client Control Protocol (SCCP)
smtp	25	Simple Mail Transfer Protocol (SMTP)
sql-net	1521	SQL-NET
streamworks	1558	StreamWorks Protocol
sunrpc	111	SUN Remote Procedure Call
tftp	69	Trivial File Transfer Protocol
vdolive	7000	VDOLive Protocol

Note You can override the system-defined entries for a specific host or subnet using the **list** option in the **ip port-map** command.

User-Defined Port Mapping

Network applications that use non-standard ports require user-defined entries in the mapping table. Use the **ip port-map** command to create default user-defined entries in the PAM table.

To map a range of port numbers with a service or application, you must create a separate entry for each port number.

Note If you try to map an application to a system-defined port, a message appears warning you of a mapping conflict.

Use the **no** form of the **ip port-map** command to delete user-defined entries from the PAM table.

To overwrite an existing user-defined port mapping, use the **ip port-map** command to associate another service or application with the specific port.

Host-Specific Port Mapping

User-defined entries in the mapping table can include host-specific mapping information, which establishes port mapping information for specific hosts or subnets. In some environments, it might be necessary to override the default port mapping information for a specific host or subnet, including a system-defined default port mapping information. Use the **list** option for the **ip port-map** command to specify an ACL for a host or subnet that uses PAM.

Note If the host-specific port mapping information is the same as existing system-defined or user-defined default entries, host-specific port changes have no effect.

Examples

The following example provides examples for adding and removing user-defined PAM configuration entries at the firewall.

In the following example, non-standard port 8000 is established as the user-defined default port for HTTP services:

```
ip port-map http port 8000
```

The following example shows PAM entries establish a range of nonstandard ports for HTTP services:

```
ip port-map http 8001
ip port-map http 8002
ip port-map http 8003
ip port-map http 8004
```

In the following example the command fails because it tries to map port 21, which is the system-defined default port for FTP, with HTTP:

```
ip port-map http port 21
```

In the following example, a specific host uses port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), while port 8000 is mapped with FTP services:

```
access-list 10 permit 192.168.32.43
ip port-map ftp port 8000 list 10
```

In the following example, port 21, which is normally reserved for FTP services, is mapped to the RealAudio application for the hosts in list 10. In this configuration, hosts in list 10 do not recognize FTP activity on port 21.

```
ip port-map realaudio port 21 list 10
```

In the following example, the **ip port-map** command fails and generates an error message:

```
ip port-map netshow port 21
Command fail: the port 21 has already been defined for ftp by the system.
              No change can be made to the system defined port mappings.
```

The **no** form of this command deletes user-defined entries from the PAM table. It has no effect on the system-defined port mappings. This command deletes the host-specific port mapping of FTP.

```
no ip port-map ftp port 1022 list 10
```

In the following example, the command fails because it tries to delete the system-defined default port for HTTP:

```
no ip port-map http port 80
```

In the following example, a specific host uses port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), while port 8000 is mapped with FTP services.

```
access-list 10 permit 192.168.32.43
ip port-map ftp port 8000 list 10
```

In the following example, a specific subnet runs HTTP services on port 8080. ACL 50 identifies the subnet, while the PAM entry maps port 8080 with HTTP services.

```
access-list 50 permit 192.168.92.0
ip port-map http 8080 list 50
```

In the following example, a specific host runs HTTP services on port 25, which is the system-defined port number for SMTP services. This requires a host-specific PAM entry that overrides the system-defined default port mapping for HTTP, which is port 80. ACL 15 identifies the host address (192.168.33.43), while port 25 is mapped with HTTP services.

```
access-list 15 permit 192.168.33.43
ip port-map http port 25 list 15
```

In the following example, the same port number is required by different services running on different hosts. Port 8000 is required for HTTP services by host 192.168.3.4, while port 8000 is required for Telnet services by host 192.168.5.6. ACL 10 and ACL 20 identify the specific hosts, while PAM maps the ports with the services for each ACL.

```
access-list 10 permit 192.168.3.4
access-list 20 permit 192.168.5.6
ip port-map http port 8000 list 10
ip port-map http ftp 8000 list 20
```

Related Commands

Command	Description
show ip port-map	Displays the PAM information.

ip radius source-interface

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the **ip radius source-interface** command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the **no** form of this command.

ip radius source-interface *subinterface-name* [**vrf** *vrf-name*]

no ip radius source-interface

Syntax Description

subinterface-name	Name of the interface that RADIUS uses for all of its outgoing packets.
vrf *vrf-name*	(Optional) Per Virtual Route Forwarding (VRF) configuration.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to set the IP address of a subinterface to be used as the source address for all outgoing RADIUS packets. The IP address is used as long as the subinterface is in the *up* state. In this way, the RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses.

This command is especially useful in cases where the router has many subinterfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address.

The specified subinterface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in the *down* state, then RADIUS reverts to the default. To avoid this, add an IP address to the subinterface or bring the subinterface to the *up* state.

Use the **vrf** *vrf-name* keyword and argument to configure this command per VRF, which allows multiple disjoined routing or forwarding tables, where the routes of a user have no correlation with the routes of another user.

Examples

The following example shows how to configure RADIUS to use the IP address of subinterface s2 for all outgoing RADIUS packets:

```
ip radius source-interface s2
```

The following example shows how to configure RADIUS to use the IP address of subinterface Ethernet0 for VRF definition:

```
ip radius source-interface Ethernet 0 vrf water
```

Related Commands

Command	Description
ip tacacs source-interface	Uses the IP address of a specified interface for all outgoing TACACS packets.
ip telnet source-interface	Allows a user to select an address of an interface as the source address for Telnet connections.
ip tftp source-interface	Allows a user to select the interface whose address will be used as the source address for TFTP connections.

ip reflexive-list timeout

To specify the length of time that reflexive access list entries will continue to exist when no packets in the session are detected, use the **ip reflexive-list timeout** command in global configuration mode. To reset the timeout period to the default timeout, use the **no** form of this command.

ip reflexive-list timeout *seconds*

no ip reflexive-list timeout

Syntax Description

seconds	Specifies the number of seconds to wait (when no session traffic is being detected) before temporary access list entries expire. Use a positive integer from 0 to 2,147,483. The default is 300 seconds.

Defaults

300 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command is used with reflexive filtering, a form of session filtering.

This command specifies when a reflexive access list entry will be removed after a period of no traffic for the session (the timeout period).

With reflexive filtering, when an IP upper-layer session begins from within your network, a temporary entry is created within the reflexive access list, and a timer is set. Whenever a packet belonging to this session is forwarded (inbound or outbound) the timer is reset. When this timer counts down to zero without being reset, the temporary reflexive access list entry is removed.

The timer is set to the *timeout period*. Individual timeout periods can be defined for specific reflexive access lists, but for reflexive access lists that do not have individually defined timeout periods, the global timeout period is used. The global timeout value is 300 seconds by default; however, you can change the global timeout to a different value at any time using this command.

This command does not take effect for reflexive access list entries that were already created when the command is entered; this command only changes the timeout period for entries created after the command is entered.

Examples

The following example sets the global timeout period for reflexive access list entries to 120 seconds:

```
ip reflexive-list timeout 120
```

The following example returns the global timeout period to the default of 300 seconds:

```
no ip reflexive-list timeout
```

Related Commands

Command	Description
evaluate	Nests a reflexive access list within an access list.
ip access-list	Defines an IP access list by name.
permit (reflexive)	Creates a reflexive access list and enables its temporary entries to be automatically generated.

ip scp server enable

To enable the router to securely copy files from a remote workstation, use the **ip scp server enable** command in global configuration mode. To disable secure copy functionality (the default), use the **no** form of this command.

ip scp server enable

no ip scp server enable

Syntax Description

This command has no arguments or keywords.

Defaults

The secure copy function is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)S	This command was integrated into Cisco IOS Release 12.0(21)S and support for the Cisco 7500 series and Cisco 12000 series routers was added.

Usage Guidelines

Use this command to enable secure copying of files from systems using the Secure Shell (SSH) application. This secure copy function is accomplished by an addition to the **copy** command in the Cisco IOS software, which takes care of using the secure copy protocol (scp) to copy to and from a router while logged in to the router itself. Because copying files is generally a restricted operation in the Cisco IOS software, a user attempting to copy such files needs to be at the correct enable level.

The Cisco IOS software must also allow files to be copied to or from itself from a remote workstation running the SSH application (which is supported by both the Microsoft Windows and UNIX operating systems). To get this information, the Cisco IOS software must have authentication and authorization configured in the authentication, authorization, and accounting (AAA) feature. SSH already relies on AAA authentication to authenticate the user username and password. Scp adds the requirement that AAA authorization be turned on so that the operating system can determine whether or not the user is at the correct privilege level.

Examples

The following example shows a typical configuration that allows the router to securely copy files from a remote workstation. Because scp relies on AAA authentication and authorization to function properly, AAA must be configured.

```
aaa new-model
aaa authentication login default tac-group tacacs+
aaa authorization exec default local
username user1 privilege 15 password 0 lab
ip scp server enable
```

The following example shows how to use scp to copy a system image from Flash memory to a server that supports SSH:

```
Router# copy flash:c4500-ik2s-mz.scp scp://user1@host1/

Address or name of remote host [host1]?
Destination username [user1]?
Destination filename [c4500-ik2s-mz.scp]?
Writing c4500-ik2s-mz.scp
Password:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Note When using scp, you cannot enter the password into the **copy** command; enter the password when prompted.

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.
aaa authorization	Sets parameters that restrict user access to a network.
copy	Copies any file from a source to a destination.
debug ip scp	Troubleshoots scp authentication problems.
ip ssh port	Enables secure network access to the tty lines.
username	Establishes a username-based authentication system.

ip sdee events

To set the maximum number of Security Device Event Exchange (SDEE) events that can be stored in the event buffer, use the **ip sdee events** command in global configuration mode. To change the buffer size or return to the default buffer size, use the **no** form of this command.

ip sdee events *events*

no ip sdee events *events*

Syntax Description

events	Maximum number of events; maximum number of allowable events: 1000.

Defaults

200 events

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

When SDEE notification is enabled (via the **ip ips notify sdee** command), 200 hundred events can automatically be stored in the buffer. When SDEE notification is disabled, all stored events are lost. A new buffer is allocated when the notifications are reenabled.

When specifying the size of an events buffer, note the following functionality:

- It is circular. When the end of the buffer is reached, the buffer will start overwriting the earliest stored events. (If overwritten events have not yet been reported, you will receive a buffer overflow notice.)
- If a new, smaller buffer is requested, all events that are stored in the previous buffer will be lost.
- If a new, larger buffer is requested, all existing events will be saved.

Examples

The following example shows how to set the maximum buffer events size to 500:

```
configure terminal
 ip ips notify sdee
 ip sdee events 500
```

Related Commands

Command	Description
ip ips notify	Specifies the method of event notification.

ip sdee subscriptions

To set the maximum number of Security Device Event Exchange (SDEE) subscriptions that can be open simultaneously, use the **ip sdee subscriptions** command in global configuration mode. To change the current selection or return to the default, use the **no** form of this command.

ip sdee subscriptions *subscriptions*

no ip sdee subscriptions *subscriptions*

Syntax Description

subscriptions	Maximum number of subscriptions; valid value ranges from 1 to 3.

Defaults

1 subscription

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

After you have enabled SDEE to receive and process events from Intrusion Prevention System (IPS) unless SDEE, you can issue the **ip sdee subscriptions** command to modify the number of allowed open SDEE subscriptions.

Examples

The following example shows how to change the number of allowed open subscriptions to 2:

```
configure terminal
 ip ips notify sdee
 ip sdee events 500
 ip sdee subscriptions 2
```

Related Commands

Command	Description
ip ips notify	Specifies the method of event notification.

ip security add

To add a basic security option to all outgoing packets, use the **ip security add** command in interface configuration mode. To disable the adding of a basic security option to all outgoing packets, use the **no** form of this command.

ip security add

no ip security add

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled, when the security level of the interface is "Unclassified Genser" (or unconfigured). Otherwise, the default is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If an outgoing packet does not have a security option present, this interface configuration command will add one as the first IP option. The security label added to the option field is the label that was computed for this packet when it first entered the router. Because this action is performed after all the security tests have been passed, this label will either be the same or will fall within the range of the interface.

Examples

The following example adds a basic security option to each packet leaving Ethernet interface 0:

```
interface ethernet 0
 ip security add
```

Related Commands

Command	Description
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.

Command	Description
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security aeso

To attach Auxiliary Extended Security Options (AESOs) to an interface, use the **ip security aeso** command in interface configuration mode. To disable AESO on an interface, use the **no** form of this command.

ip security aeso *source compartment-bits*

no ip security aeso *source compartment-bits*

Syntax Description

source	Extended Security Option (ESO) source. This can be an integer from 0 to 255.
compartment-bits	Number of compartment bits in hexadecimal.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Compartment bits are specified only if this AESO is to be inserted in a packet. On every incoming packet at this level on this interface, these AESOs should be present.

Beyond being recognized, no further processing of AESO information is performed. AESO contents are not checked and are assumed to be valid if the source is listed in the configurable AESO table.

Configuring any per-interface extended IP Security Option (IPSO) information automatically enables **ip security extended-allowed** (disabled by default).

Examples

The following example defines the Extended Security Option source as 5 and sets the compartments bits to 5:

```
interface ethernet 0
 ip security aeso 5 5
```

Related Commands

Command	Description
ip security eso-info	Configures system-wide defaults for extended IPSO information.
ip security eso-max	Specifies the maximum sensitivity level for an interface.
ip security eso-min	Configures the minimum sensitivity level for an interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.

ip security dedicated

To set the level of classification and authority on the interface, use the **ip security dedicated** command in interface configuration mode. To reset the interface to the default classification and authorities, use the **no** form of this command.

ip security dedicated *level authority* [*authority...*]

no ip security dedicated *level authority* [*authority...*]

Syntax Description

level	Degree of sensitivity of information. The *level* keywords are listed in Table 25.
authority	Organization that defines the set of security levels that will be used in a network. The authority keywords are listed in Table 26.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

All traffic entering the system on this interface must have a security option that exactly matches this label. Any traffic leaving via this interface will have this label attached to it.

The following definitions apply to the descriptions of the IP Security Option (IPSO) in this section:

- level—The degree of sensitivity of information. For example, data marked TOPSECRET is more sensitive than data marked SECRET. The level keywords and their corresponding bit patterns are shown in Table 25.

Table 25 IPSO Level Keywords and Bit Patterns

Level Keyword	Bit Pattern
Reserved4	0000 0001
TopSecret	0011 1101
Secret	0101 1010
Confidential	1001 0110
Reserved3	0110 0110
Reserved2	1100 1100
Unclassified	1010 1011
Reserved1	1111 0001

- authority—An organization that defines the set of security levels that will be used in a network. For example, the Genser authority consists of level names defined by the U.S. Defense Communications Agency (DCA). The authority keywords and their corresponding bit patterns are shown in Table 26.

Table 26 IPSO Authority Keywords and Bit Patterns

Authority Keyword	Bit Pattern
Genser	1000 0000
Siop-Esi	0100 0000
DIA	0010 0000
NSA	0001 0000
DOE	0000 1000

- label—A combination of a security level and an authority or authorities.

Examples

The following example sets a confidential level with Genser authority:

```
ip security dedicated confidential Genser
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security eso-info

To configure system-wide defaults for extended IP Security Option (IPSO) information, use the **ip security eso-info** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip security eso-info *source compartment-size default-bit*

no ip security eso-info *source compartment-size default-bit*

Syntax Description

source	Hexadecimal or decimal value representing the extended IPSO source. This is an integer from 0 to 255.
compartment-size	Maximum number of bytes of compartment information allowed for a particular extended IPSO source. This is an integer from 1 to 16.
default-bit	Default bit value for any unsent compartment bits.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command configures Extended Security Option (ESO) information, including Auxiliary Extended Security Option (AESO). Transmitted compartment information is padded to the size specified by the *compartment-size* argument.

Examples

The following example sets system-wide defaults for source, compartment size, and the default bit value:

```
ip security eso-info 100 5 1
```

Related Commands

Command	Description
ip security eso-max	Specifies the maximum sensitivity level for an interface.
ip security eso-min	Configures the minimum sensitivity level for an interface.

ip security eso-max

To specify the maximum sensitivity level for an interface, use the **ip security eso-max** command in interface configuration mode. To return to the default, use the **no** form of this command.

ip security eso-max *source compartment-bits*

no ip security eso-max *source compartment-bits*

Syntax Description

source	Extended Security Option (ESO) source. This is an integer from 1 to 255.
compartment-bits	Number of compartment bits in hexadecimal.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The command is used to specify the maximum sensitivity level for a particular interface. Before the per-interface compartment information for a particular Network-Level Extended Security Option (NLESO) source can be configured, the **ip security eso-info** global configuration command must be used to specify the default information.

On every incoming packet on the interface, these Extended Security Options should be present at the minimum level and should match the configured compartment bits. Every outgoing packet must have these ESOs.

On every packet transmitted or received on this interface, any NLESO sources present in the IP header should be bounded by the minimum sensitivity level and bounded by the maximum sensitivity level configured for the interface.

When transmitting locally generated traffic out this interface, or adding security information (with the **ip security add** command), the maximum compartment bit information can be used to construct the NLESO sources placed in the IP header.

A maximum of 16 NLESO sources can be configured per interface. Due to IP header length restrictions, a maximum of 9 of these NLESO sources appear in the IP header of a packet.

Examples

In the following example, the specified ESO source is 240 and the compartment bits are specified as 500:

```
interface ethernet 0
 ip security eso-max 240 500
```

Related Commands

Command	Description
ip security eso-info	Configures system-wide defaults for extended IPSO information.
ip security eso-min	Configures the minimum sensitivity level for an interface.

ip security eso-min

To configure the minimum sensitivity for an interface, use the **ip security eso-min** command in interface configuration mode. To return to the default, use the **no** form of this command.

ip security eso-min *source compartment-bits*

no ip security eso-min *source compartment-bits*

Syntax Description

source	Extended Security Option (ESO) source. This is an integer from 1 to 255.
compartment-bits	Number of compartment bits in hexadecimal.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The command is used to specify the minimum sensitivity level for a particular interface. Before the per-interface compartment information for a particular Network Level Extended Security Option (NLESO) source can be configured, the **ip security eso-info** global configuration command must be used to specify the default information.

On every incoming packet on this interface, these Extended Security Options should be present at the minimum level and should match the configured compartment bits. Every outgoing packet must have these ESOs.

On every packet transmitted or received on this interface, any NLESO sources present in the IP header should be bounded by the minimum sensitivity level and bounded by the maximum sensitivity level configured for the interface.

When transmitting locally generated traffic out this interface, or adding security information (with the **ip security add** command), the maximum compartment bit information can be used to construct the NLESO sources placed in the IP header.

A maximum of 16 NLESO sources can be configured per interface. Due to IP header length restrictions, a maximum of 9 of these NLESO sources appear in the IP header of a packet.

Examples

In the following example, the specified ESO source is 5, and the compartment bits are specified as 5:

```
interface ethernet 0
 ip security eso-min 5 5
```

Related Commands

Command	Description
ip security eso-info	Configures system-wide defaults for extended IPSO information.
ip security eso-max	Specifies the maximum sensitivity level for an interface.

ip security extended-allowed

To accept packets on an interface that has an extended security option present, use the **ip security extended-allowed** command in interface configuration mode. To restore the default, use the **no** form of this command.

ip security extended-allowed

no ip security extended-allowed

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Packets containing extended security options are rejected.

Examples

The following example allows interface Ethernet 0 to accept packets that have an extended security option present:

```
interface ethernet 0
 ip security extended-allowed
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security first

To prioritize the presence of security options on a packet, use the **ip security first** command in interface configuration mode. To prevent packets that include security options from moving to the front of the options field, use the **no** form of this command.

ip security first

no ip security first

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If a basic security option is present on an outgoing packet, but it is not the first IP option, then the packet is moved to the front of the options field when this interface configuration command is used.

Examples

The following example ensures that, if a basic security option is present in the options field of a packet exiting interface Ethernet 0, the packet is moved to the front of the options field:

```
interface ethernet 0
 ip security first
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.

Command	Description
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security ignore-authorities

To have the Cisco IOS software ignore the authorities field of all incoming packets, use the **ip security ignore-authorities** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip security ignore-authorities

no ip security ignore-authorities

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When the packet's authority field is ignored, the value used in place of this field is the authority value declared for the specified interface. The **ip security ignore-authorities** can be configured only on interfaces that have dedicated security levels.

Examples

The following example causes interface Ethernet 0 to ignore the authorities field on all incoming packets:

```
interface ethernet 0
 ip security ignore-authorities
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.

Command	Description
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security implicit-labelling

To force the Cisco IOS software to accept packets on the interface, even if they do not include a security option, use the **ip security implicit-labelling** command in interface configuration mode. To require security options, use the **no** form of this command.

ip security implicit-labelling [*level authority* [*authority...*]]

no ip security implicit-labelling [*level authority* [*authority...*]]

Syntax Description

level	(Optional) Degree of sensitivity of information. If your interface has multilevel security set, you must specify this argument. (See the *level* keywords listed in Table 25 in the **ip security dedicated** command section.)
authority	(Optional) Organization that defines the set of security levels that will be used in a network. If your interface has multilevel security set, you must specify this argument. You can specify more than one. (See the *authority* keywords listed in Table 26 in the **ip security dedicated** command section.)

Defaults

Enabled, when the security level of the interface is "Unclassified Genser" (or unconfigured). Otherwise, the default is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If your interface has multilevel security set, you must use the expanded form of the command (with the optional arguments as noted in brackets) because the arguments are used to specify the precise level and authority to use when labeling the packet. If your interface has dedicated security set, the additional arguments are ignored.

Examples

In the following example, an interface is set for security and will accept unlabeled packets:

```
ip security dedicated confidential genser
ip security implicit-labelling
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.

Command	Description
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security multilevel

To set the range of classifications and authorities on an interface, use the **ip security multilevel** command in interface configuration mode. To remove security classifications and authorities, use the **no** form of this command.

ip security multilevel *level1* [*authority1*...] **to** *level2 authority2* [*authority2*...]

no ip security multilevel

Syntax Description

level1	Degree of sensitivity of information. The classification level of incoming packets must be equal to or greater than this value for processing to occur. (See the *level* keywords found in Table 25 in the **ip security dedicated** command section.)
authority1	(Optional) Organization that defines the set of security levels that will be used in a network. The authority bits must be a superset of this value. (See the *authority* keywords listed in Table 26 in the **ip security dedicated** command section.)
to	Separates the range of classifications and authorities.
level2	Degree of sensitivity of information. The classification level of incoming packets must be equal to or less than this value for processing to occur. (See the *level* keywords found in Table 25 in the **ip security dedicated** command section.)
authority2	Organization that defines the set of security levels that will be used in a network. The authority bits must be a proper subset of this value. (See the *authority* keywords listed in Table 26 in the **ip security dedicated** command section.)

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

All traffic entering or leaving the system must have a security option that falls within this range. Being within range requires that the following two conditions be met:

- The classification level must be greater than or equal to *level1* and less than or equal to *level2*.
- The authority bits must be a superset of *authority1* and a proper subset of *authority2*. That is, *authority1* specifies those authority bits that are required on a packet, and *authority2* specifies the required bits plus any optional authorities that also can be included. If the *authority1* field is the empty set, then a packet is required to specify any one or more of the authority bits in *authority2*.

Examples

The following example specifies levels Unclassified to Secret and NSA authority:

```
ip security multilevel unclassified to secret nsa
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security reserved-allowed

To treat as valid any packets that have Reserved1 through Reserved4 security levels, use the **ip security reserved-allowed** command in interface configuration mode. To disallow packets that have security levels of Reserved3 and Reserved2, use the **no** form of this command.

ip security reserved-allowed

no ip security reserved-allowed

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

When you set multilevel security on an interface, and indicate, for example, that the highest range allowed is Confidential, and the lowest is Unclassified, the Cisco IOS software neither allows nor operates on packets that have security levels of Reserved3 and Reserved2 because they are undefined.

If you use the IP Security Option (IPSO) to block transmission out of unclassified interfaces, and you use one of the Reserved security levels, you *must* enable this feature to preserve network security.

Examples

The following example allows a security level of Reserved through Ethernet interface 0:

```
interface ethernet 0
 ip security reserved-allowed
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.

Command	Description
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security strip

To remove any basic security option on outgoing packets on an interface, use the **ip security strip** command in interface configuration mode. To restore security options, use the **no** form of this command.

ip security strip

no ip security strip

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The removal procedure is performed after all security tests in the router have been passed. This command is not allowed for multilevel interfaces.

Examples

The following example removes any basic security options on outgoing packets on Ethernet interface 0:

```
interface ethernet 0
 ip security strip
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.

ip source-track

To enable IP source tracking for a specified host, use the **ip source-track** command in global configuration mode. To disable IP source tracking, use the **no** form of this command.

ip source-track *ip-address*

no ip source-track *ip-address*

Syntax Description

ip-address	Destination IP address of the host that is to be tracked.

Defaults

IP address tracking is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

IP source tracking allows you to gather information about the traffic that is flowing to a host that is suspected of being under attack. It also allows you to easily trace a denial-of-service (DoS) attack to its entry point into the network.

After you have identified the destination that is being attacked, enable tracking for the destination address on the whole router by entering the **ip source-track** command.

Examples

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 100.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

Related Commands

Command	Description
ip source-track address-limit	Configures the maximum number of destination hosts that can be simultaneously tracked at any given moment.
ip source-track export-interval	Sets the time interval (in seconds) in which IP source tracking statistics are exported from the line card to the RP.
ip source-track syslog-interval	Sets the time interval (in minutes) in which syslog messages are generated if IP source tracking is enabled on a device.
show ip source-track	Displays traffic flow statistics for tracked IP host addresses.
show ip source-track export flows	Displays the last 10 packet flows that were exported from the line card to the route processor.

ip source-track address-limit

To configure the maximum number of destination hosts that can be simultaneously tracked at any given moment, use the **ip source-track address-limit** command in global configuration mode. To cancel this administrative limit and return to the default, use the **no** form of this command.

ip source-track address-limit *number*

no ip source-track address-limit *number*

Syntax Description

number	Maximum number of hosts that can be tracked.

Defaults

An unlimited number of hosts can be tracked.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

After you have configured at least one destination IP address for source tracking (via the **ip source-track** command), you can limit the number of destination IP addresses that can be tracked via the **ip source-track address-limit** command.

Examples

The following example shows how to configure IP source tracking for data that flows to host 100.10.1.1 and limit IP source tracking to 10 IP addresses:

```
Router(config)# ip source-track 100.10.0.1
Router(config)# ip source-track address-limit 10
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
show ip source-track	Displays traffic flow statistics for tracked IP host addresses.

ip source-track export-interval

To set the time interval (in seconds) in which IP source tracking statistics are exported from the line card to the route processor (RP), use the **ip source-track export-interval** command in global configuration mode. To return to default functionality, use the **no** form of this command.

ip source-track export-interval *number*

no ip source-track export-interval *number*

Syntax Description

number	Number of seconds that pass before IP source tracking statistics are exported.

Defaults

Traffic flow information is exported from the line card to the RP every 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

Use the **ip source-track export-interval** command to specify the frequency in which IP source tracking information is sent to the RP for viewing.

Note This command can be issued only on distributed platforms such as the gigabit route processor (GRP) and the route switch processor (RSP).

Examples

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 100.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
show ip source-track export flows	Displays the last 10 packet flows that were exported from the line card to the route processor.

ip source-track syslog-interval

To set the time interval (in minutes) in which syslog messages are generated if IP source tracking is enabled on a device, use the **ip source-track syslog-interval** command in global configuration mode. To cancel this setting and disable syslog generation, use the **no** form of this command.

ip source-track syslog-interval *number*

no ip source-track syslog-interval *number*

Syntax Description

number	IP address of the destination that is to be tracked.

Defaults

Syslog messages are not generated.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

Use the **ip source-track syslog-interval** command to track the source interfaces of traffic that are destined to a particular address.

Examples

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 100.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
show ip source-track	Displays traffic flow statistics for tracked IP host addresses.

ip ssh

To configure Secure Shell (SSH) control parameters on your router, use the **ip ssh** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip ssh [**timeout** *seconds* | **authentication-retries** *integer*]

no ip ssh [**timeout** *seconds* | **authentication-retries** *integer*]

Syntax Description

timeout	(Optional) The time interval that the router waits for the SSH client to respond. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0–4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.
seconds	(Optional) The number of seconds until timeout disconnects, with a maximum of 120 seconds. The default is 120 seconds.
authentication-retries	(Optional) The number of attempts after which the interface is reset.
integer	(Optional) The number of retries, with a maximum of 5 authentication retries. The default is 3.

Defaults

120 seconds for the timeout timer

3 authentication retries

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1) T.

Usage Guidelines

Before you configure SSH on your router, you must enable the SSH server using the **crypto key generate rsa** command.

Examples

The following examples configure SSH control parameters on your router:

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

ip ssh port

To enable secure access to tty (asynchronous) lines, use the **ip ssh port** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip ssh port *por-tnum* **rotary** *group*

no ip ssh port *por-tnum* **rotary** *group*

Syntax Description

port-num	Specifies the port, such as 2001, to which Secure Shell (SSH) needs to connect.
rotary *group*	Specifies the defined rotary that should search for a valid name.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The **ip ssh port** command supports a functionality that replaces reverse Telnet with SSH. Use this command to securely access the devices attached to the serial ports of a router and to perform the following tasks:

- Connect to a router with multiple terminal lines that are connected to consoles of other devices.
- Allow network available modems to be securely accessed for dial-out.

Examples

The following example shows how to configure the SSH Terminal-Line Access feature on a modem that is used for dial-out on lines 1 through 200:

```
line 1 200
 no exec
 login authentication default
 rotary 1
 transport input ssh

ip ssh port 2000 rotary 1
```

The following example shows how to configure the SSH Terminal-Line Access feature to access the console ports of various devices that are attached to the serial ports of the router. For this type of access, each line is put into its own rotary, and each rotary is used for a single port. In this example, lines 1 through 3 are used, and the port (line) mappings of the configuration are as follows: Port 2001 = Line 1, Port 2002 = Line 2, and Port 2003 = Line 3.

```
line 1
 no exec
```

```
 login authentication default
 rotary 1
 transport input ssh
line 2
 no exec
 login authentication default
 rotary 2
 transport input ssh
line 3
 no exec
 login authentication default
 rotary 3
 transport input ssh

ip ssh port 2001 rotary 1 3
```

From any UNIX or UNIX-like device, the following command is typically used to form an SSH session:

```
ssh -c 3des -p 2002 router.example.com
```

This command will initiate an SSH session using the 3DES cipher to the device known as "router.example.com," which uses port 2002. This device will connect to the device on Line 2, which was associated with port 2002. Similarly, many Windows SSH packages have related methods of selecting the cipher and the port for this access.

Related Commands

Command	Description
ip ssh	Configures SSH control variables on your router.
line	Identifies a specific line for configuration and begins the command in line configuration mode.
rotary	Defines a group of lines consisting of one or more lines.
ssh	Starts an encrypted session with a remote networking device.
transport input	Defines which protocols to use to connect to a specific line of the router.

ip ssh rsa keypair-name

To specify which Rivest, Shimar, and Adelman (RSA) key pair to use for a Secure Shell (SSH) connection, use the **ip ssh rsa keypair-name** command in global configuration mode. To disable the key pair that was configured, use the **no** form of this command.

ip ssh rsa keypair-name *keypair-name*

no ip ssh rsa keypair-name *keypair-name*

Syntax Description

keypair-name	Name of the key pair.

Defaults

If this command is not configured, SSH will use the first RSA key pair that is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(2)XE	This command was introduced into Cisco IOS Release 12.3(2)XE.

Usage Guidelines

Using the **ip ssh rsa keypair-name** command, you can enable an SSH connection using RSA keys that you have configured using the *keypair-name* argument. Previously, SSH was tied to the first RSA keys that were generated (that is, SSH was enabled when the first RSA key pair was generated). The previous behavior still exists but by using the **ip ssh rsa keypair-name** command, you can overcome that behavior. If you configure the **ip ssh rsa keypair-name** command with a key pair name, SSH is enabled if the key pair exists, or SSH will be enabled if the key pair is generated later. If you use this command, you are not forced to configure a host name and a domain name.

Note A Cisco IOS router can have many RSA key pairs.

Examples

The following example shows that the **ip ssh rsa keypair-name** command has been used to specify the RSA key pair "sshkeys" for a SSH connection:

```
Router# configure terminal
Router (config)# ip ssh rsa keypair-name sshkeys
```

Related Commands

Command	Description
debug ip ssh	Displays debug messages for SSH.
disconnect ssh	Terminates a SSH connection on your router.
ip ssh	Configures SSH control parameters on your router.

Command	Description
ip ssh version	Specifies the version of SSH to be run on a router.
show ip ssh	Displays the SSH connections of your router.

ip ssh version

To specify the version of Secure Shell (SSH) to be run on a router, use the **ip ssh version** command in global configuration mode. To disable the version of SSH that was configured and to return to compatibility mode, use the **no** form of this command.

ip ssh version [1 | 2]

no ip ssh version [1 | 2]

Syntax Description

1	(Optional) Router runs only SSH Version 1.
2	(Optional) Router runs only SSH Version 2.

Defaults

If this command is not configured, SSH operates in compatibility mode, that is, Version 1 and Version 2 are both supported.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(2)XE	This command was introduced into Cisco IOS Release 12.3(2)XE.

Usage Guidelines

You can use this command with the **2** keyword to ensure that your router will not inadvertently establish a weaker SSH Version 1 connection.

Examples

The following example shows that only SSH Version 1 support is configured:

```
Router (config)# ip ssh version 1
```

The following example shows that only SSH Version 2 is configured:

Router (config)# **ip ssh version 2**

The following example shows that SSH Versions 1 and 2 are configured:

Router (config)# **no ip ssh version**

Related Commands

Command	Description
debug ip ssh	Displays debug messages for SSH.
disconnect ssh	Terminates a SSH connection on your router.
ip ssh	Configures SSH control parameters on your router.

Command	Description
ip ssh rsa keypair-name	Specifies which RSA key pair to use for a SSH connection.
show ip ssh	Displays the SSH connections of your router.

ip tacacs source-interface

To use the IP address of a specified interface for all outgoing TACACS+ packets, use the **ip tacacs source-interface** command in global configuration or server-group configuration mode. To disable use of the specified interface IP address, use the **no** form of this command.

ip tacacs source-interface *subinterface-name*

no ip tacacs source-interface

Syntax Description

subinterface-name	Name of the interface that TACACS+ uses for all of its outgoing packets.

Defaults

No default behavior or values.

Command Modes

Global configuration

Server-group configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	This command was introduced in server-group configuration mode.

Usage Guidelines

Use this command to set the IP address of a subinterface for all outgoing TACACS+ packets. This address is used as long as the interface is in the *up* state. In this way, the TACACS+ server can use one IP address entry associated with the network access client instead of maintaining a list of all IP addresses.

This command is especially useful in cases where the router has many interfaces and you want to ensure that all TACACS+ packets from a particular router have the same IP address.

The specified interface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in a *down* state, TACACS+ reverts to the default. To avoid this situation, add an IP address to the subinterface or bring the interface to the *up* state.

Note This command can be configured globally or in server-group configuration mode. If this command is configured in the server-group configuration mode, the IP address of the specified interface is used for packets that are going only to servers that are defined in that server group. If this command is not configured in server-group configuration mode, the global configuration applies.

Examples

The following example makes TACACS+ use the IP address of subinterface “s2” for all outgoing TACACS+ packets:

```
ip tacacs source-interface s2
```

In the following example, TACACS+ is to use the IP address of Loopback0 for packets that are going only to server 10.1.1.1:

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0

  ip vrf cisco
   rd 100:1

  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
ip telnet source-interface	Allows a user to select an address of an interface as the source address for Telnet connections.
ip tftp source-interface	Allows a user to select the interface whose address will be used as the source address for TFTP connections.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.
server-private	Configures the IP address of the private RADIUS or TACACS+ server for the group server.

ip tcp intercept connection-timeout

To change how long a TCP connection will be managed by the TCP intercept after no activity, use the **ip tcp intercept connection-timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept connection-timeout *seconds*

no ip tcp intercept connection-timeout [*seconds*]

Syntax Description

seconds	Time (in seconds) that the software will still manage the connection after no activity. The minimum value is 1 second. The default is 86,400 seconds (24 hours).

Defaults

86,400 seconds (24 hours)

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

Use the **ip tcp intercept connection-timeout** command to change how long a TCP connection will be managed by the TCP intercept after a period of inactivity.

Examples

The following example sets the software to manage the connection for 12 hours (43,200 seconds) after no activity:

```
ip tcp intercept connection-timeout 43200
```

ip tcp intercept drop-mode

To set the TCP intercept drop mode, use the **ip tcp intercept drop-mode** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept drop-mode [**oldest** | **random**]

no ip tcp intercept drop-mode [**oldest** | **random**]

Syntax Description

oldest	(Optional) Software drops the oldest partial connection. This is the default.
random	(Optional) Software drops a randomly selected partial connection.

Defaults

oldest

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

If the number of incomplete connections exceeds 1100 or the number of connections arriving in the last 1 minute exceeds 1100, the TCP intercept feature becomes more aggressive. When this happens, each new arriving connection causes the oldest partial connection to be deleted, and the initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection will be cut in half).

Note that the 1100 thresholds can be configured with the **ip tcp intercept max-incomplete high** and **ip tcp intercept one-minute high** commands.

Use the **ip tcp intercept drop-mode** command to change the dropping strategy from oldest to a random drop.

Examples

The following example sets the drop mode to random:

```
ip tcp intercept drop-mode random
```

Related Commands

Command	Description
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.

Command	Description
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept finrst-timeout

To change how long after receipt of a reset or FIN-exchange the software ceases to manage the connection, use the **ip tcp intercept finrst-timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept finrst-timeout *seconds*

no ip tcp intercept finrst-timeout [*seconds*]

Syntax Description

seconds	Time (in seconds) after receiving a reset or FIN-exchange that the software ceases to manage the connection. The minimum value is 1 second. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

Even after the two ends of the connection are joined, the software intercepts packets being sent back and forth. Use this command if you need to adjust how soon after receiving a reset or FIN-exchange the software stops intercepting packets.

Examples

The following example sets the software to wait for 10 seconds before it leaves intercept mode:

```
ip tcp intercept finrst-timeout 10
```

ip tcp intercept list

To enable TCP intercept, use the **ip tcp intercept list** command in global configuration mode. To disable TCP intercept, use the **no** form of this command.

ip tcp intercept list *access-list-number*

no ip tcp intercept list *access-list-number*

Syntax Description

access-list-number	Extended access list number in the range from 100 to 199.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

The TCP intercept feature intercepts TCP connection attempts and shields servers from TCP SYN-flood attacks, also known as denial-of-service attacks.

TCP packets matching the access list are presented to the TCP intercept code for processing, as determined by the **ip tcp intercept mode** command. The TCP intercept code either intercepts or watches the connections.

To have all TCP connection attempts submitted to the TCP intercept code, have the access list match everything.

Examples

The following example configuration defines access list 101, causing the software to intercept packets for all TCP servers on the 192.168.1.0/24 subnet:

```
ip tcp intercept list 101
!
access-list 101 permit tcp any 192.168.1.0 0.0.0.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
ip tcp intercept mode	Changes the TCP intercept mode.
show tcp intercept connections	Displays TCP incomplete and established connections.
show tcp intercept statistics	Displays TCP intercept statistics.

ip tcp intercept max-incomplete high

To define the maximum number of incomplete connections allowed before the software enters aggressive mode, use the **ip tcp intercept max-incomplete high** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept max-incomplete high *number*

no ip tcp intercept max-incomplete high [*number*]

Syntax Description

number	Defines the number of incomplete connections allowed, above which the software enters aggressive mode. The range is from 1 to 2147483647. The default is 1100.

Defaults

1100 incomplete connections

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

If the number of incomplete connections exceeds the *number* configured, the TCP intercept feature becomes aggressive. The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.
- The initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection is cut in half).
- The watch-timeout is cut in half (from 30 seconds to 15 seconds).

You can change the drop strategy from the oldest connection to a random connection with the **ip tcp intercept drop-mode** command.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of ip tcp intercept one-minute low and **ip tcp intercept max-incomplete low**, aggressive mode ends.

The software will back off from its aggressive mode when the number of incomplete connections falls below the number specified by the **ip tcp intercept max-incomplete low** command.

Examples

The following example allows 1500 incomplete connections before the software enters aggressive mode:

```
ip tcp intercept max-incomplete high 1500
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept max-incomplete low

To define the number of incomplete connections below which the software leaves aggressive mode, use the **ip tcp intercept max-incomplete low** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept max-incomplete low *number*

no ip tcp intercept max-incomplete low [*number*]

Syntax Description

number	Defines the number of incomplete connections below which the software leaves aggressive mode. The range is 1 to 2147483647. The default is 900.

Defaults

900 incomplete connections

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, the TCP intercept feature leaves aggressive mode.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

See the **ip tcp intercept max-incomplete high** command for a description of aggressive mode.

Examples

The following example sets the software to leave aggressive mode when the number of incomplete connections falls below 1000:

```
ip tcp intercept max-incomplete low 1000
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept mode

To change the TCP intercept mode, use the **ip tcp intercept mode** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept mode {**intercept** | **watch**}

no ip tcp intercept mode [**intercept** | **watch**]

Syntax Description

intercept	Active mode in which the TCP intercept software intercepts TCP packets from clients to servers that match the configured access list and performs intercept duties. This is the default.
watch	Monitoring mode in which the software allows connection attempts to pass through the router and watches them until they are established.

Defaults

intercept

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

When TCP intercept is enabled, it operates in intercept mode by default. In intercept mode, the software actively intercepts TCP SYN packets from clients to servers that match the specified access list. For each SYN, the software responds on behalf of the server with an ACK and SYN, and waits for an ACK of the SYN from the client. When that ACK is received, the original SYN is sent to the server, and the code then performs a three-way handshake with the server. Then the two half-connections are joined.

In watch mode, the software allows connection attempts to pass through the router, but watches them until they become established. If they fail to become established in 30 seconds (or the value set by the **ip tcp intercept watch-timeout** command), a Reset is sent to the server to clear its state.

Examples

The following example sets the mode to watch mode:

```
ip tcp intercept mode watch
```

Related Commands

Command	Description
ip tcp intercept watch-timeout	Defines how long the software will wait for a watched TCP intercept connection to reach established state before sending a reset to the server.

ip tcp intercept one-minute high

To define the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode, use the **ip tcp intercept one-minute high** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept one-minute high *number*

no ip tcp intercept one-minute high [*number*]

Syntax Description

number	Specifies the number of connection requests that can be received in the last one-minute sample period before the software enters aggressive mode. The range is 1 to 2147483647. The default is 1100.

Defaults

1100 connection requests

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

If the number of connection requests exceeds the *number* value configured, the TCP intercept feature becomes aggressive. The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.
- The initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection is cut in half).
- The watch-timeout is cut in half (from 30 seconds to 15 seconds).

You can change the drop strategy from the oldest connection to a random connection with the **ip tcp intercept drop-mode** command.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

Examples

The following example allows 1400 connection requests before the software enters aggressive mode:

```
ip tcp intercept one-minute high 1400
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept one-minute low

To define the number of connection requests below which the software leaves aggressive mode, use the **ip tcp intercept one-minute low** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept one-minute low *number*

no ip tcp intercept one-minute low [*number*]

Syntax Description

number	Defines the number of connection requests in the last one-minute sample period below which the software leaves aggressive mode. The range is from 1 to 2147483647. The default is 900.

Defaults

900 connection requests

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, the TCP intercept feature leaves aggressive mode.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

See the **ip tcp intercept one-minute high** command for a description of aggressive mode.

Examples

The following example sets the software to leave aggressive mode when the number of connection requests falls below 1000:

```
ip tcp intercept one-minute low 1000
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.

ip tcp intercept watch-timeout

To define how long the software will wait for a watched TCP intercept connection to reach established state before sending a reset to the server, use the **ip tcp intercept watch-timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept watch-timeout *seconds*

no ip tcp intercept watch-timeout [*seconds*]

Syntax Description

seconds	Time (in seconds) that the software waits for a watched connection to reach established state before sending a Reset to the server. The minimum value is 1 second. The default is 30 seconds.

Defaults

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

Use this command if you have set the TCP intercept to passive watch mode and you want to change the default time the connection is watched. During aggressive mode, the watch timeout time is cut in half.

Examples

The following example sets the software to wait 60 seconds for a watched connection to reach established state before sending a Reset to the server:

```
ip tcp intercept watch-timeout 60
```

Related Commands

Command	Description
ip tcp intercept mode	Changes the TCP intercept mode.

ip traffic-export apply profile

To apply an IP traffic export profile to a specific interface, use the **ip traffic-export apply profile** command in interface configuration mode. To remove an IP traffic export profile from an interface, use the **no** form of this command.

ip traffic-export apply profile *profile-name*

no ip traffic-export apply profile *profile-name*

Syntax Description

profile-name	Name of the profile that is to be applied to a specified interface. The *profile-name* argument must match a name that was specified via the **ip traffic-export profile** command.

Defaults

If this command is not issued, a sucessfully configured profile is not active.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

After you have configured at least one profile, you should use the **ip traffic-export apply profile** command to activate an IP traffic export on the specified ingress interface.

Examples

The following example shows how to apply the profile “corp1” to interface Fast Ethernet 0/0:

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list spam_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

After the profile is activated on the interface, a logging message such as the following will appear:

```
%RITE-5-ACTIVATE: Activated IP traffic export on interface FastEthernet 0/0.
```

After the profile is removed from the interface, a logging message such as the following will appear:

```
%RITE-5-DEACTIVATE: Deactivated IP traffic export on interface FastEthernet 0/0.
```

If you attempt to apply an incomplete profile to an interface, you will receive the following message:

```
Router(config-if)# ip traffic-export apply newone
RITE: profile newone has missing outgoing interface
```

Related Commands

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.

ip traffic-export profile

To create or edit an IP traffic export profile and enable the profile on an ingress interface, use the **ip traffic-export profile** command in global configuration mode. To remove an IP traffic export profile from your router configuration, use the **no** form of this command.

ip traffic-export profile *profile-name*

no ip traffic-export profile *profile-name*

Syntax Description

profile-name	IP traffic export profile name.

Defaults

A profile does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

The **ip traffic-export profile** command allows you to begin a profile that can be configured to export IP packets as they arrive on or leave from a selected router ingress interface. A designated egress interface exports the captured IP packets out of the router. Thus, the router can export unaltered IP packets to a directly connected device.

IP Traffic Export Profiles

All exported IP traffic configurations are specified via profiles, which consist of RITE-related command-line interfaces (CLIs) that control various attributes of both incoming and outgoing IP traffic. You can configure a router with multiple profiles. (Each profile must have a different name.) You can apply different profiles on different interfaces.

The two profiles that you should configure are as follows:

- The global configuration profile, which is configured via the **ip traffic-export profile** command.
- The submode configuration profile, which is configured via any of the following RITE commands—**bidirectional**, **incoming**, **interface**, **mac-address**, and **outgoing**.

The **interface** and **mac-address** commands are required to successfully create a profile. If these commands are not issued, the user will receive a profile incomplete messages such as the following:

```
ip traffic-export profile newone
! No outgoing interface configured
! No destination mac-address configured
```

After you configure your profiles, you can apply (which will activate) the profile to an interface via the **ip traffic-export apply profile** command.

Examples

The following example shows how to configure the profile "corp1," which will send captured IP traffic to host "00a.8aab.90a0" at the interface "FastEthernet 0/1." This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the access control list (ACL) "ham_ACL."

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported across a monitored interface.
incoming	Configures filtering for incoming export traffic.
interface (RITE)	Specifies the outgoing interface for exporting traffic
ip traffic-export apply profile	Applies an IP traffic export profile to a specific interface.
mac-address	Specifies the Ethernet address of the destination host.
outgoing	Configures filtering for outgoing export traffic.

ip trigger-authentication (global)

To enable the automated part of double authentication at a device, use the **ip trigger-authentication** command in global configuration mode. To disable the automated part of double authentication, use the **no** form of this command.

ip trigger-authentication [**timeout** *seconds*] [**port** *number*]

no ip trigger-authentication

Syntax Description

timeout *seconds*	(Optional) Specifies how frequently the local device sends a User Datagram Protocol (UDP) packet to the remote host to request the user's username and password (or PIN). The default is 90 seconds. See "The Timeout Keyword" in the Usage Guidelines section for details.
port *number*	(Optional) Specifies the UDP port to which the local router should send the UPD packet requesting the user's username and password (or PIN). The default is port 7500. See "The Port Keyword" in the Usage Guidelines section for details.

Defaults

The default timeout is 90 seconds, and the default port number is 7500.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Configure this command on the local device (router or network access server) that remote users dial in to. Use this command only if the local device has already been configured to provide double authentication; this command enables automation of the second authentication of double authentication.

The timeout Keyword

During the second authentication stage of double authentication—when the remote user is authenticated—the remote user must send a username and password (or PIN) to the local device. With automated double authentication, the local device sends a UDP packet to the remote user's host during the second user-authentication stage. This UDP packet triggers the remote host to launch a dialog box requesting a username and password (or PIN).

If the local device does not receive a valid response to the UDP packet within a timeout period, the local device will send another UDP packet. The device will continue to send UDP packets at the timeout intervals until it receives a response and can authenticate the user.

By default, the UDP packet timeout interval is 90 seconds. Use the **timeout** keyword to specify a different interval.

(This timeout also applies to how long entries will remain in the remote host table; see the **show ip trigger-authentication** command for details.)

The port Keyword

As described in the previous section, the local device sends a UDP packet to the remote user's host to request the user's username and password (or PIN). This UDP packet is sent to UDP port 7500 by default. (The remote host client software listens to UDP port 7500 by default.) If you need to change the port number because port 7500 is used by another application, you should change the port number using the **port** keyword. If you change the port number you need to change it in both places—both on the local device and in the remote host client software.

Examples

The following example globally enables automated double authentication and sets the timeout to 120 seconds:

```
ip trigger-authentication timeout 120
```

Related Commands

Command	Description
ip trigger-authentication (interface)	Specifies automated double authentication at an interface.
show ip trigger-authentication	Displays the list of remote hosts for which automated double authentication has been attempted.

ip trigger-authentication (interface)

To specify automated double authentication at an interface, use the **ip trigger-authentication** command in interface configuration mode. To turn off automated double authentication at an interface, use the **no** form of this command.

ip trigger-authentication

no ip trigger-authentication

Syntax Description

This command has no arguments or keywords.

Defaults

Automated double authentication is not enabled for specific interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Configure this command on the local router or network access server that remote users dial into. Use this command only if the local device has already been configured to provide double authentication and if automated double authentication has been enabled with the **ip trigger-authentication** (global) command.

This command causes double authentication to occur automatically when users dial into the interface.

Examples

The following example turns on automated double authentication at the ISDN BRI interface BRI0:

```
interface BRI0
 ip trigger-authentication
 encapsulation ppp
 ppp authentication chap
```

Related Commands

Command	Description
ip trigger-authentication (global)	Enables the automated part of double authentication at a device.

ip urlfilter alert

To enable URL filtering system alert messages, use the **ip urlfilter alert** command in global configuration mode. To disable the system alert, use the **no** form of this command.

ip urlfilter alert

no ip urlfilter alert

Syntax Description

This command has no arguments or keywords.

Defaults

URL filtering messages are enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

Use the **ip urlfilter alert** command to display system messages, such as a server entering allow mode, a server going down, or a URL that is too long for the lookup request.

Examples

The following example shows how to enable URL filtering alert messages:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Afterward, system alert messages such as the following are displayed:

```
%URLF-3-SERVER_DOWN:Connection to the URL filter server 10.92.0.9 is down
```

This level three LOG_ERR-type message is displayed when a configured URL filter server (UFS) goes down. When this happens, the firewall will mark the configured server as secondary and try to bring up one of the other secondary servers and mark that server as the primary server. If there is no other server configured, the firewall will enter into allow mode and display the URLF-3-ALLOW_MODE message described.

```
%URLF-3-ALLOW_MODE:Connection to all URL filter servers are down and ALLOW MODE is OFF
```

This LOG_ERR type message is displayed when all UFSs are down and the system enters into allow mode.

Note Whenever the system goes into allow mode (all filter servers are down), a periodic keepalive timer will be triggered that will try to bring up a server by opening a TCP connection.

```
%URLF-5-SERVER_UP:Connection to an URL filter server 10.92.0.9 is made, the system is
returning from ALLOW MODE
```

This LOG_NOTICE-type message is displayed when the UFSs are detected as being up and the system is returning from allow mode.

```
%URLF-4-URL_TOO_LONG:URL too long (more than 3072 bytes), possibly a fake packet?
```

This LOG_WARNING-type message is displayed when the URL in a lookup request is too long; any URL longer than 3K will be dropped.

```
%URLF-4-MAX_REQ:The number of pending request exceeds the maximum limit <1000>
```

This LOG_WARNING-type message is displayed when the number of pending requests in the system exceeds the maximum limit and all further requests are dropped.

ip urlfilter allowmode

To turn on the default mode (allow mode) of the filtering algorithm, use the **ip urlfilter allowmode** command in global configuration mode. To disable the default mode, use the **no** form of this command.

ip urlfilter allowmode [**on** | **off**]

no ip urlfilter allowmode [**on** | **off**]

Syntax Description

on	(Optional) Allow mode is on.
off	(Optional) Allow mode is off.

Defaults

Allow mode is off.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

The system will go into allow mode when connections to all vendor servers (Websense or N2H2) are down. The system will return to normal mode when a connection to at least one web vendor server is up. Allow mode directs your system to forward or drop all packets on the basis of the configurable allow mode setting: if allow mode is on and the vendor servers are down, the HTTP requests will be allowed to pass; if allow mode is off and the vendor servers are down, the HTTP requests will be forbidden.

Examples

The following example shows how to enable allow mode on your system:

```
ip urlfilter allowmode on
```

Afterward, the following alert message will be displayed when the system goes into allow mode:

```
%URLF-3-ALLOW_MODE: Connection to all URL filter servers are down and ALLOW MODE if OFF
```

The following alert message will be displayed when the system returns from allow mode:

```
%URLF-5-SERVER_UP: Connection to an URL filter server 12.0.0.3 is made, the system is
returning from allow mode
```

ip urlfilter audit-trail

To log messages into the syslog server or router, use the **ip urlfilter audit-trail** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip urlfilter audit-trail

no ip urlfilter audit-trail

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

Use the **ip urlfilter audit-trail** command to log messages such as URL request status (allow or deny) into your syslog server.

Examples

The following example shows how to enable syslog message logging:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 209.165.202.130
```

Afterward, audit trail messages such as the following are displayed and logged into the log server:

```
%URLF-6-SITE_ALLOWED:Client 209.165.201.15:12543 accessed server 10.76.82.21:8080
```

This message is logged for each request whose destination IP address is found in the cache. It includes the source IP address, source port number, destination IP address, and destination port number. The URL is not logged in this case because the IP address of the request is found in the cache; thus, parsing the request and extracting the URL is a waste of time.

```
%URLF-4-SITE-BLOCKED: Access denied for the site 'www.sports.com'; client
209.165.200.230:34557 server 209.165.201.2:80
```

This message is logged when a request finds a match against one of the blocked domains in the exclusive-domain list or the corresponding entry in the IP cache.

```
%URLF-6-URL_ALLOWED:Access allowed for URL http://www.N2H2.com/; client
209.165.200.230:54123  server 192.168.0.1:80
```

This message is logged for each URL request that is allowed by the vendor server (Websense or N2H2). It includes the allowed URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.

```
%URLF-6-URL_BLOCKED:Access denied URL http://www.google.com; client 209.165.200.230:54678
server 209.165.201.2:80
```

This message is logged for each URL request that is blocked by the vendor server. It includes the blocked URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.

ip urlfilter cache

To configure cache parameters, use the **ip urlfilter cache** command in global configuration mode. To clear the configuration, use the **no** form of this command.

ip urlfilter cache *number*

no ip urlfilter cache *number*

Syntax Description

number	Maximum number of destination IP addresses that can be cached into the cache table. The default value is 5000.

Defaults

Maximum number of destination IP addresses is 5000.

The cache table is cleared out every 12 hours.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

The cache table consists of the most recently requested IP addresses and respective authorization status for each IP address.

The caching algorithm involves three parameters—the maximum number of IP addresses that can be cached, an idle time, and an absolute time. The algorithm also involves two timers—idle timer and absolute timer. The idle timer is a small periodic timer (1 minute) that checks to see whether the number of cached IP addresses in the cache table exceeds 80 percent of the maximum limit. If the cached IP addresses have exceeded 80 percent, it will start removing idle entries; if it has not exceeded 80 percent, it will quit and wait for the next cycle. The absolute timer is a large periodic timer (1 hour) that is used to remove all of the elapsed entries. (The age of an elapsed entry is greater than the absolute time.) An elapsed entry will also be removed during cache lookup.

The idle time value is fixed at 10 minutes. The absolute time value is taken from the vendor server look-up response, which is often greater than 15 hours. The absolute value for cache entries made out of exclusive-domains is 12 hours. The maximum number of cache entries is configurable by enabling the **ip urlfilter cache** command.

Note The vendor server is not able to inform the Cisco IOS firewall of filtering policy changes in the database.

Examples

The following example shows how to configure the cache table to hold a maximum of five destination IP addresses:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Related Commands

Command	Description
clear ip urlfilter cache	Clears the cache table.
show ip urlfilter cache	Displays the destination IP addresses that are cached into the cache table.

ip urlfilter exclusive-domain

To add or remove a domain name to or from the exclusive domain list so that the firewall does not have to send lookup requests to the vendor server, use the **ip urlfilter exclusive-domain** command in global configuration mode. To remove a domain name from the exclusive domain name list, use the **no** form of this command.

ip urlfilter exclusive-domain {**permit** | **deny**} *domain-name*

no ip urlfilter exclusive-domain {**permit** | **deny**} *domain-name*

Syntax Description

permit	Permits all traffic destined for the specified domain name.
deny	Blocks all traffic destined for the specified domain name.
domain-name	Domain name that is added or removed from the exclusive domain name list; for example, www.cisco.com.

Defaults

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

The **ip urlfilter exclusive-domain** command allows you to specify a list of domain names (exclusive domains) so that the firewall will not create a lookup request for the HTTP traffic that is destined for one of the domains in the exclusive list. Thus, you can avoid sending look-up requests to the web server for HTTP traffic that is destined for a host that is completely allowed to all users.

Flexibility when entering domain names is also provided; that is, the user can enter the complete domain name or a partial domain name.

Complete Domain Name

If the user adds a complete domain name, such as “www.cisco.com,” to the exclusive domain list, all HTTP traffic whose URLs are destined for this domain (such as www.cisco.com/news and www.cisco.com/index) will be excluded from the URL filtering policies of the vendor server (Websense or N2H2), and on the basis of the configuration, the URLs will be permitted or blocked (denied).

Partial Domain Name

If the user adds only a partial domain name to the exclusive domain list, such as “.cisco.com,” all URLs whose domain names end with this partial domain name (such as www.cisco.com/products and www.cisco.com/eng) will be excluded from the URL filtering policies of the vendor server (Websense or N2H2), and on the basis of the configuration, the URLs will be permitted or blocked (denied).

Examples

The following example shows how to add the complete domain name “www.cisco.com” to the exclusive domain name list. This configuration will block all traffic destined to the www.cisco.com domain.

```
ip urlfilter exclusive-domain deny www.cisco.com
```

The following example shows how to add the partial domain name “.cisco.com” to the exclusive domain name list. This configuration will permit all traffic destined to domains that end with .cisco.com.

```
ip urlfilter exclusive-domain permit .cisco.com
```

ip urlfilter max-request

To set the maximum number of outstanding requests that can exist at any given time, use the **ip urlfilter max-request** command in global configuration mode. To disable this function, use the **no** form of this command.

ip urlfilter max-request *number*

no ip urlfilter max-request *number*

Syntax Description

number	Maximum number of outstanding requests. The default value is 1000.

Defaults

Maximum number of requests is 1000.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

If the specified maximum number of outstanding requests is exceeded, new requests will be dropped.

Note Allow mode is not considered because it should be used only when servers are down.

Examples

The following example shows how to configure the maximum number of outstanding requests to 950:

```
ip inspect name url_filter http
ip urlfilter max-request 950
```

Related Commands

Command	Description
ip inspect name	Defines a set of inspection rules.
ip urlfilter server vendor	Configures a vendor server for URL filtering.

ip urlfilter max-resp-pak

To configure the maximum number of HTTP responses that the firewall can keep in its packet buffer, use the **ip urlfilter max-resp-pak** command in global configuration mode. To return to the default, use the **no** form of this command.

ip urlfilter max-resp-pak *number*

no ip urlfilter max-resp-pak *number*

Syntax Description

number	Maximum number of HTTP responses that can be stored in the packet buffer of the firewall. After the maximum number has been reached, the firewall will drop further responses. The default, and absolute maximum, value is 200.

Defaults

200 HTTP responses

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

When an HTTP request arrives at a Cisco IOS firewall, the firewall forwards the request to the web server while simultaneously sending a URL look-up request to the vendor server (Websense or N2H2). If the vendor server reply arrives before the HTTP response, the firewall will know whether to permit or block the HTTP response; if the HTTP response arrives before the vendor server reply, the firewall will not know whether to allow or block the response, so the firewall will drop the response until it hears from the vendor server. The **ip urlfilter max-resp-pak** command allows you to configure your firewall to store the HTTP responses in a buffer, which allows your firewall to store a maximum of 200 HTTP responses. Each response will remain in the buffer until an allow or deny message is received from the vendor server. If the vendor server reply allows the URL, the firewall will release the HTTP response from the buffer to the end user; if the vendor server reply denies the URL, the firewall will discard the HTTP response from the buffer and close the connection to both ends.

Examples

The following example shows how to configure your firewall to hold 150 HTTP responses:

```
ip urlfilter max-resp-pak 150
```

ip urlfilter server vendor

To configure a vendor server for URL filtering, use the **ip urlfilter server vendor** command in global configuration mode. To remove a server from your configuration, use the **no** form of this command.

ip urlfilter server vendor {**websense** | **n2h2**} *ip-address* [**port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*] [**outside**]

no **ip urlfilter server vendor** {**websense** | **n2h2**} *ip-address* [**port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*] [**outside**]

Syntax Description

websense	Websense server will be used.
n2h2	N2H2 server will be used.
ip-address	IP address of the vendor server.
port *port-number*	(Optional) Port number that the vendor server listens on. The default port number is 15868.
timeout *seconds*	(Optional) Length of time, in seconds, that the Cisco IOS firewall will wait for a response from the vendor server. The default timeout is 5 seconds.
retransmit *number*	(Optional) Number of times the Cisco IOS firewall will retransmit the request when a response does not arrive for the request. The default value is two times.
outside	(Optional) Vendor server will be deployed on the outside network.

Defaults

A vendor server is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(1.07)T	The optional keyword was added.

Usage Guidelines

Use the **ip urlfilter server vendor** command to configure a Websense or N2H2 server, which will interact with the Cisco IOS Firewall to filter HTTP requests on the basis of a specified policy—global filtering, user- or group-based filtering, keyword-based filtering, category-based filtering, or customized filtering.

If the firewall has not received a response from the vendor server within the time specified in the **timeout** *seconds* keyword and argument, the firewall will check the **retransmit** *number* keyword and argument configured for the vendor server. If the firewall *has not* exceeded the maximum retransmit tries allowed, it will resend the HTTP lookup request. If the firewall *has* exceeded the maximum retransmit tries allowed, it will delete the outstanding request from the queue and check the status of the allow mode value. The firewall will forward the request if the allow mode is on; otherwise, it will drop the request.

By default, URL lookup requests that are made to the vendor server contain non-natted client IP addresses because the vendor server is deployed on the inside network. The **outside** keyword allows the vendor server to be deployed on the outside network, thereby, allowing Cisco IOS software to send the natted IP address of the client in the URL lookup request.

Primary and Secondary Servers

When users configure multiple vendor servers, the firewall will use only one server at a time—the primary server; all other servers are called secondary servers. When the primary server becomes unavailable for any reason, it becomes a secondary server and one of the secondary servers becomes the primary server.

A firewall marks a primary server as down when sending a request to or receiving a response from the server fails. When a primary server goes down, the system will go to the beginning of the configured servers list and try to activate the first server on the list. If the first server on the list is unavailable, it will try the second server on the list; the system will keep trying to activate a server until it is successful or until it reaches the end of the server list. If the system reaches the end of the server list, it will set a flag indicating that all of the servers are down, and it will enter allow mode.

Examples

The following example shows how to configure the Websense server for URL filtering:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Related Commands

Command	Description
ip urlfilter allowmode	Turns on the default mode (allow mode) of the filtering algorithm.
ip urlfilter max-request	Sets the maximum number of outstanding requests that can exist at any given time.

ip urlfilter urlf-server-log

To enable the logging of system messages on the URL filtering server, use the **ip urlfilter urlf-server-log** command in global configuration mode. To disable the logging of system messages, use the **no** form of this command.

ip urlfilter urlf-server-log

no ip urlfilter urlf-server-log

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

Use the **ip urlfilter urlf-server-log** command to enable Cisco IOS to send a log request immediately after the URL lookup request. The firewall will not make a URL lookup request if the destination IP address is in the cache, but it will still make a log request to the server. (The log request contains the URL, host name, source IP address, and the destination IP address.) The server records the log request into its own log server so your can view this information as necessary.

Examples

The following example shows how to enable system message logging on the URL filter server:

```
ip urlfilter urlf-server-log
```

ip verify unicast reachable-via

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast reachable-via** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ip verify unicast reachable-via {**rx** | **any**} [**allow-default**] [**allow-self-ping**] [*list*]

no ip verify unicast

Syntax Description

list	(Optional) Specifies a numbered access control list (ACL) in the following ranges: • 1 to 99 (IP standard access list) • 100 to 199 (IP extended access list) • 1300 to 1999 (IP standard access list, expanded range) • 2000 to 2699 (IP extended access list, expanded range)
rx	The source is reachable through the interface on which the packet was received.
any	The source is reachable through any interface. Examines incoming packets only if the source address is in the Forwarding Information Base (FIB). This would be a tool for some DOS/DDOS attacks that used unallocated IPaddresses as the "spoofed" source.
allow-default	allow-default flag means allow the lookup to match the default route and use it for verification.
allow-self-ping	Allows a router to ping its own interface. When used, this keyword enables a denial-of-service (DoS) hole.

Defaults

Unicast RPF is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
11.1(CC), 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3
12.1(2)T	Added ACL support using the *list* argument. Added per-interface statistics on dropped or suppressed packets.
12.0 S	This command replaced the **ip verify unicast reverse-path** command, and the following keywords were added: **allow-default, allow-self-ping**, **rx**, and **any**.
12.2 T	Cisco IOS Release 12.0 S was integrated into Cisco IOS Release 12.2 T.
12.1 E	Cisco IOS Release 12.2 T was integrated into Cisco IOS Release 12.1 E.
12.2 S	Cisco IOS Release 12.1 E was integrated into Cisco IOS Release 12.2 S.

Usage Guidelines

Use the **ip verify unicast reachable-via** interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate DoS attacks on the basis of source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source address appears in the routing table and matches the interface on which the packet was received. This ability to "look backwards" is available only when Cisco Express Forwarding (CEF) is enabled on the router because the lookup relies on the presence of the FIB. CEF generates the FIB as part of its operation.

Note Unicast RPF is an input function and is applied only on the input interface of a router at the upstream end of a connection.

The Unicast Reverse Path Forwarding feature checks to see if any packet received at a router interface arrives on one of the best return paths to the source of the packet. The feature does this checking by doing a reverse lookup in the CEF table. If Unicast RPF does not find a reverse path for the packet, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast Reverse Path Forwarding command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to see if the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast Reverse Path Forwarding command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast Reverse Path Forwarding command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Note With Unicast RPF, all equal-cost "best" return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

To use Unicast RPF, enable CEF switching or distributed CEF (dCEF) switching in the router. There is no need to configure the input interface for CEF switching. As long as CEF is running on the router, individual interfaces can be configured with other switching modes.

Note It is very important for CEF to be configured globally in the router. Unicast RPF will not work without CEF.

Where to Use RPF in Your Network

Unicast RPF should not be used on interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, meaning that there are multiple routes to the source of a packet. Unicast RPF should be applied only where there is natural or configured symmetry.

For example, routers at the edge of the network of an Internet service provider (ISP) are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. Hence, it is not recommended that you apply Unicast RPF where there is a chance of asymmetric routing. It is simplest to place Unicast RPF only at the edge of a network or, for an ISP, at the customer edge of the network.

Exists-only or Loose Mode RPF

If source address is in the FIB, then the packet is passed. If the source is not in FIB, the packet is dropped.

The source address must be in the FIB and reachable through any interface on the router. The syntax used for this method is **ip verify unicast reachable-via any.**

Regardless of which interface the packet enters, this uRPF option is used on the ISP routers peered with other ISPs. Packets that have not been allocated on the Internet, yet which are used for spoofed source addresses, are dropped. Other packets that have an entry in the FIB are passed.

Strict Mode RPF

The source address must be in the FIB and reachable through the interface on which the packet was received. The syntax to accomplish this is **ip verify unicast reachable-via rx**.

allow-self-ping

The verification check to allow the router to ping its own interface. You must specify the **allow-self-ping** keyword in the command to enable a DoS hole.

Examples

The following example shows enabling the Unicast Reverse Path Forwarding feature on a serial interface:

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
interface serial 5/0/0
 ip verify unicast reverse-path
```

The following example uses a simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 209.165.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
ip cef distributed
!
interface Serial 5/0/0
 description Connection to Upstream ISP
 ip address 209.165.200.225 255.255.255.252
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reachable-via any
 ip access-group 111 in
 ip access-group 110 out
!
access-list 110 permit ip 209.165.202.128 0.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 0.0.0.0 any log
access-list 111 deny ip 127.0.0.0 0.255.255.255 any log
```

```
access-list 111 deny ip 10.0.0.0 0.255.255.255 any log
access-list 111 deny ip 172.16.0.0 0.15.255.255 any log
access-list 111 deny ip 192.168.0.0 0.0.255.255 any log
access-list 111 deny ip 209.165.202.128 0.0.0.31 any log
access-list 111 permit ip any any
```

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet 0 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet 0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.0
 ip verify unicast reachable-via rx 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny   ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny   ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log-input
access-list 197 deny ip 127.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 197 deny ip 192.168.0.0 0.0.255.255 any log-input
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor card.

ip verify unicast reverse-path

Note This command was replaced by the **ip verify unicast reachable-vi**a command effective with Cisco IOS Release 12.0 S.

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast reverse-path** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ip verify unicast reverse-path [*list*]

no ip verify unicast reverse-path [*list*]

Syntax Description

list	(Optional) Specifies a numbered access control list (ACL) in the following ranges: • 1 to 99 (IP standard access list) • 100 to 199 (IP extended access list) • 1300 to 1999 (IP standard access list, expanded range) • 2000 to 2699 (IP extended access list, expanded range)

Defaults

Unicast RPF is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
11.1(CC), 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3
12.1(2)T	Added ACL support using the *list* argument. Added per-interface statistics on dropped or suppressed packets.

Usage Guidelines

Use the **ip verify unicast reverse-path** interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source address appears in the routing table and matches the interface on which the packet was received. This “look backwards” ability is available only when Cisco Express Forwarding (CEF) is enabled on the router because the lookup relies on the presence of the Forwarding Information Base (FIB). CEF generates the FIB as part of its operation.

Note Unicast RPF is an input function and is applied only on the input interface of a router at the upstream end of a connection.

The Unicast Reverse Path Forwarding feature checks to see if any packet received at a router interface arrives on one of the best return paths to the source of the packet. The feature does this by doing a reverse lookup in the CEF table. If Unicast RPF does not find a reverse path for the packet, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast Reverse Path Forwarding command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to see if the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast Reverse Path Forwarding command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast Reverse Path Forwarding command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Note With Unicast RPF, all equal-cost “best” return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

To use Unicast RPF, enable CEF switching or distributed CEF (dCEF) switching in the router. There is no need to configure the input interface for CEF switching. As long as CEF is running on the router, individual interfaces can be configured with other switching modes.

Note It is very important for CEF to be configured globally in the router. Unicast RPF will not work without CEF.

Unicast RPF should not be used on interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, meaning that there are multiple routes to the source of a packet. Unicast RPF should be applied only where there is natural or configured symmetry.

For example, routers at the edge of the network of an Internet service provider (ISP) are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. Hence, it is not recommended that you apply Unicast RPF where there is a chance of asymmetric routing. It is simplest to place Unicast RPF only at the edge of a network or, for an ISP, at the customer edge of the network.

Examples

The following example shows enabling the Unicast Reverse Path Forwarding feature on a serial interface:

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
```

```
interface serial 5/0/0
 ip verify unicast reverse-path
```

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 209.165.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
ip cef distributed
!
interface Serial 5/0/0
 description Connection to Upstream ISP
 ip address 209.165.200.225 255.255.255.252
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reverse-path
 ip access-group 111 in
 ip access-group 110 out
!
access-list 110 permit ip 209.165.202.128 0.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 0.0.0.0 any log
access-list 111 deny ip 127.0.0.0 0.255.255.255 any log
access-list 111 deny ip 10.0.0.0 0.255.255.255 any log
access-list 111 deny ip 172.16.0.0 0.15.255.255 any log
access-list 111 deny ip 192.168.0.0 0.0.255.255 any log
access-list 111 deny ip 209.165.202.128 0.0.0.31 any log
access-list 111 permit ip any any
```

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet0 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.0
 ip verify unicast reverse-path 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny   ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny   ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log-input
access-list 197 deny ip 127.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 197 deny ip 192.168.0.0 0.0.255.255 any log-input
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor card.

ip virtual-reassembly

To enable virtual fragment reassembly (VFR) on an interface, use the **ip virtual-reassembly** command in interface configuration mode. To disable VFR on an interface, use the **no** form of this command.

ip virtual-reassembly [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**drop-fragments**]

no ip virtual-reassembly [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**drop-fragments**]

Syntax Description

max-reassemblies *number*	(Optional) Maximum number of IP datagrams that can be reassembled at any given time. Default value: 64. If the maximum value is reached, all fragments within the following fragment set will be dropped and an alert message will be logged to the syslog server.
max-fragments *number*	(Optional) Maximum number of fragments that are allowed per IP datagram (fragment set). Default value: 16. If an IP datagram that is being reassembled receives more than the maximum allowed fragments, the IP datagram will be dropped and an alert message will be logged to the syslog server.
timeout *seconds*	(Optional) Timeout value, in seconds, for an IP datagram that is being reassembled. Default value: 3 seconds. If an IP datagram does not receive all of the fragments within the specified time, the IP datagram (and all of its fragments) will be dropped.
drop-fragments	(Optional) Enables the VFR to drop all fragments that arrive on the configured interface. By default, this function is disabled.

Defaults

VFR is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

A buffer overflow attack can occur when an attacker continuously sends a large number of incomplete IP fragments, causing the firewall to lose time and memory while trying to reassemble the fake packets.

The **max-reassemblies** *number* option and the **max-fragments** *number* option allow you to configure maximum threshold values to avoid a buffer overflow attack and to control memory usage.

In addition to configuring the maximum threshold values, each IP datagram is associated with a managed timer. If the IP datagram does not receive all of the fragments within the specified time (which can be configured via the **timeout** *seconds* option), the timer will expire and the IP datagram (and all of its fragments) will be dropped.

Automatically Enabling or Disabling VFR

VFR is designed to work with any feature that requires fragment reassembly (such as Cisco IOS Firewall and NAT). Currently, NAT enables and disables VFR internally; that is, when NAT is enabled on an interface, VFR is automatically enabled on that interface.

If more than one feature attempts to automatically enable VFR on an interface, VFR will maintain a reference count to keep track of the number of features that have enabled VFR. When the reference count is reduced to zero, VFR is automatically disabled

Examples

The following example shows how to configure VFR on interfaces ethernet2/1, ethernet2/2, and serial3/0 to facilitate the firewall that is enabled in the outbound direction on interface serial3/0. In this example, the firewall rules that specify the list of LAN1 and LAN2 originating protocols (FTP, HTTP and SMTP) are to be inspected.

```
ip inspect name INTERNET-FW ftp
ip inspect name INTERNET-FW http
ip inspect name INTERNET-FW smtp!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Ethernet2/0
 ip address 9.4.21.9 255.255.0.0
 no ip proxy-arp
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet2/1
 description LAN1
 ip address 14.0.0.2 255.255.255.0
 ip virtual-reassembly
 duplex half
!
interface Ethernet2/2
 description LAN2
 ip address 15.0.0.2 255.255.255.0
 ip virtual-reassembly
 duplex half
!
interface Ethernet2/3
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
!
interface Serial3/0
 description Internet
 ip unnumbered Loopback0
 encapsulation ppp
 ip access-group 102 in
 ip inspect INTERNET-FW out
 ip virtual-reassembly
 serial restart-delay 0
```

Related Commands

Command	Description
show ip virtual-reassembly	Displays the configuration and statistical information of the VFR on a given interface.

ip vrf forwarding (server-group)

To configure the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an authentication, authorization, and accounting (AAA) RADIUS or TACACS+ server group, use the **ip vrf forwarding** command in server-group configuration mode. To enable server groups to use the global (default) routing table, use the **no** form of this command.

ip vrf forwarding *vrf-name*

no ip vrf forwarding *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Defaults

Server groups use the global routing table.

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(2)DD	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(7)T	Functionality was added for TACACS+ servers.

Usage Guidelines

Use the **ip vrf forwarding** command to specify a VRF for a AAA RADIUS or TACACS+ server group. This command enables dial users to utilize AAA servers in different routing domains.

Examples

The following example shows how to configure the VRF user to reference the RADIUS server in a different VRF server group:

```
aaa group server radius sg_global
 server-private 172.16.0.0 timeout 5 retransmit 3
!
aaa group server radius sg_water
 server-private 10.10.0.0 timeout 5 retransmit 3 key water
 ip vrf forwarding water
```

The following example shows how to configure the VRF user to reference the TACACS+ server in the server group tacacs1:

```
aaa group server tacacs+ tacacs1
    server-private 1.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0

  ip vrf cisco
```

```
 rd 100:1

interface Loopback0
 ip address 10.0.0.2 255.0.0.0
 ip vrf forwarding cisco
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
ip tacacs source-interface	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.
server-private	Configures the IP address of the private RADIUS server for the group server.

isakmp authorization list

To configure an Internet Key Exchange (IKE) shared secret using the authentication, authorization, and accounting (AAA) server in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **isakmp authorization list** command in ISAKMP profile configuration mode. To disable the shared secret, use the **no** form of this command.

isakmp authorization list *list-name*

no isakmp authorization list *list-name*

Syntax Description

list-name	AAA authorization list used for configuration mode attributes or preshared keys for aggresive mode.

Defaults

No default behaviors or values

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command allows you to retrieve a shared secret from an AAA server.

Examples

The following example shows that an IKE shared secret is configured using an AAA server on a router:

```
crypto isakmp profile vpnprofile
 isakmp authorization list ikessaaalist
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

issuer-name

To specify the distinguished name (DN) as the certification authority (CA) issuer name for the certificate server, use the **issuer-name** command in certificate server configuration mode. To clear the issuer name and return to the default, use the **no** form of this command.

issuer-name *DN-string*

no issuer-name *DN-string*

Syntax Description

DN-string	Name of the DN string.

Defaults

If the issuer name is not configured, **CN** = *cs-label*

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The DN-string value cannot be changed after the certificate server generates its signed certificate.

Examples

The following example shows how to define an issuer name for the certificate server “mycertserver”:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# database level minimal
Router(cs-server)# database url nvram:
Router(cs-server)# issuer-name CN = ipsec_cs,L = My Town,C = US
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

keepalive (isakmp profile)

To allow the gateway to send dead peer detection (DPD) messages to the peer, use the **keepalive** command in Internet Security Association Key Management Protocol (ISAKMP) profile configuration mode. To return to the default, use the **no** form of this command.

keepalive *seconds* **retry** *retry-seconds*

no keepalive *seconds* **retry** *retry-seconds*

Syntax Description

seconds	Number of seconds between DPD messages. The range is from 10 to 3600 seconds.
retry *retry-seconds*	Number of seconds between retries if DPD message fails. The range is from 2 to 60 seconds.

Defaults

If this command is not configured, a DPD message is not sent to the client.

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use this command to enable the gateway (instead of the client) to send DPD messages to the client. Internet Key Exchange (IKE) DPD is a new keepalive scheme that sends messages to let the router know that the client is still connected.

Examples

The following example shows that DPD messages have been configured to be sent every 60 seconds and every 5 seconds between retries if the peer does not respond:

```
crypto isakmp profile vpnprofile
 keepalive 60 retry 5
```

kerberos clients mandatory

To cause the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server, use the **kerberos clients mandatory** command in global configuration mode. To make Kerberos optional, use the **no** form of this command.

kerberos clients mandatory

no kerberos clients mandatory

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If this command is not configured and the user has Kerberos credentials stored locally, the **rsh**, **rcp**, **rlogin**, and **telnet** commands attempt to negotiate the Kerberos protocol with the remote server and will use the non-Kerberized protocols if unsuccessful.

If this command is not configured and the user has no Kerberos credentials, the standard protocols for **rcp** and **rsh** are used to negotiate.

Examples

The following example causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server:

```
kerberos clients mandatory
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
kerberos credentials forward	Forces all network application clients on the router to forward the Kerberos credentials of users upon successful Kerberos authentication.
rlogin	Logs in to a UNIX host using rlogin.
rsh	Executes a command remotely on a remote rsh host.
telnet	Logs in to a host that supports Telnet.

kerberos credentials forward

To force all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication, use the **kerberos credentials forward** command in global configuration mode. To turn off forwarding of Kerberos credentials, use the **no** form of this command.

kerberos credentials forward

no kerberos credentials forward

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Enable credentials forwarding to have users' ticket granting tickets (TGTs) forwarded to the host on which they authenticate. In this way, users can connect to multiple hosts in the Kerberos realm without running the KINIT program each time they need to get a TGT.

Examples

The following example forces all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication:

```
kerberos credentials forward
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
rlogin	Logs in to a UNIX host using rlogin.
rsh	Executes a command remotely on a remote rsh host.
telnet	Logs in to a host that supports Telnet.

kerberos instance map

To map Kerberos instances to Cisco IOS privilege levels, use the **kerberos instance map** command in global configuration mode. To remove a Kerberos instance map, use the **no** form of this command.

kerberos instance map *instance privilege-level*

no kerberos instance map *instance*

Syntax Description

instance	Name of a Kerberos instance.
privilege-level	The privilege level at which a user is set if the user's Kerberos principal contains the matching Kerberos instance. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges.

Defaults

Privilege level 1

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to create user instances with access to administrative commands.

Examples

The following example sets the privilege level to 15 for authenticated Kerberos users with the *admin* instance in Kerberos realm:

```
kerberos instance map admin 15
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

kerberos local-realm

To specify the Kerberos realm in which the router is located, use the **kerberos local-realm** command in global configuration mode. To remove the specified Kerberos realm from this router, use the **no** form of this command.

kerberos local-realm *kerberos-realm*

no kerberos local-realm

Syntax Description

kerberos-realm	The name of the default Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The router can be located in more than one realm at a time. However, there can only be one instance of Kerberos local-realm. The realm specified with this command is the default realm.

Examples

The following example specify the Kerberos realm in which the router is located as EXAMPLE.COM:

```
kerberos local-realm EXAMPLE.COM
```

Related Commands

Command	Description
kerberos preauth	Specifies a preauthentication method to use to communicate with the KDC.
kerberos realm	Maps a host name or DNS domain to a Kerberos realm.
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.

kerberos preauth

To specify a preauthentication method to use to communicate with the key distribution center (KDC), use the **kerberos preauth** command in global configuration mode. To disable Kerberos preauthentication, use the **no** form of this command.

kerberos preauth [**encrypted-unix-timestamp** | **encrypted-kerberos-timestamp** | **none**]

no kerberos preauth

Syntax Description

encrypted-unix-timestamp	(Optional) Use an encrypted UNIX timestamp as a quick authentication method when communicating with the KDC.
encrypted-kerberos-timestamp	(Optional) Use the RFC1510 kerberos timestamp as a quick authentication method when communicating with the KDC.
none	(Optional) Do not use Kerberos preauthentication.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

It is more secure to use a preauthentication for communications with the KDC. However, communication with the KDC will fail if the KDC does not support this particular version of **kerberos preauth.** If that happens, turn off the preauthentication with the **none** option.

The **no** form of this command is equivalent to using the **none** keyword.

Examples

The following example enables Kerberos preauthentication:

```
kerberos preauth encrypted-unix-timestamp
```

The following example disables Kerberos preauthentication:

```
kerberos preauth none
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.

Command	Description
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.

kerberos realm

To map a host name or Domain Name System (DNS) domain to a Kerberos realm, use the **kerberos realm** command in global configuration mode. To remove a Kerberos realm map, use the **no** form of this command.

kerberos realm {*dns-domain* | *host*} *kerberos-realm*

no kerberos realm {*dns-domain* | *host*} *kerberos-realm*

Syntax Description

dns-domain	Name of a DNS domain or host.
host	Name of a DNS host.
kerberos-realm	Name of the Kerberos realm to which the specified domain or host belongs.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

DNS domains are specified with a leading dot (.) character; host names cannot begin with a dot (.) character. There can be multiple entries of this line.

A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters. The router can be located in more than one realm at a time. Kerberos realm names must be in all uppercase characters.

Examples

The following example maps the domain name “example.com” to the Kerberos realm, EXAMPLE.COM:

```
kerberos realm .example.com EXAMPLE.COM
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

kerberos server

To specify the location of the Kerberos server for a given Kerberos realm, use the **kerberos server** command in global configuration mode. To remove a Kerberos server for a specified Kerberos realm, use the **no** form of this command.

kerberos server *kerberos-realm* {*host-name* | *ip-address*} [*port-number*]

no kerberos server *kerberos-realm* {*host-name* | *ip-address*}

Syntax Description

kerberos-realm	Name of the Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase letters.
host-name	Name of the host functioning as a Kerberos server for the specified Kerberos realm (translated into an IP address at the time of entry).
ip-address	IP address of the host functioning as the Kerberos server for the specified Kerberos realm.
port-number	(Optional) Port that the key distribution center (KDC) monitors (defaults to 88).

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use the **kerberos server** command to specify the location of the Kerberos server for a given realm.

Examples

The following example specifies 192.168.47.66 as the Kerberos server for the Kerberos realm EXAMPLE.COM:

```
kerberos server EXAMPLE.COM 192.168.47.66
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.
kerberos realm	Maps a host name or DNS domain to a Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

kerberos srvtab entry

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the **kerberos srvtab entry** command in global configuration mode. To remove a SRVTAB entry from the router's configuration, use the **no** form of this command.

kerberos srvtab entry *kerberos-principal principal-type timestamp key-version number key-type key-length encrypted-keytab*

no kerberos srvtab entry *kerberos-principal principal-type*

Syntax Description

kerberos-principal	A service on the router.
principal-type	Version of the Kerberos SRVTAB.
timestamp	Number representing the date and time the SRVTAB entry was created.
key-version number	Version of the encryption key format.
key-type	Type of encryption used.
key-length	Length, in bytes, of the encryption key.
encrypted-keytab	Secret key the router shares with the key distribution center (KDC). It is encrypted with the private Data Encryption Standard (DES) key (if available) when you write out your configuration.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When you use the **kerberos srvtab remote** command to copy the SRVTAB file from a remote host (generally the KDC), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry** format. The key for each SRVTAB entry is encrypted with a private DES key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** router configuration command to write the router's running configuration to NVRAM.

If you reload a configuration, with a SRVTAB encrypted with a private DES key, on to a router that does not have a private DES key defined, the router displays a message informing you that the SRVTAB entry has been corrupted, and discards the entry.

If you change the private DES key and reload an old version of the router's configuration that contains SRVTAB entries encrypted with the old private DES keys, the router will restore your Kerberos SRVTAB entries, but the SRVTAB keys will be corrupted. In this case, you must delete your old Kerberos SRVTAB entries and reload your Kerberos SRVTABs on to the router using the **kerberos srvtab remote** command.

Although you can configure **kerberos srvtab entry** on the router manually, generally you would not do this because the keytab is encrypted automatically by the router when you copy the SRVTAB using the **kerberos srvtab remote** command.

Examples

In the following example, host/new-router.example.com@EXAMPLE.COM is the host, 0 is the type, 817680774 is the timestamp, 1 is the version of the key, 1 indicates the DES is the encryption type, 8 is the number of bytes, and .cCN.YoU.okK is the encrypted key:

```
kerberos srvtab entry host/new-router.example.com@EXAMPLE.COM 0 817680774 1 1 8
.cCN.YoU.okK
```

Related Commands

Command	Description
kerberos srvtab remote	Retrieves a krb5 SRVTAB file from the specified host.
key config-key	Defines a private DES key for the router.

kerberos srvtab remote

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the **kerberos srvtab remote** command in global configuration mode.

kerberos srvtab remote {boot_device:*URL*}

Syntax Description

URL	Machine that has the Kerberos SRVTAB file.
ip-address	IP address of the machine that has the Kerberos SRVTAB file.
filename	Name of the SRVTAB file.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When you use the **kerberos srvtab remote** command to copy the SRVTAB file from the remote host (generally the key distribution center [KDC]), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry** format. The key for each SRVTAB entry is encrypted with the private Data Encryption Standard (DES) key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** configuration command to write the router's running configuration to NVRAM.

Examples

The following example copies the SRVTAB file residing on b1.example.com to a router named s1.example.com:

```
kerberos srvtab remote tftp://b1.example.com/s1.example.com-new-srvtab
```

Related Commands

Command	Description
kerberos srvtab entry	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.
key config-key	Defines a private DES key for the router.

key (isakmp-group)

To specify the Internet Key Exchange (IKE) preshared key for group policy attribute definition, use the **key** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove a preshared key, use the **no** form of this command.

key *name*

no key *name*

Syntax Description

name	IKE preshared key that matches the password entered on the client. **Note** This value must match the "password" field that is defined in the Cisco VPN Client 3.x configuration GUI.

Defaults

No default behavior or values.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **key** command to specify the IKE preshared key when defining group policy information for Mode Configuration push. (It follows the **crypto isakmp client configuration group** command.) You *must* configure this command if the client identifies itself to the router with a preshared key. (You do not have to enable this command if the client uses a certificate for identification.)

Examples

The following example shows how to specify the preshared key "cisco":

```
crypto isakmp client configuration group default
  key cisco
  dns 2.2.2.2 2.3.2.3
  pool dog
  acl 199
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

key config-key

To define a private DES key for the router, use the **key config-key** command in global configuration mode. To delete a private Data Encryption Standard (DES) key from the router, use the **no** form of this command.

key config-key 1 *string*

no key config-key 1 *string*

Syntax Description

1	Key number. This number is always 1.
string	Private DES key (can be up to eight alphanumeric characters).

Defaults

No DES-key defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was released.

Usage Guidelines

This command defines a private DES key for the router that will not show up in the router configuration. This private DES key can be used to DES-encrypt certain parts of the router's configuration.

Caution The private DES key is unrecoverable. If you encrypt part of your configuration with the private DES key and lose or forget the key, you will not be able to recover the encrypted data.

Examples

The following example sets *keyxx* as the private DES key on the router:

```
key config-key 1 keyxx
```

Related Commands

Command	Description
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

key config-key password-encryption

To store a type 6 encryption key in private NVRAM, use the **key config-key password-encryption** command in global configuration mode. To disable the encryption, use the **no** form of this command.

key config-key password-encryption [*text***]**

no key config-key password-encryption [*text***]**

Syntax Description

text	(Optional) **Password or master key**.

Note It is recommended that you do not use the *text* argument but instead use interactive mode (using the enter key after you enter the **key config-key password-encryption** command) so that the preshared key will not be printed anywhere and, therefore, cannot be seen.

Defaults

No type 6 password encryption

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

You can securely store plain text passwords in type 6 format in NVRAM using a command-line interface (CLI). Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encryption** command with the **password encryption aes** command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) configured using the **key config-key password-encryption** command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the **password encryption aes** command without configuring the **key config-key password-encryption** command, the following message is printed at startup or during any nonvolatile generation (NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands have been configured:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

Changing a Password

If the password (master key) is changed, or reencrypted, using the **key config-key password-encryption** command), the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

Deleting a Password

If the master key that was configured using the **key config-key password-encryption** command is deleted from the system, a warning is printed (and a confirm prompt is issued) that states that all type 6 passwords will become useless. As a security measure, after the passwords have been encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be reencrypted as explained in the previous paragraph.

Caution If the password configured using the **key config-key password-encryption** command is lost, it cannot be recovered. The password should be stored in a safe location.

Unconfiguring Password Encryption

If you later unconfigure password encryption using the **no password encryption aes** command, all existing type 6 passwords are left unchanged, and as long as the password (master key) that was configured using the **key config-key password-encryption** command exists, the type 6 passwords will be decrypted as and when required by the application.

Storing Passwords

Because no one can "read" the password (configured using the **key config-key password-encryption** command), there is no way that the password can be retrieved from the router. Existing management stations cannot "know" what it is unless the stations are enhanced to include this key somewhere, in which case the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the **key config-key password-encryption** command). The password can be manually added to the stored configuration but is not recommended because adding the password manually allows anyone to decrypt all passwords in that configuration.

Configuring New or Unknown Passwords

If you enter or cut and paste cipher text that does not match the master key, or if there is no master key, the cipher text is accepted or saved, but an alert message is printed. The alert message is as follows:

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

If a new master key is configured, all the plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or unknown, you have the option of deleting the master key using the **no key config-key password-encryption** command. Deleting the master key using the **no key config-key password-encryption** command causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

Examples

The following example shows that a type 6 encryption key is to be stored in NVRAM:

```
Router (config)# key config-key password-encryption
```

Related Commands

Command	Description
password encryption aes	Enables a type 6 encrypted preshared key.
password logging	Provides a log of debugging output for a type 6 password operation.

keyring

To configure a keyring with an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **keyring** command in ISAKMP profile configuration mode. To remove the keyring from the ISAKMP profile, use the **no** form of this command.

keyring *keyring-name*

no keyring *keyring-name*

Syntax Description

keyring-name	The keyring name, which must match the keyring name that was defined in the global configuration.

Defaults

If this command is not used, the ISAKMP profile uses the keys defined in the global configuration.

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The ISAKMP profile successfully completes authentication of peers if the peer keys are defined in the keyring that is attached to this profile. If no keyring is defined in the profile, the global keys that were defined in the global configuration are used.

Examples

The following example shows that “vpnkeyring” is configured as the keyring name:

```
crypto isakmp profile vpnprofile
 keyring vpnkeyring
```

key-string (IKE)

To specify the Rivest, Shamir, and Adelman (RSA) public key of the remote peer, use the **key-string** command in public key configuration mode. To remove the RSA public key, use the **no** form of this command.

key-string *key-string*

no key-string *key-string*

Syntax Description

key-string	Enter the key in hexadecimal format. While entering the key data, you can press Return to continue entering data.

Defaults

No default behavior or values

Command Modes

Public key configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Before using this command, you must enter the **rsa-pubkey** command in the crypto keyring mode.

If possible, to avoid mistakes, you should cut and paste the key data (instead of attempting to type in the data).

To complete the command, you must return to the global configuration mode by typing **quit** at the config-pubkey prompt.

Examples

The following example manually specifies the RSA public keys of an IP Security (IPSec) peer:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
crypto keyring	Defines a crypto keyring.
rsa-pubkey	Defines the RSA public key to be used for encryption or signatures during IKE authentication.
show crypto keyring	Displays keyrings on your router.

lifetime (certificate server)

To specify the lifetime of the certification authority (CA) or a certificate, use the **lifetime** command in certificate server configuration mode. To return to the default lifetime values, use the **no** form of this command.

lifetime {**ca-certificate** | **certificate**} *time*

no lifetime {**ca-certificate** | **certificate**} *time*

Syntax Description

ca-certificate	Lifetime is for the CA certificate of the certificate server.
certificate	Lifetime is for the certificate of the certificate server. The maximum certificate lifetime is one month less than the expiration date of the CA certificate's lifetime.
time	Lifetime value in days. Valid values range from 1 day to 1825 days. All certificates are valid on the date that they are issued.

Defaults

The default CA certificate lifetime is 3 years.

The default certificate lifetime is 1 year.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

After you enable a certificate server via the **crypto pki server** command, use the **lifetime** command if you wish to specify lifetime values other than the default values for the CA certificate and the certificate of the certificate server.

After the certificate generates its signed certificate, the lifetime cannot be changed.

Examples

The following example shows how to set the lifetime value for the CA to 30 days:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# lifetime ca certificate 30
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

lifetime (IKE policy)

To specify the lifetime of an Internet Key Exchange (IKE) security association (SA), use the **lifetime** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. To reset the SA lifetime to the default value, use the **no** form of this command.

lifetime *seconds*

no lifetime

Syntax Description

seconds	Number of many seconds for each each SA should exist before expiring. Use an integer from 60 to 86,400 seconds, which is the default value.

Defaults

86,400 seconds (one day)

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command to specify how long an IKE SA exists before expiring.

When IKE begins negotiations, the first thing it does is agree upon the security parameters for its own session. The agreed-upon parameters are then referenced by an SA at each peer. The SA is retained by each peer until the SA's lifetime expires. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec SAs. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec SAs. New IPSec SAs are negotiated before current IPSec SAs expire.

So, to save setup time for IPSec, configure a longer IKE SA lifetime. However, shorter lifetimes limit the exposure to attackers of this SA. The longer an SA is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.

Note that when your local peer initiates an IKE negotiation between itself and a remote peer, an IKE policy can be selected only if the lifetime of the remote peer's policy is shorter than or equal to the lifetime of the local peer's policy. Then, if the lifetimes are not equal, the shorter lifetime will be selected. To restate this behavior: If the two peer's policies' lifetimes are not the same, the initiating peer's lifetime must be longer and the responding peer's lifetime must be shorter, and the shorter lifetime will be used.

Examples

The following example configures an IKE policy with a security association lifetime of 600 seconds (10 minutes), and all other parameters are set to the defaults:

```
crypto isakmp policy 15
 lifetime 600
 exit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
show crypto isakmp policy	Displays the parameters for each IKE policy.

lifetime crl

To define the lifetime of the certificate revocation list (CRL) that is used by the certificate server, use the **lifetime crl** command in certificate server configuration mode. To return to the default value of 1 week, use the **no** form of this command.

lifetime crl *time*

no lifetime crl *time*

Syntax Description

time	Lifetime value, in hours, of the CRL. Maximum lifetime value is 336 hours (2 weeks). The default value is 168 hours (1 week).

Defaults

168 hours (1 week)

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

After you create a certificate server via the **crypto pki server** command, use the **lifetime crl** command if you want to specify a value other than the default value for the CRL. The lifetime value is added to the CRL when the CRL is created.

The CRL is written to the specified database location as *ca-label*.crl.

Examples

The following example shows how to set the lifetime value for the CRL to 24 hours:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# lifetime crl 24
```

Related Commands

Command	Description
cdp-url	Specifies that CDP should be used in the certificates that are issued by the certificate server.
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.

lifetime enrollment-request

To specify how long an enrollment request should stay in the enrollment database, use the **lifetime enrollment-request** command in certificate server configuration mode. To return to the default value of 1 week, use the **no** form of this command.

lifetime enrollment-request *time*

no lifetime enrollment-request

Syntax Description

time	Lifetime value, in hours, of an enrollment request. The maximum lifetime value is 1000 hours. The default value is 168 hours (1 week).

Defaults

Lifetime value default is 168 hours.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

After the certificate server receives an enrollment request, it can leave the request in pending, reject it, or grant it. The request is left in the Enrollment Request Database for the lifetime of the enrollment request until the client polls the certificate server for the result of the request.

Examples

The following example shows how to set the lifetime value for the enrollment request to 24 hours:

```
Router (config)# crypto pki server mycs
Router (cs-server)# lifetime enrollment-request 24
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server.
crypto pki server grant	Grants all or certain SCEP requests.
crypto pki server remove	Removes enrollment requests that are in the certificate server Enrollment Request Database.

li-view

To initialize a lawful intercept view, use the **li-view** command in global configuration mode.

li-view *li-password* **user** *username* **password** *password*

Syntax Description

li-password	Associates the lawful interface view with a password. The password can contain any number of alphanumeric characters. **Note** The password is case sensitive.
user *username*	User who can access the lawful intercept view.
password *password*	Associates a password with the specified **user** *username* option; that is, the user must provide the specified password to access the view.

Defaults

A lawful intercept view cannot be accessed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Like a command-line interface (CLI) view, a lawful intercept view restricts access to specified commands and configuration information. Specifically, a lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of simple network management protocol (SNMP) commands that stores information about calls and users.

Commands available in lawful intercept view belong to one of the following categories:

- Lawful intercept commands that should not be made available to any other view or privilege level.
- CLI that are useful for lawful intercept users but do not need to be excluded from other views or privilege levels.

Note Only a system administrator or a level 15 privilege user can initialize a lawful intercept view.

Examples

The following example shows how to configure a lawful intercept view, add users to the view, and verify the users that were added to the view:

```
!Initialize the LI-View.
Router(config-view)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config-view)# end

! Enter the LI-View; that is, check to see what commands are available within the view.
Router# enable view li-view
```

```
Password:

Router#
00:22:57:%PARSER-6-VIEW_SWITCH:successfully set to view 'li-view'.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view li-view
Router(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name      ===This option only resides in LI View.
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views

Router(config-view)#

! NOTE:LI View configurations are never shown as part of 'running-configuration'.

! Configure LI Users.
Router(config)# username lawful-intercept li-user1 password li-user1pass
Router(config)# username lawful-intercept li-user2 password li-user2pass

! Displaying LI User information.
Router# show users lawful-intercept

li_admin
li-user1
li-user2
Router#
```

Related Commands

Command	Description
show users	Displays information about the active lines on the router.
username	Establishes a username-based authentication system.

login authentication

To enable authentication, authorization, and accounting (AAA) authentication for logins, use the **login authentication** command in line configuration mode. To return to the default specified by the **aaa authentication login** command, use the **no** form of this command.

login authentication {**default** | *list-name*}

no login authentication {**default** | *list-name*}

Syntax Description

default	Uses the default list created with the **aaa authentication login** command.
list-name	Uses the indicated list created with the **aaa authentication login** command.

Defaults

Uses the default set with **aaa authentication login**.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command is a per-line command used with AAA that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line).

Caution If you use a *list-name* value that was not configured with the **aaa authentication login** command, you will disable login on this line.

Entering the **no** version of **login authentication** has the same effect as entering the command with the **default** keyword.

Before issuing this command, create a list of authentication processes by using the global configuration **aaa authentication login** command.

Examples

The following example specifies that the default AAA authentication is to be used on line 4:

```
line 4
 login authentication default
```

The following example specifies that the AAA authentication list called *list1* is to be used on line 7:

```
line 7
 login authentication list1
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.

login block-for

To configure your Cisco IOS device for login parameters that help provide denial-of-service (DoS) detection, use the **login block-for** command in global configuration mode. To disable the specified login parameters and return to the default functionality, use the **no** form of this command.

login block-for *seconds* **attempts** *tries* **within** *seconds*

no login block-for

Syntax Description

seconds	Duration of time in which login attempts are denied (also known as a quiet period) by the Cisco IOS device. Valid values range from 1 to 65535 (18 hours) seconds.
attempts *tries*	Maximum number of failed login attempts that triggers the quiet period. Valid values range from 1 to 65535 tries.
within *seconds*	Duration of time in which the allowed number of failed login attempts must be made before the quiet period is triggered. Valid values range from 1 to 65535 (18 hours) seconds.

Defaults

No login parameters are defined.

A quiet period is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25).

Usage Guidelines

If the specified number of connection attempts (via the **attempts** *tries* option) fail within a specified time (via the **within** *seconds* option), the Cisco IOS device will not accept any additional login attempts for a specified period of time (via the *seconds* argument).

All login parameters are disabled by default. You must issue the **login block-for** command, which enables default login functionality, before using any other login commands. After the **login block-for** command is enabled, the following defaults are enforced:

- A default login delay of 1 second
- All login attempts made via Telnet, secure shell (SSH), and HTTP are denied during the quiet period; that is, no access control lists (ACLs) are exempt from the login period until the **login quiet-mode access-class** command is issued.

System Logging Messages

The following logging message is generated after the router switches to quiet mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still timeleft for watching failures is 158 seconds,
[user:sfd] [Source:10.4.2.11] [localport:23] [Reason:Invalid login], [ACL:22] at 16:17:23
UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF, because block period timed out at
16:22:23 UTC Wed Feb 26 2003
```

Examples

The following example shows how to configure your router to block all login requests for 100 seconds if 15 failed login attempts are exceeded within 100 seconds. Thereafter, the **show login** command is issued to verify the login settings.

```
Router(config)# login block-for 100 attempts 15 within 100
Router(config)# exit
Router# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.

Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.

Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5
```

The following example shows how to disable login paramters. Thereafter, the **show login** command is issued to verify that login paramters are no longer configured.

```
Router(config)# no login block-for
Router(config)# exit
Router# show login

No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps

Router NOT enabled to watch for login Attacks
```

Related Commands

Command	Description
login delay	Configures a uniform delay between successive login attempts.
login on-failure	Generates system logging messages for failed login attempts.
login on-success	Generates system logging messages for successful login attempts.
login quiet-mode access-class	Specifies an ACL that is to be applied to the router when it switches to quiet mode.
show login	Displays login parameters.

login delay

To configure a uniform delay between successive login attempts, use the **login delay** command in global configuration mode. To return to the default functionality (which is a 1 second delay), use the **no** form of this command.

login delay *seconds*

no login delay

Syntax Description

seconds	Number of seconds between each login attempt. Valid values range from 1 to 10 seconds.

Defaults

If this command is not enabled, a login delay of 1 second is automatically enforced.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

A Cisco IOS device can accept connections (such as Telnet, secure shell (SSH), and HTTP) as fast as they can be processed. The **login delay** command introduces a uniform delay between successive login attempts. (The delay occurs for all login attempts—failed or successful attempts.) Thus, user users can better secure their Cisco IOS device from dictionary attacks, which are an attempt to gain username and password access to your device.

Although the **login delay** command allows users to configure a specific a delay, a uniform delay of 1 second is enabled if the **auto secure** command is issued. After the **auto secure** command is enabled, the autosecure dialog prompts users for login parameters; if login parameters have already been configured, the autosecure dialog will retain the specified values.

Examples

The following example shows how to configure your router to issue a delay of 90 seconds between each successive login attempt:

```
Router(config)# login delay 90
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
show login	Displays login parameters.

login on-failure

To generate logging messages for failed login attempts, use the **login on-failure** command in global configuration mode. To disable logging messages, use the **no** form of this command.

login on-failure log [**every** *login*]

no login on-failure log [**every** *login*]

Syntax Description

log	Logging messages are generated.
every *login*	(Optional) Number of failed login attempts that must occur before a logging message is generated; that is, a logging message is not generated for every failed login attempt. The default value is one attempt. Valid values range from 1 to 65535 attempts.

Defaults

Logging messages are not generated.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

Logging messages allow users to receive notice for every failed login attempt that is made to their device.

This functionality is automatically enabled when the **auto secure** command is issued.

Note Currently, only logging messages can be generated for login-related events. Support for simple network management protocol (SNMP) traps will be added in a later release.

Examples

The following example shows how to enable logging messages for every fifth failed login attempt:

```
Router(config)# login on-failure log every 5
```

The following logging message is generated upon a failed login request:

```
00:03:34:%SEC_LOGIN-4-LOGIN_FAILED:Login failed [user:sdfs] [Source:10.4.2.11]
[localport:23] [Reason:Invalid login] at 20:54:42 UTC Fri Feb 28 2003
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
login on-success	Generates system logging messages for successful login attempts.
show login	Displays login parameters.

login on-success

To generate logging messages for successful login attempts, use the **login on-success** command in global configuration mode. To disable logging messages, use the **no** form of this command.

login on-success log [**every** *login*]

no login on-success log [**every** *login*]

Syntax Description

log	Logging messages are generated.
every *login*	(Optional) Number of failed login attempts that must occur before a logging message is generated; that is, a logging message is not generated for every failed login attempt. The default value is one attempt. Valid values range from 1 to 65535 attempts.

Defaults

Logging messages are not generated.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

Logging messages allow users to receive notice for every successful login that is made to their device.

Note Currently, only logging messages can be generated for login-related events. Support for simple network management protocol (SNMP) traps will be added in a later release.

Examples

The following example shows how to enable logging messages for every fifth successful login attempt:

```
Router(config)# login on-success log every 5
```

The following logging message is generated upon a successful login request:

```
00:04:32:%SEC_LOGIN-5-LOGIN_SUCCESS:Login Success [user:test] [Source:10.4.2.11]
[localport:23] at 20:55:40 UTC Fri Feb 28 2003
```

Related Commands

Command	Description
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.

Command	Description
login on-failure	Generates system logging messages for failed login attempts.
show login	Displays login parameters.

login quiet-mode access-class

To specify an access control list (ACL) that is to be applied to the router when the router switches to quiet mode, use the **login quiet-mode access-class** command in global configuration mode. To remove this ACL and allow the router to deny all login attempts, use the **no** form of this command.

login quiet-mode access-class {*acl-name* | *acl-number*}

no login quiet-mode access-class {*acl-name* | *acl-number*}

Syntax Description

acl-name	Named ACL that is to be enforced during quiet mode.
acl-number	Numbered (standard or extended) ACL that is to be enforced during quiet mode.

Defaults

All login attempts via Telnet, secure shell (SSH), and HTTP are denied.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

Before using this command, you must issue the **login block-for** command, which allows you to specify the necessary parameters to enable a quiet period.

Use the **login quiet-mode access-class** command to selectively allow hosts on the basis of a specified ACL. You may use this command to grant an active client or list of clients an infinite number of failed attempts that are not counted by the router; that is, the active clients are placed on a "safe list" that allows them access to the router despite a quiet period.

System Logging Messages

The following logging message is generated after the router switches to quiet mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still timeleft for watching failures is 158 seconds,
[user:sfd] [Source:10.4.2.11] [localport:23] [Reason:Invalid login], [ACL:22] at 16:17:23
UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF, because block period timed out at
16:22:23 UTC Wed Feb 26 2003
```

Examples

The following example shows how to configure your router to accept hosts only from the ACL "myacl" during the next quiet period:

```
Router(config)# login quiet-mode access-class myacl
```

Related Commands

Command	Description
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
show login	Displays login parameters.

mac-address (RITE)

To specify the Ethernet address of the destination host, use the **mac-address** command in router IP traffic export (RITE) configuration mode. To change the MAC address of the destination host, use the **no** form of this command.

mac-address *H.H.H*

no mac-address *H.H.H*

Syntax Description

H.H.H	48-bit MAC address.

Defaults

A destination host is not known.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

The **mac-address** command, which is used to specify the destination host that is receiving the exported traffic, is part of suite of RITE configuration mode commands that are used to control various attributes for both incoming and outgoing IP traffic export.

The **ip traffic-export profile** command allows you to begin a profile that can be configured to export IP packets as they arrive or leave a selected router ingress interface. A designated egress interface exports the captured IP packets out of the router. Thus, the router can export unaltered IP packets to a directly connected device.

Examples

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the access control lists (ACL) “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.

match address (IPSec)

To specify an extended access list for a crypto map entry, use the **match address** command in crypto map configuration mode. To remove the extended access list from a crypto map entry, use the **no** form of this command.

match address [*access-list-id* | *name*]

no match address [*access-list-id* | *name*]

Syntax Description

access-list-id	(Optional) Identifies the extended access list by its name or number. This value should match the *access-list-number* or *name* argument of the extended access list being matched.
name	(Optional) Identifies the named encryption access list. This name should match the *name* argument of the named encryption access list being matched.

Defaults

No access lists are matched to the crypto map entry.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command is required for all static crypto map entries. If you are defining a dynamic crypto map entry (with the **crypto dynamic-map** command), this command is not required but is strongly recommended.

Use this command to assign an extended access list to a crypto map entry. You also need to define this access list using the **access-list** or **ip access-list extended** commands.

The extended access list specified with this command will be used by IPSec to determine which traffic should be protected by crypto and which traffic does not need crypto protection. (Traffic that is permitted by the access list will be protected. Traffic that is denied by the access list will not be protected in the context of the corresponding crypto map entry.)

Note that the crypto access list is *not* used to determine whether to permit or deny traffic through the interface. An access list applied directly to the interface makes that determination.

The crypto access list specified by this command is used when evaluating both inbound and outbound traffic. Outbound traffic is evaluated against the crypto access lists specified by the interface's crypto map entries to determine if it should be protected by crypto and if so (if traffic matches a **permit** entry) which crypto policy applies. (If necessary, in the case of static IPSec crypto maps, new security associations are established using the data flow identity as specified in the **permit** entry; in the case of dynamic crypto map entries, if no SA exists, the packet is dropped.) After passing the regular access lists at the interface, inbound traffic is evaluated against the crypto access lists specified by the entries of the

interface's crypto map set to determine if it should be protected by crypto and, if so, which crypto policy applies. (In the case of IPSec, unprotected traffic is discarded because it should have been protected by IPSec.)

In the case of IPSec, the access list is also used to identify the flow for which the IPSec security associations are established. In the outbound case, the **permit** entry is used as the data flow identity (in general), while in the inbound case the data flow identity specified by the peer must be "permitted" by the crypto access list.

Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the security associations. (This example is for a static crypto map.)

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for this crypto map entry, or that IPSec requires PFS when receiving requests for new security associations.
set security-association level per-host	Specifies that separate IPSec security associations should be requested for each source/destination host pair.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations.
set session-key	Specifies the IPSec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

match certificate (ca-trustpoint)

To associate a certificate-based access control list (ACL) that is defined with the **crypto ca certificate map** command, use the **match certificate** command in ca-trustpoint configuration mode. To remove the association, use the **no** form of this command.

match certificate *certificate-map-label [***allow expired-certificate** | **skip revocation-check** | **skip authorization-check***]*

no match certificate *certificate-map-label [***allow expired-certificate** | **skip revocation-check** | **skip authorization-check***]*

Syntax Description

certificate-map-label	Matches the *label* argument specified in a previously defined **crypto ca certificate map** command.
allow expired-certificate	(Optional) Ignores expired certificates. **Note** If this keyword is not configured, the router does not ignore expired certificates.
skip revocation-check	(Optional) Allows a trustpoint to enforce certificate revocation lists (CRLs) except for specific certificates. **Note** If this keyword is not configured, the trustpoint enforces CRLs for all certificates.
skip authorization-check	(Optional) Skips the authentication, authorization, and accounting (AAA) check of a certificate when public key infrastructure (PKI) integration with an AAA server is configured. **Note** If this keyword is not configured and PKI integration with an AAA server is configured, the AAA checking of a certificate is done.

Defaults

If this command is not configured, no default match certificate is configured. Each of the **allow expired-certificate**, **skip revocation-check**, and **skip authorization-check** keywords have a default (see the "Syntax Description" section).

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(4)T	The **allow expired-certificate**, **skip revocation-check**, and **skip authorization-check** keywords were added.

Usage Guidelines

The **match certificate** command associates the certificate-based ACL defined with the **crypto ca certificate map** command to the trustpoint. The *certificate-map-label* argument in the **match certificate** command must match the *label* argument specified in a previously defined **crypto ca certificate map** command.

The certificate map with the label *certificate-map-label* must be defined before it can be used with the **match certificate** subcommand.

A certificate referenced in a **match certificate** command may not be deleted until all references to the certificate map are removed from configured trustpoints (that is, no **match certificate** commands can reference the certificate map being deleted).

When the certificate of a peer has been verified, the certificate-based ACL as specified by the certificate map is checked. If the certificate of the peer matches the certificate ACL, or a certificate map is not associated with the trustpoint used to verify the certificate of the peer, the certificate of the peer is considered valid.

If the certificate map does not have any attributes defined, the certificate is rejected.

Using the allow expired-certificate Keyword

The **allow expired-certificate** keyword has two purposes:

- If the certificate of a peer has expired, this keyword may be used to "allow" the expired certificate until the peer is able to obtain a new certificate.
- If your router clock has not yet been set to the correct time, the certificate of a peer will appear to be not yet valid until the clock is set. This keyword may be used to allow the certificate of the peer even though your router clock is not set.

Note

- If Network Time Protocol (NTP) is available only via the IPSec connection (usually via the hub in a hub-and-spoke configuration), the router clock can never be set. The tunnel to the hub cannot be "brought up" because the certificate of the hub is not yet valid.
- "Expired" is a generic term for a certificate that is expired or that is not yet valid. The certificate has a start and end time. An expired certificate, for purposes of the ACL, is one for which the current time of the router is outside the start and end time specified in the certificate.

Using the skip revocation-check Keyword

The type of enforcement provided using the **skip revocation-check** keyword is most useful in a hub-and-spoke configuration in which you also want to allow direct spoke-to-spoke connections. In pure hub-and-spoke configurations, all spokes connect only to the hub, so CRL checking is necessary only on the hub. If one spoke communicates directly with another spoke, the CRLs must be checked. However, if the trustpoint is configured to require CRLs, the connection to the hub to retrieve the CRL usually cannot be made because the CRL is available only via the connection hub.

Using the skip authorization-check Keyword

If the communication with an AAA server is protected with a certificate, and you want to skip the AAA check of the certificate, use the **skip authorization-check** keyword. For example, if a Virtual Private Network (VPN) tunnel is configured so that all AAA traffic goes over that tunnel, and the tunnel is protected with a certificate, you can use the **skip authorization-check keyword** to skip the certificate check so that the tunnel can be established.

The **skip authorization-check** keyword should be configured after PKI integration with an AAA server is configured.

Examples

The following example shows a certificate-based ACL with the label "Group" defined in a **crypto ca certificate map** command and included in the **match certificate** command:

```
crypto ca certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto ca trustpoint pki
 match certificate Group
```

The following example shows a configuration for a central site using the **allow expired-certificate** keyword. The router at a branch site has an expired certificate named "branch1" and has to establish a tunnel to the central site to renew its certificate.

```
crypto pki trustpoint VPN-GW
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none
 ip-address none
 subject-name o=Home Office Inc,cn=Central VPN Gateway
 revocation-check crl
 match certificate branch1 allow expired-certificate
```

The following example shows a branch office configuration using the **skip revocation-check** keyword. The trustpoint is being allowed to enforce CRLs except for "central-site" certificates.

```
crypto pki trustpoint home-office
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none
 ip-address none
 subject-name o=Home Office Inc,cn=Branch 1
 revocation-check crl
 match certificate central-site skip revocation-check
```

The following example shows a branch office configuration using the **skip authorization-check** keyword. The trustpoint is being allowed to skip AAA checking for the central site.

```
crypto pki trustpoint home-office
 auth list allow_list
 auth user subj commonname
 match certificate central-site skip authorization-check
```

Related Commands

Command	Description
crypto ca certificate map	Defines certificate-based ACLs.
crypto ca trustpoint	Declares the CA that your router should use.

match certificate (ISAKMP)

To assign an Internet Security Association Key Management Protocol (ISAKMP) profile to a peer on the basis of the contents of arbitrary fields in the certificate, use the **match certificate** command in crypto ISAKMP profile configuration mode. To remove the profile, use the **no** form of this command.

match certificate *certificate-map*

no match certificate *certificate-map*

Syntax Description

certificate-map	Name of the certificate map.

Defaults

No default behavior or values

Command Modes

Crypto ISAKMP profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **match certificate** command is used after the certificate map has been configured and the ISAKMP profiles have been assigned to them.

Examples

The following configuration example shows that whenever a certificate contains “ou = green,” the ISAKMP profile “cert_pro” will be assigned to the peer.

```
crypto pki certificate map cert_map 10
 subject-name co ou = green
!
!
crypto isakmp identity dn
crypto isakmp profile cert_pro
   ca trust-point 2315
   ca trust-point LaBcA
   initiate mode aggressive
   match certificate cert_map
```

Related Commands

Command	Description
client configuration group	Associates a group with the peer that has been assigned an ISAKMP profile.

match certificate override cdp

To manually override the existing certificate distribution point (CDP) entries for a certificate with a URL or directory specification, use the **match certificate override cdp** command in ca-trustpoint configuration mode. To remove the override, use the **no** form of this command.

match certificate *certificate-map-label* **override cdp** {**url** | **directory**} *string*

no match certificate *certificate-map-label* **override cdp** {**url** | **directory**} *string*

Syntax Description

certificate-map-label	A user-specified label that must match the *label* argument specified in a previously defined **crypto ca certificate map** command.
url	Specifies that the certificates CDPs will be overridden with an http or ldap URL.
directory	Specifies that the certificate's CDPs will be overridden with an ldap directory specification.
string	The URL or directory specification.

Defaults

The existing CDP entries for the certificate are used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **match certificate override cdp** command to replace all of the existing CDPs in a certificate with a manually configured CDP URL or directory specification.

The *certificate-map-label* argument in the **match certificate override cdp** command must match the *label* argument specified in a previously defined **crypto ca certificate map** command.

Note Some applications may time out before all CDPs have been tried and will report an error message. This will not affect the router, and the Cisco IOS software will continue attempting to retrieve a CRL until all CDPs have been tried.

Examples

The following example uses the **match certificate override cdp** command to override the CDPs for the certificate map named Group1 defined in a **crypto ca certificate map** command:

```
crypto ca certificate map Group1 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto ca trustpoint pki
```

```
match certificate Group1 override cdp url http://server.cisco.com
```

Related Commands

Command	Description
crypto ca certificate map	Defines certificate-based ACLs.
crypto ca trustpoint	Declares the CA that your router should use.

match identity

To match an identity from a peer in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **match identity** command in ISAKMP profile configuration mode. To remove the identity, use the **no** form of this command.

match identity {**group** *group-name* | **address** *address* [*mask*] [*fvrf*] | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}

no match identity {**group** *group-name* | **address** *address* [*mask*] [*fvrf*] | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}

Syntax Description

group *group-name*	A Unity group that matches identification (ID) type ID_KEY_ID. If Unity and main mode Rivest, Shamir, and Adelman (RSA) signatures are used, the *group-name* argument matches the Organizational Unit (OU) field of the Distinguished Name (DN).
address *address* [*mask*] [*fvrf*]	An identity that matches the identity of type ID_IPV4_ADDR. • *mask*—Use to match the range of the address. • *fvrf*—Use to match the address in the front door Virtual Route Forwarding (FVRF) Virtual Private Network (VPN) space.
host *host-name*	Identity that matches an identity of the type ID_FQDN.
host domain *domain-name*	Identity that matches an identity of the type ID_FQDN, whose fully qualified domain name (FQDN) ends with the domain name.
user *user-fqdn*	Identity that matches the FQDN.
user domain *domain-name*	Identity that matches the identities of the type ID_USER_FQDN. When the **user domain** keyword is present, all users having identities of the type ID_USER_FQDN and ending with "*domain-name*" will be matched.

Defaults

No default behavior or values

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

There must be at least one **match identity** command in an ISAKMP profile configuration. The peers are mapped to an ISAKMP profile when their identities are matched (as given in the ID payload of the Internet Key Exchange [IKE] exchange) against the identities that are defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid.

Examples

The following example shows that the **match identity** command is configured:

```
crypto isakmp profile vpnprofile
 match identity group vpngroup
 match identity address 10.53.11.1
 match identity host domain vpn.com
 match identity host server.vpn.com
```

max-logins

To limit the number of simultaneous logins for users in a specific server group, use the **max-logins** command in global configuration mode. To remove the number of connections that were set, use the **no** form of this command.

max-logins *number-of-users*

no max-logins *number-of-users*

Syntax Description

number-of-users	Number of logins. The value ranges from 1 through 10.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **crypto isakmp client configuration group** command must be configured before this command can be configured.

This command makes it possible to mimic the functionality provided by some RADIUS servers for limiting the number of simultaneous logins for users in that group.

The **max-users** and **max-logins** keywords can be enabled together or individually to control the usage of resources by any groups or individuals.

Examples

The following example shows that the maximum number of logins for users in server group “cisco” has been set to 8:

```
Router (config)# crypto isakmp client configuration group cisco
Router (config)# max-logins 8
```

The following shows the RADIUS attribute-value (AV) pairs for the maximum users and maximum logins parameters:

```
ipsec:max-users=1000
ipsec:max-logins=1
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
max-users	Limits the number of connections to a specific server group.

max-users

To limit the number of connections to a specific server group, use the **max-users** command in global configuration mode. To remove the number of connections that were set, use the **no** form of this command.

max-users *number-of-users*

no max-users *number-of-users*

Syntax Description

number-of-users	Number of users. The value ranges from 1 through 5000.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

The **crypto isakmp client configuration group** command must be configured before this command can be configured.

This command makes it possible to mimic the functionality provided by some RADIUS servers for limiting the number of connections to a specific server group.

The **max-users** and **max-logins** keywords can be enabled together or individually to control the usage of resources by any groups or individuals.

Examples

The following example shows that the maximum number of connections to server group "cisco" has been set to 1200:

```
Router (config)# crypto isakmp client configuration group cisco
Router (config)# max-users 1200
```

The following shows the RADIUS attribute-value (AV) pairs for the maximum users and maximum logins parameters:

```
ipsec:max-users=1000
ipsec:max-logins=1
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
max-logins	Limits the number of simultaneous logins for users in a specific server group.

mode (IPSec)

To change the mode for a transform set, use the **mode** command in crypto transform configuration mode. To reset the mode to the default value of tunnel mode, use the **no** form of this command.

mode [**tunnel** | **transport**]

no mode

Syntax Description

tunnel | **transport**	(Optional) Specifies the mode for a transform set: either tunnel or transport mode. If neither **tunnel** nor **transport** is specified, the default (tunnel mode) is assigned.

Defaults

Tunnel mode

Command Modes

Crypto transform configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command to change the mode specified for the transform. This setting is only used when the traffic to be protected has the same IP addresses as the IPSec peers (this traffic can be encapsulated either in tunnel or transport mode). This setting is ignored for all other traffic (all other traffic is encapsulated in tunnel mode).

If the traffic to be protected has the same IP address as the IP Security peers and transport mode is specified, during negotiation the router will request transport mode but will accept either transport or tunnel mode. If tunnel mode is specified, the router will request tunnel mode and will accept only tunnel mode.

After you define a transform set, you are put into the crypto transform configuration mode. While in this mode you can change the mode to either tunnel or transport. This change applies only to the transform set just defined.

If you do not change the mode when you first define the transform set, but later decide you want to change the mode for the transform set, you must re-enter the transform set (specifying the transform name and all its transforms) and then change the mode.

If you use this command to change the mode, the change will only affect the negotiation of subsequent IPSec security associations via crypto map entries which specify this transform set. (If you want the new settings to take effect sooner, you can clear all or part of the security association database. See the **clear crypto sa** command for more details.

Tunnel Mode

With tunnel mode, the entire original IP packet is protected (encrypted, authenticated, or both) and is encapsulated by the IPSec headers and trailers (an Encapsulation Security Protocol header and trailer, an Authentication Header, or both). Then a new IP header is prefixed to the packet, specifying the IPSec endpoints as the source and destination.

Tunnel mode can be used with any IP traffic. Tunnel mode must be used if IPSec is protecting traffic from hosts behind the IPSec peers. For example, tunnel mode is used with Virtual Private Networks (VPNs) where hosts on one protected network send packets to hosts on a different protected network via a pair of IPSec peers. With VPNs, the IPSec peers "tunnel" the protected traffic between the peers while the hosts on their protected networks are the session endpoints.

Transport Mode

With transport mode, only the payload (data) of the original IP packet is protected (encrypted, authenticated, or both). The payload is encapsulated by the IPSec headers and trailers (an ESP header and trailer, an AH header, or both). The original IP headers remain intact and are not protected by IPSec.

Use transport mode only when the IP traffic to be protected has IPSec peers as both the source and destination. For example, you could use transport mode to protect router management traffic. Specifying transport mode allows the router to negotiate with the remote peer whether to use transport or tunnel mode.

Examples

The following example defines a transform set and changes the mode to transport mode. The mode value only applies to IP traffic with the source and destination addresses at the local and remote IPSec peers.

```
crypto ipsec transform-set newer esp-des esp-sha-hmac
 mode transport
 exit
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set—an acceptable combination of security protocols and algorithms.

mode ra

To place the public key infrastructure (PKI) server into Registration Authority (RA) certificate server mode, use the **mode ra** command in certificate server configuration mode. To remove the PKI server from RA certificate mode, use the **no** form of this command.

mode ra

no mode ra

Syntax Description

This command has no arguments or keywords.

Defaults

The PKI server is not placed into RA certificate server mode.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When this command is configured, ensure that the **crypto pki trustpoint** command has also been configured and that the enrollment URL is pointed to a Cisco IOS issuing certification authority (CA). If the **mode ra** command is not configured and the certificate server is enabled for the first time, a self-signed CA certificate will be generated and the certificate server will operate as a root CA.

Examples

The following configuration example shows that a RA mode certificate server named "myra" has been configured:

```
Router (config)# crypto pki trustpoint myra
Router (ca-trustpoint)# enrollment url http://10.3.0.6
Router (ca-trustpoint)# subject-name cn=myra, ou=ioscs RA, o=cisco, c=us
Router (ca-trustpoint)# exit

Router (config)# crypto pki server myra
Router (cs-server)# mode ra
Router (cs-server)# no shutdown
```

Related Commands:

Command	Description
crypto pki server	Enables a Cisco IOS certificate server.
crypto pki trustpoint	Declares the trustpoint that your router should use.
enrollment	Specifies the enrollment parameters of a CA.
show crypto pki server	Displays the current state and configuration of the certificate server.

name (view)

To change the name of a lawful intercept view, use the **name** command in view configuration mode. To return to the default lawful intercept view name, which is "li-view," use the **no** form of this command.

name *new-name*

no name *new-name*

Syntax Description

new-name	Lawful intercept view name.

Defaults

A lawful intercept view is called "li-view."

Command Modes

View configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Only a system administrator or a level 15 privilege user can change the name of a lawful intercept view.

Examples

The following example shows how to configure a lawful intercept view and change the view name to "myliview":

```
!Initialize the LI-View.
Router(config-view)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config-view)# name myliview
Router(config-view)# end
```

Related Commands

Command	Description
li-view	Creates a lawful intercept view.
parser view	Creates or changes a CLI view and enters view configuration mode.

named-key

To specify which peer's RSA public key you will manually configure and enter public key configuration mode, use the **named-key** command in public key chain configuration mode. This command should be used only when the router has a single interface that processes IP Security (IPSec).

named-key *key-name* [**encryption** | **signature**]

Syntax Description

key-name	Specifies the name of the remote peer's RSA keys. This is always the fully qualified domain name of the remote peer; for example, router.example.com.
encryption	(Optional) Indicates that the RSA public key to be specified will be an encryption special-usage key.
signature	(Optional) Indicates that the RSA public key to be specified will be a signature special-usage key.

Defaults

If neither the **encryption** nor the **signature** keyword is used, general-purpose keys will be specified.

Command Modes

Public key chain configuration.

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command or the **addressed-key** command to specify which IPSec peer's RSA public key you will manually configure next.

Follow this command with the **key-string** command to specify the key.

If you use the **named-key** command, you also need to use the **address** public key configuration command to specify the IP address of the peer.

If the IPSec remote peer generated general purpose RSA keys, do not use the **encryption** or **signature** keyword.

If the IPSec remote peer generated special usage keys, you must manually specify both keys: perform this command and the **key-string** command twice and use the **encryption** and **signature** keywords in turn.

Examples

The following example manually specifies the RSA public keys of two IPSec peers. The peer at 10.5.5.1 uses general-purpose keys, and the other peer uses special-purpose keys.

```
crypto key pubkey-chain rsa
  named-key otherpeer.example.com
  address 10.5.5.1
  key-string
 005C300D 06092A86 4886F70D 01010105
 00034B00 30480241 00C5E23B 55D6AB22
```

```
04AEF1BA A54028A6 9ACC01C5 129D99E4
64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
D58AD221 B583D7A4 71020301 0001
quit
exit
 addressed-key 10.1.1.2 encryption
 key-string
00302017 4A7D385B 1234EF29 335FC973
2DD50A37 C4F4B0FD 9DADE748 429618D5
18242BA3 2EDFBDD3 4296142A DDF7D3D8
08407685 2F2190A0 0B43F1BD 9A8A26DB
07953829 791FCDE9 A98420F0 6A82045B
90288A26 DBC64468 7789F76E EE21
quit
 exit
 addressed-key 10.1.1.2 signature
 key-string
0738BC7A 2BC3E9F0 679B00FE 098533AB
01030201 42DD06AF E228D24C 458AD228
58BB5DDD F4836401 2A2D7163 219F882E
64CE69D4 B583748A 241BED0F 6E7F2F16
0DE0986E DF02031F 4B0B0912 F68200C4
C625C389 0BFF3321 A2598935 C1B1
quit
 exit
 exit
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer you will manually configure.
addressed-key	Specifies the RSA public key of the peer you will manually configure.
crypto key pubkey-chain rsa	Enters public key configuration mode (to allow you to manually specify the RSA public keys of other devices).
key-string (IKE)	Specifies the RSA public key of a remote peer.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

nas

To add an access point or router to the list of devices that use the local authentication server, use the **nas** command in local RADIUS server configuration mode. To remove the identity of the network access server (NAS) that is configured on the local RADIUS server, use the **no** form of this command

nas *ip-address* **key** *shared-key*

no nas *ip-address* **key** *shared-key*

Syntax Description

ip-address	IP address of the access point or router.
key	Specifies a key.
shared-key	Shared key that is used to authenticate communication between the local authentication server and the access points and routers that use this authenticator.

Defaults

No default behavior or values

Command Modes

Local RADIUS server configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following command adds the access point having the IP address 192.168.12.17 to the list of devices that use the local authentication server, using the shared key “shared256.”

```
nas 192.168.12.17 key shared256
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.

Command	Description
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

no crypto xauth

To ignore extended authentication (Xauth) during an Internet Key Exchange (IKE) Phase 1 negotiation, use the **no crypto xauth** command in global configuration mode. To consider Xauth proposals, use the **crypto xauth** command.

no crypto xauth *interface*

crypto xauth *interface*

Syntax Description

interface	Interface whose IP address is the local endpoint to which the remote peer will send IKE requests.

Defaults

No default behaviors or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The **no** version of this command was introduced to support Unity clients that do not require Xauth when using Internet Security Association and Key Management Protocol (ISAKMP) profiles.

Examples

The following example shows that Xauth proposals on Ethernet 1/1 are to be ignored:

```
no crypto xauth Ethernet1/1
```

no ip inspect

To turn off Context-based Access Control (CBAC) completely at a firewall, use the **no ip inspect** command in global configuration mode.

no ip inspect

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

Turn off CBAC with the **no ip inspect** global configuration command.

Note The **no ip inspect** command removes all CBAC configuration entries and resets all CBAC global timeouts and thresholds to the defaults. All existing sessions are deleted and their associated access lists are removed.

Examples

The following example turns off CBAC at a firewall:

```
no ip inspect
```

no ip ips sdf builtin

To instruct the router not to load the built-in signatures if it cannot find the specified signature definition files (SDFs), use the **no ip ips sdf builtin** command in global configuration mode.

no ip ips sdf builtin

Syntax Description

This command has no arguments or keywords.

Defaults

If the router fails to load the SDF, the router will load the default, built-in signatures.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Caution If the **no ip ips sdf builtin** command is issued and the router running Intrusion Prevention System (IPS) fails to load the SDF, you will receive an error message stating that IPS is completely disabled.

Examples

The following example shows how to instruct the router not to refer to the default, built-in signature if the attack-drop.sdf file fails to load:

```
Router(config) no ip ips sdf builtin
```

Related Commands

Command	Description
copy ips-sdf	Loads or saves the SDF in the router.
ip ips sdf location	Specifies the location in which the router will load the SDF.

ocsp url

To enable an online certificate status protocol (OCSP) server, use the **ocsp url** command in ca-trustpoint configuration mode. To disable the OCSP server, use the **no** form of this command.

ocsp url [*url*]

no ocsp url [*url*]

Syntax Description

url	(Optional) All certificates associated with a configured trustpoint will be checked by the OCSP server at the specified HTTP URL.

Defaults

OCSP is not enabled.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

A central OCSP server can be configured to collect and update certificate revocation lists (CRLs) from different certification authority (CA) servers. Thus, the devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every device.

If the *url* option is not enabled, the certificate will be checked by the OCSP server in the Authority Info Access (AIA) extension of the certificate.

Examples

The following example shows how to configure your router to use the OCSP server at the HTTP URL "http://myocspserver:81." If the server is down, revocation check will be ignored.

```
Router(config)# crypto ca trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
revocation-check	Checks the revocation status of a certificate.

outgoing

To configure filtering for outgoing export traffic, use the **outgoing** command in router IP traffic export (RITE) configuration mode. To disable filtering for outgoing traffic, use the **no** form of this command.

outgoing {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}

no outgoing {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}

Syntax Description

access-list {*standard* | *extended* | *named*}	An existing numbered (standard or extended) or named access control list (ACL). **Note** The filter is applied only to exported traffic.
sample one-in-every *packet-number*	Export only one packet out of every specified number of packets. Valid range for the *packet-number* argument is 2 to 2147483647 packets.

Defaults

If this command is not enabled, outgoing IP traffic is not exported.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

When configuring a network device for IP traffic export, you can issue the **outgoing** command to filter unwanted outgoing traffic via the following methods:

- ACLs, which accept or deny an IP packet for export
- Sampling, which allows you to export one in every few packets in which you are interested. Use this option when it is not necessary to export all incoming traffic. Also, sampling is useful when a monitored ingress interface can send traffic faster than the egress interface can transmit it.

Note If you issue this command, you must also issue the **bidirectional** command, which enables outgoing traffic to be exported. However, only routed traffic (such as passthrough traffic) is exported; that is, traffic that originates from the network device is not exported.

Examples

The following example shows how to configure the profile "corp1," which will send captured IP traffic to host "00a.8aab.90a0" at the interface "FastEthernet 0/1." This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the ACL "ham_ACL."

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
```

```
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported across a monitored interface.
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
incoming	Configures filtering for incoming IP traffic.

parameter

To specify parameters for an enrollment profile, use the **parameter** command in ca-profile-enroll configuration mode. To disable specified parameters, use the **no** form of this command.

parameter *number* {**value** *value* | **prompt** *string*}

no parameter *number* {**value** *value* | **prompt** *string*}

Syntax Description

number	User parameters. Valid values range from 1 to 8.
value *value*	To be used if the parameter has a constant value.
prompt *string*	To be used if the parameter is supplied after the **crypto ca authenticate** command or the **crypto ca enroll** command has been entered. **Note** The value of the *string* argument does not have an effect on the value that is used by the router.

Defaults

No enrollment profile paramters are specified.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The **parameter** command can be used within an enrollment profile after the **authentication command** command or the **enrollment command** has been enabled.

Examples

The following example shows how to specify parameters for the enrollment profile named “E”:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
authentication command	Specifies the HTTP command that is sent to the CA for authentication.
crypto ca profile enrollment	Defines an enrollment profile.
enrollment command	Specifies the HTTP command that is sent to the CA for enrollment.

parser view

To create or change a command-line interface (CLI) view and enter view configuration mode, use the **parser view** command in global configuration mode. To delete a view, use the **no** form of this command.

parser view *view-name*

no parser view *view-name*

Syntax Description

view-name	View name, which can include 1 to 30 alphanumeric characters. The *view-name* argument must not have a number as the first character; otherwise, you will receive the following error message: "Invalid view name."

Defaults

A CLI view does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

A CLI view is a set of operational commands and configuration capabilities that restrict user access to the CLI and configuration information; that is, a view allows users to define what commands are accepted and what configuration information is visible.

After you have issued the **parser view** command, you can configure the view via the **password 5** command and the **commands** command.

To use the **parser view** command, the system of the user must be set to root view. The root view can be enabled via the **enable view** command.

Examples

The following example show how to configure two CLI views, "first" and "second."

```
Router(config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Router(config-view)# password 5 firstpass
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command exec include all show ip
Router(config-view)# exit
Router(config)# parser view second
00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully created.
Router(config-view)# password 5 secondpass
Router(config-view)# command exec include-exclusive show ip interface
Router(config-view)# command exec include logout
Router(config-view)# exit
```

After you have successfully created a view, a system message such as the following will be displayed:

```
%PARSER-6-VIEW_CREATED: view 'first' successfully created.
```

After you have successfully deleted a view, a system message such as the following will be displayed:

```
%PARSER-6-VIEW_DELETED: view 'first' successfully deleted.
```

Related Commands

Command	Description
commands (view)	Adds commands to a CLI view.
password 5	Associates a CLI view or a superview with a password.

password (ca-trustpoint)

To specify the revocation password for the certificate, use the **password** command in ca-trustpoint configuration mode. To erase any stored passwords, use the **no** form of this command.

password *string*

no password

Syntax Description

string	Name of the password.

Defaults

You are prompted for the password during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Before you can issue the **password** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

This command allows you to specify the revocation password for the certificate before actual certificate enrollment begins. The specified password is encrypted when the updated configuration is written to NVRAM by the router.

If this command is enabled, you will not be prompted for a password during certificate enrollment.

Examples

The following example shows how to specify the password “revokme” for the certificate request:

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 auto-enroll regenerate
 password revokme
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

password (line configuration)

To specify a password on a line, use the **password** command in line configuration mode. To remove the password, use the **no** form of this command.

password *password*

no password

Syntax Description

password	Character string that specifies the line password. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. The space after the number causes problems. For example, hello 21 is a legal password, but 21 hello is not. The password checking is case sensitive. For example, the password Secret is different than the password secret.

Defaults

No password is specified.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When an EXEC process is started on a line with password protection, the EXEC prompts for the password. If the user enters the correct password, the EXEC prints its normal privileged prompt. The user can try three times to enter a password before the EXEC exits and returns the terminal to the idle state.

Examples

The following example removes the password from virtual terminal lines 1 to 4:

```
line vty 1 4
 no password
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.

password 5

To associate a command-line interface (CLI) view or a superview with a password, use the **password 5** command in view configuration mode.

password 5 *password*

Syntax Description

password	Password for users to enter the CLI view or superview. A password can contain any combination of alphanumeric characters. **Note** The password is case sensitive.

Defaults

A user cannot access a CLI view or superview.

Command Modes

View configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	This command was enhanced to support superviews.

Usage Guidelines

A user cannot access any commands within the CLI view or superview until the **password 5** command has been issued.

Examples

The following example show how to configure two CLI views, “first” and “second” and associate each view with a password:

```
Router(config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Router(config-view)# password 5 firstpass
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command exec include all show ip
Router(config-view)# exit
Router(config)# parser view second
00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully created.
Router(config-view)# password 5 secondpass
Router(config-view)# command exec include-exclusive show ip interface
Router(config-view)# command exec include logout
Router(config-view)# exit
```

Related Commands

Command	Description
parser superview	Creates or changes a superview and enters view configuration mode.
parser view	Creates or changes a CLI view and enters view configuration mode.

password encryption aes

To enable a type 6 encrypted preshared key, use the **password encryption aes** command in global configuration mode. To disable password encryption, use the **no** form of this command.

password encryption aes

no password encryption aes

Syntax Description

This command has no arguments or keywords.

Defaults

Preshared keys are not encrypted.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

You can securely store plain text passwords in type 6 format in NVRAM using a command-line interface (CLI). Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encryption** command with the **password encryption aes** command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) configured using the **key config-key password-encryption** command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the **password encryption aes** command without configuring the **key config-key password-encryption** command, the following message is printed at startup or during any nonvolatile generation (NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands have been configured:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

Note For Cisco 836 routers, please note that support for Advanced Encryption Standard (AES) is available only on IP plus images.

Changing a Password

If the password (master key) is changed, or reencrypted, using the **key config-key password-encryption** command), the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

Deleting a Password

If the master key that was configured using the **key config-key password-encryption** command is deleted from the system, a warning is printed (and a confirm prompt is issued) that states that all type 6 passwords will become useless. As a security measure, after the passwords have been encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be reencrypted as explained in the previous paragraph.

Caution If the password configured using the **key config-key password-encryption** command is lost, it cannot be recovered. The password should be stored in a safe location.

Unconfiguring Password Encryption

If you later unconfigure password encryption using the **no password encryption aes** command, all existing type 6 passwords are left unchanged, and as long as the password (master key) that was configured using the **key config-key password-encryption** command exists, the type 6 passwords will be decrypted as and when required by the application.

Storing Passwords

Because no one can "read" the password (configured using the **key config-key password-encryption** command), there is no way that the password can be retrieved from the router. Existing management stations cannot "know" what it is unless the stations are enhanced to include this key somewhere, in which case the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the **key config-key password-encryption** command). The password can be manually added to the stored configuration but is not recommended because adding the password manually allows anyone to decrypt all passwords in that configuration.

Configuring New or Unknown Passwords

If you enter or cut and paste cipher text that does not match the master key, or if there is no master key, the cipher text is accepted or saved, but an alert message is printed. The alert message is as follows:

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

If a new master key is configured, all the plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or unknown, you have the option of deleting the master key using the **no key config-key password-encryption** command. Deleting the master key using the **no key config-key password-encryption** command causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

Examples

The following example shows that a type 6 encrypted preshared key has been enabled:

```
Router (config)# password encryption aes
```

Related Commands

Command	Description
key config-key password-encryption	Stores a type 6 encryption key in private NVRAM.
password logging	Provides a log of debugging output for a type 6 password operation.

password logging

To get a log of debugging output for a type 6 password operation, use the **password logging** command in privileged EXEC mode. To disable the debugging, use the **no** form of this command.

password logging

no password logging

Syntax Description

This command has no arguments or keywords.

Defaults

Debug logging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.

Examples

The following example shows that debug logging is configured:

```
Router# password logging
```

Related Commands

Command	Description
key config-key password-encryption	Stores an encryption key in private NVRAM.
password encryption aes	Enables a type 6 encrypted preshared key.

permit (reflexive)

To create a reflexive access list and to enable its temporary entries to be automatically generated, use the **permit** command in access-list configuration mode. To delete the reflexive access list (if only one protocol was defined) or to delete protocol entries from the reflexive access list (if multiple protocols are defined), use the **no** form of this command.

permit *protocol source source-wildcard destination destination-wildcard* **reflect** *name* [**timeout** *seconds*]

no permit *protocol source-wildcard destination destination-wildcard* **reflect** *name*

Syntax Description

protocol	Name or number of an IP protocol. It can be one of the keywords **gre**, **icmp**, **ip**, **ipinip**, **nos**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol, Transmission Control Protocol, and User Datagram Protocol), use the keyword **ip**.
source	Number of the network or host from which the packet is being sent. There are three other ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. This keyword is normally not recommended (see the section "Usage Guidelines"). • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits (mask) to be applied to source. There are three other ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. This keyword is normally not recommended (see the section "Usage Guidelines"). • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are three other ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. This keyword is normally *not* recommended (see the section "Usage Guidelines"). • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0.

destination-wildcard	Wildcard bits to be applied to the destination. There are three other ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. This keyword is normally *not* recommended (see the section "Usage Guidelines"). • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
reflect	Identifies this access list as a reflexive access list.
name	Specifies the name of the reflexive access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists. The name can be up to 64 characters long.
timeout *seconds*	(Optional) Specifies the number of seconds to wait (when no session traffic is being detected) before entries expire in this reflexive access list. Use a positive integer from 0 to 2^{32}–1. If not specified, the number of seconds defaults to the global timeout value.

Defaults

If this command is not configured, no reflexive access lists will exist, and no session filtering will occur.

If this command is configured without specifying a **timeout** value, entries in this reflexive access list will expire after the global timeout period.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command is used to achieve reflexive filtering, a form of session filtering.

For this command to work, you must also nest the reflexive access list using the **evaluate** command.

This command creates a reflexive access list and triggers the creation of entries in the same reflexive access list. This command must be an entry (condition statement) in an extended named IP access list.

If you are configuring reflexive access lists for an external interface, the extended named IP access list should be one which is applied to outbound traffic.

If you are configuring reflexive access lists for an internal interface, the extended named IP access list should be one which is applied to inbound traffic.

IP sessions that originate from within your network are initiated with a packet exiting your network. When such a packet is evaluated against the statements in the extended named IP access list, the packet is also evaluated against this reflexive **permit** entry.

As with all access list entries, the order of entries is important, because they are evaluated in sequential order. When an IP packet reaches the interface, it will be evaluated sequentially by each entry in the access list until a match occurs.

If the packet matches an entry prior to the reflexive **permit** entry, the packet will not be evaluated by the reflexive **permit** entry, and no temporary entry will be created for the reflexive access list (session filtering will not be triggered).

The packet will be evaluated by the reflexive **permit** entry if no other match occurs first. Then, if the packet matches the protocol specified in the reflexive **permit** entry, the packet is forwarded and a corresponding temporary entry is created in the reflexive access list (unless the corresponding entry already exists, indicating the packet belongs to a session in progress). The temporary entry specifies criteria that permits traffic into your network only for the same session.

Characteristics of Reflexive Access List Entries

This command enables the creation of temporary entries in the same reflexive access list that was defined by this command. The temporary entries are created when a packet exiting your network matches the protocol specified in this command. (The packet "triggers" the creation of a temporary entry.) These entries have the following characteristics:

- The entry is a **permit** entry.
- The entry specifies the same IP upper-layer protocol as the original triggering packet.
- The entry specifies the same source and destination addresses as the original triggering packet, except the addresses are swapped.
- If the original triggering packet is TCP or UDP, the entry specifies the same source and destination port numbers as the original packet, except the port numbers are swapped.

  If the original triggering packet is a protocol other than TCP or UDP, port numbers do not apply, and other criteria are specified. For example, for ICMP, type numbers are used: the temporary entry specifies the same type number as the original packet (with only one exception: if the original ICMP packet is type 8, the returning ICMP packet must be type 0 to be matched).
- The entry inherits all the values of the original triggering packet, with exceptions only as noted in the previous four bullets.
- IP traffic entering your internal network will be evaluated against the entry, until the entry expires. If an IP packet matches the entry, the packet will be forwarded into your network.
- The entry will expire (be removed) after the last packet of the session is matched.
- If no packets belonging to the session are detected for a configurable length of time (the timeout period), the entry will expire.

Examples

The following example defines a reflexive access list *tcptraffic*, in an outbound access list that permits all Border Gateway Protocol and Enhanced Interior Gateway Routing Protocol traffic and denies all ICMP traffic. This example is for an external interface (an interface connecting to an external network).

First, the interface is defined and the access list is applied to the interface for outbound traffic.

```
interface Serial 1
 description Access to the Internet via this interface
 ip access-group outboundfilters out
```

Next, the outbound access list is defined and the reflexive access list *tcptraffic* is created with a reflexive **permit** entry.

```
ip access-list extended outboundfilters
 permit tcp any any reflect tcptraffic
```

Related Commands

Command	Description
evaluate	Nests a reflexive access list within an access list.
ip access-list	Defines an IP access list by name.
ip reflexive-list timeout	Specifies the length of time that reflexive access list entries will continue to exist when no packets in the session are detected.

pfs

To configure a server to notify the client of the central-site policy regarding whether PFS is required for any IP Security (IPSec) Security Association (SA), use the **pfs** command in global configuration mode. To restore the default behavior, use the **no** form of this command.

pfs

no pfs

Syntax Description

This command has no arguments or keywords.

Defaults

The server will not notify the client of the central-site policy regarding whether PFS is required for any IPSec SA.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Before you use the **pfs** command, you must first configure the **crypto isakmp client configuration group** command.

An example of an attribute-value (AV) pair for the PFS attribute is as follows:

```
ipsec:pfs=1
```

Examples

The following example shows that the server has been configured to notify the client of the central-site policy regarding whether PFS is required for any IPSec SA:

```
crypto isakmp client configuration group
 pfs
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

pki-server

To specify the certificate server that is to be associated with the Trusted Transitive Introduction (TTI) exchange between the easy secure device deployment (EzSDD) petitioner and the EzSDD registrar, use the **pki-server** command in tti-registrar configuration mode. To change the specified certificate server, use the **no** form of this command.

pki-server *label*

no pki-server *label*

Syntax Description

label	Name of certificate server.

Defaults

A certificate server is not associated with the TTI exchange; thus, the petitioner and registrar will not be able to communicate.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Although any device that contains a crypto image can be the registrar, it is recommended that the registrar be either a Cisco IOS certificate server registration authority (RA) or a Cisco IOS certificate server root.

Examples

The following example shows how to associate the certificate server "cs1" with the TTI exchange:

```
crypto wui tti registrar
 pki-server cs1
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto wui tti registrar	Configures a device to become an EzSDD registrar and enters tti-registrar configuration mode.

pool (isakmp-group)

To define a local pool address, use the **pool** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove a local pool from your configuration, use the **no** form of this command.

pool *name*

no pool *name*

Syntax Description

name	Name of the local pool address.

Defaults

No default behavior or values.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **pool** command to refer to an IP local pool address, which defines a range of addresses that will be used to allocate an internal IP address to a client. Although a user must define at least one pool name, a separate pool may be defined for each group policy.

Note This command must be defined and refer to a valid IP local pool address, or the client connection will fail.

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **pool** command.

Examples

The following example shows how to refer to the local pool address “dog”:

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
!
ip local pool dog 10.1.1.1 10.1.1.254
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

ppp accounting

To enable authentication, authorization, and accounting (AAA) accounting services on the selected interface, use the **ppp accounting** command in interface configuration mode. To disable AAA accounting services, use the **no** form of this command.

ppp accounting default

no ppp accounting

Syntax Description

default	The name of the method list is created with the **aaa accounting** command.

Defaults

Accounting is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for accounting services to take place. Use the **ppp accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.

Examples

The following example enables accounting on asynchronous interface 4 and uses the accounting method list named charlie:

```
interface async 4
 encapsulation ppp
 ppp accounting charlie
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

ppp authentication

To enable at least one PPP authentication protocol and to specify the order in which the protocols are selected on the interface, use the **ppp authentication** command in interface configuration mode. To disable this authentication, use the **no** form of this command.

ppp authentication {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**]

no ppp authentication

Syntax Description

protocol1 [*protocol2...*]	At least one of the keywords described in Table 27.
if-needed	(Optional) Used with TACACS and extended TACACS. Does not perform Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication if authentication has already been provided. This option is available only on asynchronous interfaces.
list-name	(Optional) Used with authentication, authorization, and accounting (AAA). Specifies the name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command.
default	(Optional) Name of the method list created with the **aaa authentication ppp** command.
callin	(Optional) Authentication on incoming (received) calls only.
one-time	(Optional) The username and password are accepted in the username field.
optional	(Optional) Accepts the connection even if the peer refuses to accept the authentication methods that the router has requested.

Defaults

PPP authentication is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(1)	The **optional** keyword was added.
12.1(3)XS	The **optional** keyword was added.
12.2(2)XB5	Support for the **eap** authentication protocol was added on the Cisco 2650, Cisco 3640, Cisco 3660, Cisco AS5300, and Cisco AS5400 platforms.
12.2(13)T	The **eap** authentication protocol support introduced in Cisco IOS Release 12.2(2)XB5 was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

When you enable PAP, CHAP, or Extensible Authentication Protocol (EAP) authentication (or all three methods), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a Response message. The local router attempts to match the name of the remote device with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match. EAP works much as CHAP does, except that identity request and response packets are exchanged when EAP starts.

You can enable CHAP, Microsoft CHAP (MS-CHAP), PAP, or EAP in any order. If you enable all four methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the ability of the remote device to correctly negotiate the appropriate method and on the level of data-line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.

Caution If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, you will disable PPP on this interface.

Table 27 lists the protocols used to negotiate PPP authentication.

Table 27 ppp authentication Protocols

chap	Enables CHAP on a serial interface.
eap	Enables EAP on a serial interface.
ms-chap	Enables MS-CHAP on a serial interface.
pap	Enables PAP on a serial interface.

Enabling or disabling PPP authentication does not affect the ability of the local router to authenticate itself to the remote device.

If you are using autoselect on a tty line, you can use the **ppp authentication** command to turn on PPP authentication for the corresponding interface.

MS-CHAP is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; authentication occurs between a personal computer using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

To configure Cisco PDSN in compliance with the TIA/EIA/IS-835-B standard, you must configure the PDSN virtual template as follows:

```
ppp authentication chap pap optional
```

Examples

The following example configures virtual-template interface 4:

```
interface virtual-template 4
 ip unnumbered loopback0
 ppp authentication chap pap optional
```

The following example enables CHAP on asynchronous interface 4 and uses the authentication list MIS-access:

```
interface async 4
 encapsulation ppp
 ppp authentication chap MIS-access
```

The following example enables EAP on dialer interface 1:

```
interface dialer 1
 encapsulation ppp
 ppp authentication eap
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa new-model	Enables the AAA access control model.
autoselect	Configures a line to start an ARAP, PPP, or SLIP session.
encapsulation	Sets the encapsulation method used by the interface.
ppp accm	Identifies the ACCM table.
username	Establishes a username-based authentication system, such as PPP, CHAP, and PAP.

ppp authentication ms-chap-v2

To enable Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication on a network access server (NAS), use the **ppp authentication ms-chap-v2** command in interface configuration mode. To disable MSCHAP V2 authentication, use the **no** form of this command.

ppp authentication ms-chap-v2

no ppp authentication ms-chap-v2

Syntax Description

This command has no arguments or keywords.

Defaults

MSCHAP V2 authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

To enable MSCHAP V2 authentication, first configure PPP on the NAS. For the NAS to properly interpret authentication failure attributes and vendor-specific attributes, the **ppp max-bad-auth** command must be configured to allow at least two authentication retries and the **radius-server vsa send** command and **authentication** keyword must be enabled. The NAS must be able to interpret authentication failure attributes and vendor-specific attributes to support the ability to change an expired password.

Examples

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication locally:

```
interface Async65
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 ppp max-bad-auth 3
 ppp authentication ms-chap-v2
 username client password secret
```

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication via RADIUS:

```
interface Async65
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 async mode dedicated
```

```
 no peer default ip address
 ppp max-bad-auth 3
 ppp authentication ms-chap-v2
 exit
aaa authentication ppp default group radius
 radius-server host 10.0.0.2 255.0.0.0
 radius-server key secret
 radius-server vsa send authentication
```

Related Commands

Command	Description
debug aaa authentication	Displays information on AAA/TACACS+ authorization.
debug ppp	Displays information on traffic and exchanges in a network that is implementing PPP.
debug radius	Displays information associated with RADIUS.
ppp max-bad-auth	Configures a point-to-point interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.
radius-server vsa send	Configures the network access server to recognize and use VSAs.

ppp authorization

To enable authentication, authorization, and accounting (AAA) authorization on the selected interface, use the **ppp authorization** command in interface configuration mode. To disable authorization, use the **no** form of this command.

ppp authorization [**default** | *list-name*]

no ppp authorization

Syntax Description

default	(Optional) The name of the method list is created with the **aaa authorization** command.
list-name	(Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa authorization** command.

Defaults

Authorization is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for authorization to take place. Use the **ppp authorization** command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.

Examples

The following example enables authorization on asynchronous interface 4 and uses the method list named charlie:

```
interface async 4
 encapsulation ppp
 ppp authorization charlie
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

ppp chap hostname

To create a pool of dialup routers that all appear to be the same host when authenticating with Challenge Handshake Authentication Protocol (CHAP), use the **ppp chap hostname** command in interface configuration mode. To disable this function, use the **no** form of this command.

ppp chap hostname *hostname*

no ppp chap hostname *hostname*

Syntax Description

hostname	The name sent in the CHAP challenge.

Defaults

Disabled. The router name is sent in any CHAP challenges.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The **ppp chap hostname** command allows you to specify a common alias for all routers in a rotary group to use so that only one username must be configured on the dialing routers.

This command is normally used with local CHAP authentication (when the router authenticates to the peer), but it can also be used for remote CHAP authentication.

Examples

The following example identifies dialer interface 0 as the dialer rotary group leader and specifies "ppp" as the encapsulation method used by all member interfaces. This example shows that CHAP authentication is used on received calls only and the username *ISPCorp* will be sent in all CHAP challenges and responses.

```
interface dialer 0
 encapsulation ppp
 ppp authentication chap callin
 ppp chap hostname ISPCorp
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.

Command	Description
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap refuse	Refuses CHAP authentication from peers requesting it.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

ppp chap password

To enable a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common Challenge Handshake Authentication Protocol (CHAP) secret password to use in response to challenges from an unknown peer, use the **ppp chap password** command in interface configuration mode. To disable the PPP CHAP password, use the **no** form of this command.

ppp chap password *secret*

no ppp chap password *secret*

Syntax Description

secret	The secret used to compute the response value for any CHAP challenge from an unknown peer.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

This command is used for remote CHAP authentication only (when routers authenticate to the peer) and does not affect local CHAP authentication.

Examples

The commands in the following example specify ISDN BRI number 0. The method of encapsulation on the interface is PPP. If a CHAP challenge is received from a peer whose name is not found in the global list of usernames, the encrypted secret 7 1267234591 is decrypted and used to create a CHAP response value.

```
interface bri 0
 encapsulation ppp
 ppp chap password 7 1234567891
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.

Command	Description
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap refuse	Refuses CHAP authentication from peers requesting it.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

ppp chap refuse

To refuse Challenge Handshake Authentication Protocol (CHAP) authentication from peers requesting it, use the **ppp chap refuse** command in interface configuration mode. To allow CHAP authentication, use the **no** form of this command.

ppp chap refuse [**callin**]

no ppp chap refuse [**callin**]

Syntax Description

callin	(Optional) This keyword specifies that the router will refuse to answer CHAP authentication challenges received from the peer, but will still require the peer to answer any CHAP challenges the router sends.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command specifies that CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using CHAP will be refused. If the **callin** keyword is used, CHAP authentication is disabled for incoming calls from the peer, but will still be performed on outgoing calls to the peer.

If outbound Password Authentication Protocol (PAP) has been enabled (using the **ppp pap sent-username** command), PAP will be suggested as the authentication method in the refusal packet.

Examples

The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. This example disables CHAP authentication from occurring if a peer calls in requesting CHAP authentication.

```
interface bri 0
 encapsulation ppp
 ppp chap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.

Command	Description
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

ppp chap wait

To specify that the router will not authenticate to a peer requesting Challenge Handshake Authentication Protocol (CHAP) authentication until after the peer has authenticated itself to the router, use the **ppp chap wait** command in interface configuration mode. To allow the router to respond immediately to an authentication challenge, use the **no** form of this command.

ppp chap wait *secret*

no ppp chap wait *secret*

Syntax Description

secret	The secret used to compute the response value for any CHAP challenge from an unknown peer.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command (which is enabled by default) specifies that the router will not authenticate to a peer requesting CHAP authentication until the peer has authenticated itself to the router. The **no** form of this command specifies that the router will respond immediately to an authentication challenge.

Examples

The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. This example disables the default, meaning that users do not have to wait for peers to complete CHAP authentication before authenticating themselves.

```
interface bri 0
 encapsulation ppp
 no ppp chap wait
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.

Command	Description
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap refuse	Refuses CHAP authentication from peers requesting it.

ppp eap identity

To specify the Extensible Authentication Protocol (EAP) identity, use the **ppp eap identity** command in interface configuration mode. To remove the EAP identity from your configuration, use the **no** form of this command.

ppp eap identity *string*

no ppp eap identity *string*

Syntax Description

string	EAP identity.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use the **ppp eap identity** command to configure the client to use a different identity when requested by the peer.

Examples

The following example shows how to enable EAP on dialer interface 1 and set the identity to “cat”:

```
interface dialer 1
 encapsulation ppp
 ppp eap identity cat
```

ppp eap local

To authenticate locally instead of using the RADIUS back-end server, use the **ppp eap local** command in interface configuration mode. To reenable proxy mode (which is the default), use the **no** form of this command.

ppp eap local

no ppp eap local

Syntax Description

This command has no arguments or keywords.

Defaults

Authentication is performed via proxy mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

By default, Extensible Authentication Protocol (EAP) runs in proxy mode. This means that EAP allows the entire authentication process to be negotiated by the network access server (NAS) to a back-end server that may reside on or be accessed via a RADIUS server. To disable proxy mode (and thus to authenticate locally instead of via RADIUS), use the **ppp eap local** command.

In local mode, the EAP session is authenticated using the MD5 algorithm and obeys the same authentication rules as does Challenge Handshake Authentication Protocol (CHAP).

Examples

The following example shows how to configure EAP to authenticate locally:

```
interface dialer 1
 encapsulation ppp
 ppp authentication eap
 ppp eap local
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp eap password

To set the Enhanced Authentication Protocol (EAP) password for peer authentication, use the **ppp eap password** command in interface configuration mode. To disable the password, use the **no** form of this command.

ppp eap password [*number*] *string*

no ppp eap password [*number*] *string*

Syntax Description

number	(Optional) Encryption type, including values 0 through 7; 0 means no encryption.
string	Character string that specifies the EAP password.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

For remote EAP authentication only, you can configure your router to create a common EAP password to use in response to challenges from an unknown peer; for example, if your router calls a rotary of routers (either from another vendor or from an older running version of the Cisco IOS software) to which a new (that is, unknown) router has been added, the common password will be used to respond to the new router. The **ppp eap password** command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

Examples

The following example shows how to set the EAP password “7 141B1309” on the client:

```
ppp eap identity user
ppp eap password 7 141B1309
```

ppp eap refuse

To refuse Enhanced Authentication Protocol (EAP) from peers requesting it, use the **ppp eap refuse** command in interface configuration mode. To return to the default, use the **no** form of this command.

ppp eap refuse [**callin**]

no ppp eap refuse [**callin**]

Syntax Description

callin	(Optional) Authentication is refused for incoming calls only.

Defaults

The server will not refuse EAP authentication challenges received from the peer.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use the **ppp eap refuse** command to disable EAP authentication for all calls. If the **callin** keyword is used, the server will refuse to answer EAP authentication challenges received from the peer but will still require the peer to answer any EAP challenges the server sends.

Examples

The following example shows how to refuse EAP authentication on incoming calls from the peer:

```
ppp authentication eap
ppp eap local
ppp eap refuse callin
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp eap wait

To configure the server to delay the Enhanced Authentication Protocol (EAP) authentication until after the peer has authenticated itself to the server, use the **ppp eap wait** command in interface configuration mode. To disable this functionality, use the **no** form of this command.

ppp eap wait

no ppp eap wait

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use the **ppp eap wait** command to specify that the server will not authenticate to a peer requesting EAP authentication until after the peer has authenticated itself to the server.

Examples

The following example shows how to configure the server to wait for the peer to authenticate itself first:

```
ppp authentication eap
ppp eap local
ppp eap wait
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp pap refuse

To refuse a peer request to authenticate remotely with PPP using Password Authentication Protocol (PAP), use the **ppp pap refuse** command in interface configuration mode. To disable the refusal, use the **no** form of this command.

ppp pap refuse

no ppp pap refuse

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Use this command to refuse remote PAP support; for example, to respond to the peer request to authenticate with PAP.

This is a per-interface command.

Examples

The following example shows how to enable the **ppp pap** command to refuse a peer request for remote authentication:

```
interface dialer 0
 encapsulation ppp
 ppp pap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP and TACACS+.
encapsulation ppp	Sets PPP as the encapsulation method used by a serial or ISDN interface.
ppp authentication	Enables CHAP or PAP or both, and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp pap sent-username	Reenables remote PAP support for an interface and uses the **sent-username** and **password** in the PAP authentication request packet to the peer.

ppp pap sent-username

To reenable remote Password Authentication Protocol (PAP) support for an interface and use the **sent-username** and **password** in the PAP authentication request packet to the peer, use the **ppp pap sent-username** command in interface configuration mode. To disable remote PAP support, use the **no** form of this command.

ppp pap sent-username *username* **password** *password*

no ppp pap sent-username

Syntax Description

username	Username sent in the PAP authentication request.
password	Password sent in the PAP authentication request.
password	Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.

Defaults

Remote PAP support disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to reenable remote PAP support (for example, to respond to the peer's request to authenticate with PAP) and to specify the parameters to be used when sending the PAP authentication request.

This is a per-interface command. You must configure this command for each interface.

Examples

The following example identifies dialer interface 0 as the dialer rotary group leader and specify PPP as the method of encapsulation used by the interface. Authentication is by CHAP or PAP on received calls only. *ISPCorp* is the username sent to the peer if the peer requires the router to authenticate with PAP.

```
interface dialer0
 encapsulation ppp
 ppp authentication chap pap callin
 ppp chap hostname ISPCorp
 ppp pap sent username ISPCorp password 7 fjhfeu
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.

pre-shared-key

To define a preshared key to be used for Internet Key Exchange (IKE) authentication, use the **pre-shared-key** command in keyring configuration mode. To disable the preshared key, use the **no** form of this command.

pre-shared-key {**address** *address* [*mask*] | **hostname** *hostname*} **key** *key*

no pre-shared-key {**address** *address* [*mask*] | **hostname** *hostname*} **key** *key*

Syntax Description

address *address [mask]*	IP address of the remote peer or a subnet and mask. The *mask* argument is optional.
hostname *hostname*	Fully qualified domain name (FQDN) of the peer.
key *key*	Specifies the secret.

Defaults

No default behaviors or values

Command Modes

Keyring configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(2)T	This command was modified so that output for the **pre-shared-key** command will show that the preshared key is either encrypted or unencrypted.

Usage Guidelines

Before configuring preshared keys, you must configure an Internet Security Association and Key Management Protocol (ISAKMP) profile.

Output for the **pre-shared-key** command will show that the preshared key is either unencrypted or encrypted. An output example for an unencrypted preshared key would be as follows:

```
pre-shared-key address 10.1.0.1 key test123
```

An output example for a type 6 encrypted preshared key would be as follows:

pre-shared-key address 10.1.0.1 key 6 RHZE[JACMUI\bcbTdELISAAB

Examples

The following example shows how to configure a preshared key using an IP address and host name:

```
Router (config)# crypto keyring vpnkeyring
Router (config-keyring)# pre-shared-key address 10.72.23.11 key vpnkey
Router (config-keyring)# pre-shared-key hostname www.vpn.com key vpnkey
```

primary

To assign a specified trustpoint as the primary trustpoint of the router, use the **primary** command in ca-trustpoint configuration mode.

primary *name*

Syntax Description

name	Name of the primary trustpoint of the router.

Defaults

No default behavior or values.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **primary** command to specify a given trustpoint as primary.

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which defines the trustpoint and enters ca-trustpoint configuration mode.

Examples

The following example shows how to configure the trustpoint “ka” as the primary trustpoint:

```
crypto ca trustpoint ka
 enrollment url http://xxx
 primary
 crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

privilege

To configure a new privilege level for users and associate commands with that privilege level, use the **privilege** command in global configuration mode. To revert to default privileges for the specified commands, use the **no** form of this command.

privilege *mode* [**all**] {**level** *level* | **reset**} *command-string*

no privilege *mode* [**all**] {**level** *level* | **reset**} *command-string*

Syntax Description

mode	Configuration mode for the specified command. See Table 28 in the "Usage Guidelines" section for a list of options for this argument.
all	(Optional) Changes the privilege level for all the suboptions to the same level.
level *level*	Specifies the privilege level you are configuring for the specified command or commands. The level argument must be a number from 0 to 15.
reset	Resets the privilege level of the specified command or commands to the default and removes the privilege level configuration from the running-config file. **Note** If you use the **no** form of this command to reset the privilege level to the default, the default form of this command will still appear in the configuration file. To completely remove a privilege configuration, use the **reset** keyword.
command-string	Command associated with the specified privilege level. If the **all** keyword is used, specifies the command and subcommands associated with the privilege level.

Defaults

User EXEC mode commands are privilege level 1.

Privileged EXEC mode and configuration mode commands are privilege level 15.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(22)S, 12.2(13)T	The **all** keyword was added.

Usage Guidelines

The password for a privilege level defined using the **privilege** global configuration command is configured using the **enable secret** command.

Level 0 can be used to specify a more-limited subset of commands for specific users or lines. For example, you can allow user "guest" to use only the **show users** and **exit** commands.

Note There are five commands associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included.

When you set the privilege level for a command with multiple words, note that the commands starting with the first word will also have the specified access level. For example, if you set the **show ip route** command to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15—unless you set them individually to different levels. This is necessary because you can't execute, for example, the **show ip** command unless you have access to **show** commands.

To change the privilege level of a group of commands, use the **all** keyword. When you set a group of commands to a privilege level using the **all** keyword, all commands which match the beginning string are enabled for that level, and all commands which are available in submodes of that command are enabled for that level. For example, if you set the **show ip** keywords to level 5, show and ip will be changed to level 5 and all the options that follow the **show ip** string (such as **show ip accounting**, **show ip aliases**, **show ip bgp**, and so on) will be available at privilege level 5.

Table 28 shows some of the keyword options for the mode argument in the **privilege** command. The available mode keywords will vary depending on your hardware and software version. To see a list of available mode options on your system, use the **privilege ?** command.

Table 28 Keyword Options for the Mode Argument

Command	Description
accept-dialin	VPDN group accept dialin configuration mode
accept-dialout	VPDN group accept dialout configuration mode
address-family	Address Family configuration mode
alps-ascu	ALPS ASCU configuration mode
alps-circuit	ALPS circuit configuration mode
atm-bm-config	ATM bundle member configuration mode
atm-bundle-config	ATM bundle configuration mode
atm-vc-config	ATM virtual circuit configuration mode
atmsig_e164_table_mode	ATMSIG E164 Table
cascustom	Channel-associated signalling (cas) custom configuration mode
config-rtr-http	RTR HTTP raw request Configuration
configure	Global configuration mode
controller	Controller configuration mode
crypto-map	Crypto map config mode
crypto-transform	Crypto transform config modeCrypto transform configuration mode
dhcp	DHCP pool configuration mode
dspfarm	DSP farm configuration mode
exec	Exec mode
flow-cache	Flow aggregation cache configuration mode

Table 28 Keyword Options for the Mode Argument

Command	Description
gateway	Gateway configuration mode
interface	Interface configuration mode
interface-dlci	Frame Relay DLCI configuration mode
ipenacl	IP named extended access-list configuration mode
ipsnacl	IP named simple access-list configuration mode
ip-vrf	Configure IP VRF parameters
lane	ATM Lan Emulation Lecs Configuration Table
line	Line configuration mode
map-class	Map class configuration mode
map-list	Map list configuration mode
mpoa-client	MPOA Client
mpoa-server	MPOA Server
null-interface	Null interface configuration mode
preaut	AAA Preauth definitions
request-dialin	VPDN group request dialin configuration mode
request-dialout	VPDN group request dialout configuration mode
route-map	Route map configuration mode
router	Router configuration mode
rsvp_policy_local	
rtr	RTR Entry Configuration
sg-radius	RADIUS server group definition
sg-tacacs+	TACACS+ server group
sip-ua	SIP UA configuration mode
subscriber-policy	Subscriber policy configuration mode
tcl	Tcl mode
tdm-conn	TDM connection configuration mode
template	Template configuration mode
translation-rule	Translation Rule configuration mode
vc-class	VC class configuration mode
voiceclass	Voice Class configuration mode
voiceport	Voice configuration mode
voipdialpeer	Dial Peer configuration mode
vpdn-group	VPDN group configuration mode

Examples

The following example shows how to set the **configure** command to privilege level 14 and establish SecretPswd14 as the password users must enter to use level 14 commands:

```
privilege exec level 14 configure
enable secret level 14 SecretPswd14
```

The following example shows how to set the **show and ip** keywords to level 5. The suboptions coming under **ip** will also be allowed to users with privilege level 5 access:

```
Router(config)# privilege exec all level 5 show ip
```

The following two examples demonstate the difference in behavior between the **no** form of the command and the use of the **reset** keyword.

```
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 3 configure terminal
privilege exec level 3 configure

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no privilege exec level 3 configure terminal
Router(config)# end
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 15 configure terminal
privilege exec level 15 configure
```

Note that in the **show running-config** output above, the privilege command for "configure terminal" still appears, but now has the default privilege level assigned.

To remove a previously configured privilege command entirely from the configuration, use the **reset** keyword, as shown in the following example:

```
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 3 configure terminal
privilege exec level 3 configure

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# privilege exec reset configure terminal
Router(config)#
Router# show running-config | include priv
privilege configure all level 3 interface
Router#
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the **enable password** command.
privilege level	Sets the default privilege level for a line.

privilege level

To set the default privilege level for a line, use the **privilege level** command in line configuration mode. To restore the default user privilege level to the line, use the **no** form of this command.

privilege level *level*

no privilege level

Syntax Description

level	Privilege level associated with the specified line.

Defaults

Level 15 is the level of access permitted by the enable password.

Level 1 is normal EXEC-mode user privileges.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Users can override the privilege level you set using this command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the **disable** command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level.

You can use level 0 to specify a subset of commands for specific users or lines. For example, you can allow user "guest" to use only the **show users** and **exit** commands.

You might specify a high level of privilege for your console line to restrict line usage.

Examples

The following example configures the auxiliary line for privilege level 5. Anyone using the auxiliary line has privilege level 5 by default:

```
line aux 0
 privilege level 5
```

The following example sets all **show ip** commands, which includes all **show** commands, to privilege level 7:

```
privilege exec level 7 show ip route
```

This is equivalent to the following command:

```
privilege exec level 7 show
```

The following example sets the **show ip route** to level 7 and the **show** and **show ip** commands to level 1:

```
privilege exec level 7 show ip route
privilege exec level 1 show ip
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.

qos-group

To apply a quality of service (QoS) group value to an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **qos-group** command in ISAKMP profile configuration mode. To disable the group value, use the **no** form of this command.

qos-group *group-number*

no qos-group *group-number*

Syntax Description

group-number	Number of the group number. The value ranges from 1 through 99. (There is no default value.)

Defaults

A QoS group value is not applied to an ISAKMP profile.

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

If there is no matching QoS group set in a QoS policy, or if a service policy is not configured or applied to an interface that also has a crypto map applied, the ISAKMP profile setting (using the **qos-group** command) is not enforced.

Examples

The following example shows that QoS group "2" has been applied to the ISAKMP profile "class1":

```
Router (config)# crypto isakmp profile class1
Router (conf-isa-prof)# qos-group 2
! A profile is deemed incomplete until it has match identity statements.
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.

query certificate

To configure query certificates on a per-trustpoint basis, use the **query certificate** command in ca-trustpoint configuration mode. To disable creation of query certificates per trustpoint, use the **no** form of this command.

query certificate

no query certificate

Syntax Description

This command has no arguments or keywords.

Defaults

Query certificates are stored in NVRAM.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Normally, certain certificates are stored locally in the router's NVRAM, and each certificate uses a moderate amount of memory. To save NVRAM space, you can use this command to prevent certificates from being stored locally; instead, they are retrieved from a specified certification authority (CA) trustpoint when needed. This will save NVRAM space but could result in a slight performance impact.

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which puts you in ca-trustpoint configuration mode.

Using the query certificate Command with a Specific Trustpoint

When the **query certificate** command is used, certificates associated with the specified truspoint will not be written into NVRAM, and the certificate query will be attempted during the next reload of the router.

Applying the Query Mode Globally

When the global command **crypto ca certificate query** command is used, the query certificate will be added to all trustpoints on the router. When the **no crypto ca certicate query** command is used, any previously query certificate configuration will be removed from all trustpoints, and any query in progress will be halted and the feature disabled.

Examples

The following example shows how to configure a trustpoint and initiate query mode for certificate authority:

```
crypto ca trustpoint trustpoint1
 enrollment url http://trustpoint1
 crl query ldap://trustpoint1
```

```
query certificate
exit
```

Related Commands

Command	Description
crypto ca certificate query	Specifies that certificates should not be stored locally but retrieved from a CA trustpoint.
crypto ca trustpoint	Declares the CA that your router should use.

query url

The **query url** command is replaced by the **crl** command. See the **crl** command for more information.

quit

To exit from the key-string mode while defining the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signatures during Internet Key Exchange (IKE) authentication, use the **quit** command in public key configuration mode.

quit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Public key configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use this command to exit text mode while defining the RSA public key.

Examples

The following example shows that the RSA public key of an IP Security (IPSec) peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer that you will manually configure.
key-string (IKE)	Specifies the RSA public key of a remote peer.

radius-server attribute 11 direction default

To specify the default direction of filters from RADIUS, use the **radius-server attribute 11 direction default** command in global configuration mode. To remove this functionality from your configuration, use the **no** form of this command.

radius-server attribute 11 direction default [**inbound** | **outbound**]

no radius-server attribute 11 direction default [**inbound** | **outbound**]

Syntax Description

inbound	(Optional) Filtering is applied to inbound packets only.
outbound	(Optional) Filtering is applied to outbound packets only.

Defaults

If this command is not enabled, filters are treated as outbound.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use the **radius-server attribute 11 direction default** command to change the default direction of filters from RADIUS. (RADIUS attribute 11 (Filter-Id) indicates the name of the filter list for the user.) Enabling this command allows you to change the filter direction to inbound, which stops traffic from entering a router and prevents resource consumption, rather than keeping the outbound default direction, which waits until the traffic is about to leave the network before filtering occurs.

Examples

The following example shows how to configure RADIUS attribute 11 to change the default direction of filters. In this example, the filtering is applied to inbound packets only.

```
radius-server attribute 11 direction default inbound
```

The following is an example of a RADIUS user profile (Merit Daemon format) that includes RADIUS attribute 11 (Filter-Id):

```
client Password = "cisco"
        Service-Type = Framed,
        Framed-Protocol = PPP,
        Filter-Id = "myfilter.out"
```

radius-server attribute 188 format non-standard

To send the number of remaining links in the multilink bundle in the accounting-request packet, use the **radius-server attribute 188 format non-standard** command in global configuration mode. To disable the sending of the number of links in the multilink bundle in the accounting-request packet, use the **no** form of this command.

radius-server attribute 188 format non-standard

no radius-server attribute 188 format non-standard

Syntax Description

This command has no arguments or keywords.

Defaults

RADIUS attribute 188 is not sent in accounting “start” and “stop” records.

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Use this command to send attribute 188 in accounting “start” and “stop” records.

Examples

The following example shows a configuration that sends RADIUS attribute 188 in accounting-request packets:

```
radius-server attribute 188 format non-standard
```

radius-server attribute 32 include-in-access-req

To send RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request, use the **radius-server attribute 32 include-in-access-req** command in global configuration mode. To disable sending RADIUS attribute 32, use the **no** form of this command.

radius-server attribute 32 include-in-access-req [*format*]

no radius-server attribute 32 include-in-access-req

Syntax Description

format	(Optional) A string sent in attribute 32 containing an IP address (%i), a hostname (%h), or a domain name (%d).

Defaults

RADIUS attribute 32 is not sent in access-request or accounting-request packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1 T	This command was introduced.

Usage Guidelines

Using the **radius-server attribute 32 include-in-access-req** command makes it possible to identify the network access server (NAS) manufacturer to the RADIUS server by sending RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request. If you configure the format argument, the string sent in attribute 32 will include an IP address, a hostname, or a domain name; otherwise, the Fully Qualified Domain Name (FQDN) is sent by default.

Examples

The following example shows a configuration that sends RADIUS attribute 32 in the access-request with the format configured to identify a Cisco NAS:

```
radius-server attribute 32 include-in-access-req format cisco %h.%d %i
! The following string will be sent in attribute 32 (NAS-Identifier).
"cisco router.nlab.cisco.com 10.0.1.67"
```

radius-server attribute 4

To configure an IP address for the RADIUS attribute 4 address, use the **radius-server attribute 4** command in global configuration mode. To delete an IP address as the RADIUS attribute 4 address, use the **no** form of this command.

radius-server attribute 4 *ip-address*

no radius-server attribute 4 *ip-address*

Syntax Description

ip-address	IP address to be configured as RADIUS attribute 4 inside RADIUS packets.

Defaults

If this command is not configured, the RADIUS NAS-IP-Address attribute will be the IP address on the interface that connects the network access server (NAS) to the RADIUS server.

Command Modes

Global configuration

Command History

Release	Modification
12.3(3)B	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Normally, when the **ip radius-source interface** command is configured, the IP address on the interface that is specified in the command is used as the IP address in the IP headers of the RADIUS packets and as the RADIUS attribute 4 address inside the RADIUS packets.

However, when the **radius-server attribute 4** command is configured, the IP address in the command is used as the RADIUS attribute 4 address inside the RADIUS packets. There is no impact on the IP address in the IP headers of the RADIUS packets.

If both commands are configured, the IP address that is specified in the **radius-server attribute 4** command is used as the RADIUS attribute 4 address inside the RADIUS packets. The IP address on the interface that is specified in the **ip radius-source interface** command is used as the IP address in the IP headers of the RADIUS packets.

Some authentication, authorization, and accounting (AAA) clients (such as PPP, virtual private dial-up network [VPDN] or Layer 2 Tunneling Protocol [L2TP], Voice over IP [VoIP], or Service Selection Gateway [SSG]) may try to set the RADIUS attribute 4 address using client-specific values. For example, on an L2TP network server (LNS), the IP address of the L2TP access concentrator (LAC) could be specified as the RADIUS attribute 4 address using a VPDN or L2TP command. When the **radius-server attribute 4** command is configured, the IP address specified in the command takes precedence over all IP addresses from AAA clients.

During RADIUS request retransmission and during RADIUS server failover, the specified IP address is always chosen as the value of the RADIUS attribute 4 address.

Examples

The following example shows that the IP address 10.0.0.21 has been configured as the RADIUS NAS-IP-Address attribute:

```
radius-server attribute 4 10.0.0.21
radius-server host 10.0.0.10 auth-port 1645 acct-port 1646 key cisco
```

The following **debug radius** command output shows that 10.0.0.21 has been successfully configured.

```
Router# debug radius

RADIUS/ENCODE(0000001C): acct_session_id: 29
RADIUS(0000001C): sending
RADIUS(0000001C): Send Access-Request to 10.0.0.10:1645 id 21645/17, len 81
RADIUS:  authenticator D0 27 34 C0 F0 C4 1C 1B - 3C 47 08 A2 7E E1 63 2F
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   18  "shashi@pepsi.com"
RADIUS:  CHAP-Password       [3]   19  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.0.0.21
UDP: sent src=11.1.1.1(21645), dst=10.0.0.10(1645), length=109
UDP: rcvd src=10.0.0.10(1645), dst=10.1.1.1(21645), length=40
RADIUS: Received from id 21645/17 10.0.0.10:1645, Access-Accept, len 32
RADIUS:  authenticator C6 99 EC 1A 47 0A 5F F2 - B8 30 4A 4C FF 4B 1D F0
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS(0000001C): Received from id 21645/17
```

Related Commands

Command	Description
ip radius-source interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.

radius-server attribute 44 extend-with-addr

To add the accounting IP address before the existing session ID, use the **radius-server attribute 44 extend-with-addr** command in global configuration mode. To remove this command from your configuration, use the **no** form of this command.

radius-server attribute 44 extend-with-addr

no radius-server attribute 44 extend-with-addr

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

The **radius-server attribute 44 extend-with-addr** command adds Acct-Session-Id (attribute 44) before the existing session ID (NAS-IP-Address).

When multiple network access servers (NAS) are being processed by one offload server, enable this command on all NASs and the offload server to ensure a common and unique session ID.

Note This command should be enabled only when offload servers are used.

Examples

The following example shows how to configure unique session IDs among NASs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 extend-with-addr
```

Related Commands

Command	Description
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Acct-Session-Id) in access-request packets before user authentication.
radius-server attribute 44 sync-with-client	Configures the offload server to synchronize accounting session information with the NAS clients.

radius-server attribute 44 include-in-access-req

To send RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication), use the **radius-server attribute 44 include-in-access-req** command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

radius-server attribute 44 include-in-access-req [**vrf** *vrf-name*]

no radius-server attribute 44 include-in-access-req [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Per VRF configuration.

Defaults

RADIUS attribute 44 is not sent in access-request packets.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

There is no guarantee that the Accounting Session IDs will increment uniformly and consistently. In other words, between two calls, the Accounting Session ID can increase by more than one.

The **vrf** *vrf-name* keyword and argument specify Accounting Session IDs per Virtual Private Network (VPN) routing and forwarding (VRF), which allows multiple disjoined routing or forwarding tables, where the routes of a user have no correlation with the routes of another user.

Examples

The following example shows a configuration that sends RADIUS attribute 44 in access-request packets:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
```

radius-server attribute 44 sync-with-client

To configure the offload server to synchronize accounting session information with the network access server (NAS) clients, use the **radius-server attribute 44 sync-with-client** command in global configuration mode. To disable this functionality, use the **no** form of this command.

radius-server attribute 44 sync-with-client

no radius-server attribute 44 sync-with-client

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use the **radius-server attribute 44 sync-with-client** command to allow the offload server to synchronize accounting session information with the NAS clients. The NAS-IP-Address, the Acct-Session-Id, and the Class attribute are transmitted from the client to the offload server via Layer 2 Forwarding (L2F) options.

Examples

The following example shows how to configure the offload server to synchronize accounting session information with the NAS clients:

```
radius-server attribute 44 sync-with-client
```

Related Commands

Command	Description
radius-server attribute 44 extend-with-addr	Adds the accounting IP address before the existing session ID.
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Acct-Session-Id) in access-request packets before user authentication.

radius-server attribute 55 include-in-acct-req

To send the RADIUS attribute 55 (Event-Timestamp) in accounting packets, use the **radius-server attribute 55 include-in-acct-req** command in global configuration mode. To remove this command from your configuration, use the **no** form of this command.

radius-server attribute 55 include-in-acct-req

no radius-server attribute 55 include-in-acct-req

Syntax Description

This command has no arguments or keywords.

Defaults

RADIUS attribute 55 is not sent in accounting packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

Use the **radius-server attribute 55 include-in-acct-req** command to send RADIUS attribute 55 (Event-Timestamp) in accounting packets. The Event-Timestamp attribute records the time that the event occurred on the NAS; the timestamp sent in attribute 55 is in seconds since January 1, 1970 00:00 UTC.

Note Before the Event-Timestamp attribute can be sent in accounting packets, you *must* configure the clock on the router. (For information on setting the clock on your router, refer to section "Performing Basic System Management" in the chapter "System Management" of the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*.)

To avoid configuring the clock on the router every time the router is reloaded, you can enable the **clock calendar-valid** command. (For information on this command, refer to the *Cisco IOS Configuration Fundamentals and Network Management Command Reference.*)

Examples

The following example shows how to enable your router to send the Event-Timestamp attribute in accounting packets. (To see whether the Event-Timestamp was successfully enabled, use the **debug radius** command.)

```
radius-server attribute 55 include-in-acct-req
```

Related Commands

Command	Description
clock calendar-valid	Configures a system as an authoritative time source for a network based on its hardware clock (calendar).
clock set	Manually sets the system software clock.

radius-server attribute 6

To provide for the presence of the Service-Type attribute (attribute 6) in RADIUS Access-Accept messages, use the **radius-server attribute 6** command in global configuration mode. To make the presence of the Service-Type attribute optional in Access-Accept messages, use the **no** form of this command.

radius-server attribute 6 {mandatory | on-for-login-auth | support-multiple | voice *value***}**

no radius-server attribute 6 {mandatory | on-for-login-auth | support-multiple | voice *value***}**

Syntax Description

mandatory	Makes the presence of the Service-Type attribute mandatory in RADIUS Access-Accept messages.
on-for-login-auth	Sends the Service-Type attribute in the authentication packets. **Note** The Service-Type attribute is sent by default in RADIUS Accept-Request messages. Therefore, RADIUS tunnel profiles should include "Service-Type=Outbound" as a check item, not just as a reply item. Failure to include Service-Type=Outbound as a check item can result in a security hole.
support-multiple	Supports multiple Service-Type values for each RADIUS profile.
voice *value*	Selects the Service-Type value for voice calls. The only value that can be entered is 1. The default is 12.

Defaults

If this command is not configured, the absence of the Service-Type attribute is ignored, and the authentication or authorization does not fail. The default for the **voice** keyword is 12.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(13)T	The **mandatory** keyword was added.

Usage Guidelines

If this command is configured and the Service-Type attribute is absent in the Access-Accept message packets, the authentication or authorization fails.

Examples

The following example shows that the presence of the Service-Type attribute is mandatory in RADIUS Access-Accept messages:

```
Router (config)# radius-server attribute 6 mandatory
```

The following example shows that attribute 6 is to be sent in authentication packets:

```
Router (config)# radius-server attribute 6 on-for-login-auth
```

The following example shows that multiple Service-Type values are to be supported for each RADIUS profile:

```
Router (config)# radius-server attribute support-multiple
```

The following example shows that Service-Type values are to be sent in voice calls:

```
Router (config)# radius-server attribute voice 1
```

radius-server attribute 69 clear

To receive nonencrypted tunnel passwords in attribute 69 (Tunnel-Password), use the **radius-server attribute 69 clear** command in global configuration mode. To disable this feature and receive encrypted tunnel passwords, use the **no** form of this command.

radius-server attribute 69 clear

no radius-server attribute 69 clear

Syntax Description

This command has no arguments or keywords.

Defaults

RADIUS attribute 69 is not sent and encrypted tunnel passwords are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

Use the **radius-server attribute 69 clear** command to receive nonencrypted tunnel passwords, which are sent in RADIUS attribute 69 (Tunnel-Password). This command allows tunnel passwords to be sent in a "string" encapsulated format, rather than the standard tag/salt/string format, which enables the encrypted tunnel password.

Some RADIUS servers do not encrypt Tunnel-Password; however the current NAS (network access server) implementation will decrypt a non-encrypted password that causes authorization failures. Because nonencrypted tunnel passwords can be sent in attribute 69, the NAS will no longer decrypt tunnel passwords.

Note Once this command is enabled, all tunnel passwords received will be nonencrypted until the command is manually disabled.

Examples

The following example shows how to enable attribute 69 to receive nonencrypted tunnel passwords. (To see whether the Tunnel-Password process is successful, use the **debug radius** command.)

```
radius-server attribute 69 clear
```

radius-server attribute 77

To send connection speed information to the RADIUS server in the access request, use the **radius-server attribute 77** command in global configuration mode. To prevent connection speed information from being included in the access request, use the **no** form of this command.

radius-server attribute 77 {include-in-access-req | include-in-acct-req}

no radius-server attribute 77 {include-in-access-req | include-in-acct-req}

Syntax Description

include-in-access-req	Specifies that attribute 77 will be included in access requests.
include-in-acct-req	Specifies that attribute 77 will be included in accounting requests.

Defaults

RADIUS attribute 77 is sent to the RADIUS server in the access request.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)BX	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

RADIUS attribute 77 is sent to the RADIUS server in the access request by default.

RADIUS attribute 77 allows RADIUS authentication based on connection speed. Sessions can be accepted or denied based on the allowed connection speed configured for a particular user on the RADIUS server.

RADIUS attribute 77 includes the following information:

- The accounting start/stop request
- The VC class name defined with the **class-int** command
- The VC class name defined with the **class-vc** command
- The VC class name defined with the **class-range** command

The VC class name may include letters, numbers, and the characters ":" (colon), ";" (semicolon), "-" (hyphen) and "," (comma).

Examples

The following example disables the inclusion of RADIUS attribute 77 in the access request:

```
no radius-server attribute 77 include-in-access-req
```

Related Commands

Command	Description
class-int	Assigns a VC class to an ATM main interface or subinterface.
class-range	Assigns a VC class to an ATM PVC range.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.

radius-server attribute 8 include-in-access-req

To send the IP address of a user to the RADIUS server in the access request, use the **radius-server attribute 8 include-in-access-req** command in global configuration mode. To disable sending of the user IP address to the RADIUS server during authentication, use the **no** form of this command.

radius-server attribute 8 include-in-access-req

no radius-server attribute 8 include-in-access-req

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Using the **radius-server attribute 8 include-in-access-req** command makes it possible for a network access server (NAS) to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and addresses. Using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication.

When a network device dials in to a NAS that is configured for RADIUS authentication, the NAS begins the process of contacting the RADIUS server in preparation for user authentication. Typically, the IP address of the dial-in host is not communicated to the RADIUS server until after successful user authentication. Communicating the device IP address to the server in the RADIUS access request allows other applications to begin to take advantage of that information.

As the NAS is setting up communication with the RADIUS server, the NAS assigns an IP address to the dial-in host from a pool of IP addresses configured at the specific interface. The NAS sends the IP address of the dial-in host to the RADIUS server as attribute 8. At that time, the NAS sends other user information, such as the username, to the RADIUS server.

After the RADIUS server receives the user information from the NAS, it has two options:

- If the user profile on the RADIUS server already includes attribute 8, the RADIUS server can override the IP address sent by the NAS with the IP address defined as attribute 8 in the user profile. The address defined in the user profile is returned to the NAS.
- If the user profile does not include attribute 8, the RADIUS server can accept attribute 8 from the NAS, and the same address is returned to the NAS.

The address returned by the RADIUS server is saved in memory on the NAS for the life of the session. If the NAS is configured for RADIUS accounting, the accounting start packet sent to the RADIUS server includes the same IP address as in attribute 8. All subsequent accounting packets, updates (if configured), and "stop" packets will also include the same IP address as in attribute 8.

Note Configuring the NAS to send the host IP address in the RADIUS access request assumes that the login host is configured to request an IP address from the NAS server. It also assumes that the login host is configured to accept an IP address from the NAS. In addition, the NAS must be configured with a pool of network addresses at the interface supporting the login hosts.

Examples

The following example shows a NAS configuration that sends the IP address of the dial-in host to the RADIUS server in the RADIUS access request. The NAS is configured for RADIUS authentication, authorization, and accounting (AAA). A pool of IP addresses (async1-pool) has been configured and applied at interface Async1.

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
ip address-pool local
!
interface Async1
 peer default ip address pool async1-pool
!
ip local pool async1-pool 209.165.200.225 209.165.200.229
!
radius-server host 172.31.71.146 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 8 include-in-access-req
radius-server key radhost
```

radius-server attribute list

To define an accept or reject list name, use the **radius-server attribute list** command in global configuration mode. To remove an accept or reject list name from your configuration, use the no form of this command.

radius-server attribute list *list-name*

no radius-server attribute list *list-name*

Syntax Description

list-name	Name for an accept or reject list.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401 ASR.

Usage Guidelines

A user may configure an accept or reject list with a selection of attributes on the network access server (NAS) for authorization or accounting so unwanted attributes are not accepted and processed. The **radius-server attribute list** command allows users to specify a name for an accept or reject list. This command is used in conjunction with the **attribute** (server-group configuration) command, which adds attributes to an accept or reject list.

Note The listname must be the same as the listname defined in the **accounting** or **authorization** configuration command.

Examples

The following example shows how to configure the reject list “bad-author” for RADIUS authorization and accept list “usage-only” for RADIUS accounting:

```
Router(config)# aaa new-model
Router(config)# aaa authentication ppp default group radius-sg
Router(config)# aaa authorization network default group radius-sg
Router(config)# aaa group server radius radius-sg
Router(config-sg-radius)# server 1.1.1.1
Router(config-sg-radius)# authorization reject bad-author
Router(config-sg-radius)# accounting accept usage-only
Router(config-sg-radius)# exit
```

```
Router(config)# radius-server host 1.1.1.1 key mykey1
Router(config)# radius-server attribute list usage-only
Router(config-radius-attrl)# attribute 1,40,42-43,46
Router(config-radius-attrl)# exit
Router(config)# radius-server attribute list bad-author
Router(config-radius-attrl)# attribute 22,27-28,56-59
```

Note Although you cannot configure more than one access or reject list per server group for authorization or accounting, you can configure one list for authorization and one list for accounting per server group.

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server host	Specifies a RADIUS server host.

radius-server attribute nas-port extended

The **radius-server attribute nas-port extended** command is replaced by the **radius-server attribute nas-port format** command. See the description of the **radius-server attribute nas-port format** command for more information.

radius-server attribute nas-port format

To select the NAS-Port format used for RADIUS accounting features, and to restore the default NAS-Port format, use the **radius-server attribute nas-port format** command in global configuration mode. To stop sending attribute 5 (NAS-Port) to the RADIUS server, use the **no** form of this command.

radius-server attribute nas-port format *format*

no radius-server attribute nas-port format *format*

Syntax Description

format	NAS-Port format. Possible values for the format argument are as follows: **a**—Standard NAS-Port format **b**—Extended NAS-Port format **c**—Carrier-based format **d**—PPPoX (PPP over Ethernet or PPP over ATM) extended NAS-Port format **e**—Configurable NAS-Port format

Defaults

Standard NAS-Port format

Command Modes

Global configuration

Command History

Release	Modification
11.3(7)T	This command was introduced.
11.3(9)DB	The PPP extended NAS-Port format was added.
12.1(5)T	The PPP extended NAS-Port format was expanded to support PPPoE over ATM and PPPoE over IEEE 802.1Q virtual LANS (VLANs).
12.2(4)T	Format **e** was introduced.
12.2(11)T	Format **e** was extended to support PPPoX information.
12.3(3)	Format **e** was extended to support Session ID U.

Usage Guidelines

The **radius-server attribute nas-port format** command configures RADIUS to change the size and format of the NAS-Port attribute field (RADIUS IETF attribute 5).

The following NAS-Port formats are supported:

- Standard NAS-Port format—This 16-bit NAS-Port format indicates the type, port, and channel of the controlling interface. This is the default format used by Cisco IOS software.
- Extended NAS-Port format—The standard NAS-Port attribute field is expanded to 32 bits. The upper 16 bits of the NAS-Port attribute display the type and number of the controlling interface; the lower 16 bits indicate the interface that is undergoing authentication.

- Shelf-slot NAS-Port format—This 16-bit NAS-Port format supports expanded hardware models requiring shelf and slot entries.
- PPP extended NAS-Port format—This NAS-Port format uses 32 bits to indicate the interface, virtual path identifier (VPI), and virtual channel indicator (VCI) for PPP over ATM and PPPoE over ATM, and the interface and VLAN ID for PPPoE over Institute of IEEE standard 802.1Q VLANs.

Format e

The currently supported formats **a** through **c** do not work with new Cisco platforms, such as the AS5400. For this reason, a configurable format **e** was developed. Format **e** requires you to explicitly define the usage of the 32 bits of attribute 25 (Nas-Port). The usage is defined with a given parser character for each Nas-Port field of interest for a given bit field. By configuring a single character in a row, such as x, only one bit is assigned to store that given value. Additional characters of the same type, such as x, will provide a larger available range of values to be stored. Thus, the ranges may be expanded as follows:

x	0 – 1
xx	0 – 3
xxx	0 – 7
xxxx	0 – F
xxxxx	0 – 1F

and so on.

It is imperative that one know what the valid range is for a given parameter on a platform that one wishes to support. The IOS RADIUS client will bitmask the determined value to the maximum permissible value on the basis of configuration. Thus, if one has a parameter that turns out to have a value of 8, but only 3 bits (xxx) are configures, 8 and 0x7 will give a result of 0. Therefore, one must always configure enough bits to correctly capture the value required. Care must be taken to ensure that format **e** is configured to properly work for all NAS port types within your network environment.

Currently supported parameters and their representative characters are shown below.

Zero	0 (always sets a 0 to that bit)
One	1 (always sets a 1 to that bit)
DS0 shelf	f
DS0 slot	s
DS0 adapter	a
DS0 port	p (physical port)
DS0 subinterface	i
DS0 channel	c
Async shelf	F
Async slot	S
Async port	P
Async line	L (modem line number, that is, physical terminal [TTY] number)
PPPoX slot	S
PPPoX adapter	A
PPPoX port	P
PPPoX VLAN ID	V

PPPoX VPI	I
PPPoX VCI	C
Session ID	U

All 32 bits that represent the NAS-Port must be set to one of the above characters because this format makes no assumptions for empty fields.

Access Router

The DS0 port on a T1-based card and on a T3-based card will give different results. On T1-based cards, the physical port is equal to the virtual port (as these are the same). So, **p** and **d** will give the same information for a T1 card. However, on a T3 system, the port will give you the physical port number (as there can be more than one T3 card for a given platform). As such, **d** will give you the virtual T1 line (as per configuration on a T3 controller). On a T3 system, **p** and **d** will be different, and one should capture both to properly identify the physical device. As a working example for the Cisco AS5400, the following configuration is recommended:

```
Router (config)# radius-server attribute nas-port format e
SSSSPPPPPPPPPssssppppddddccccc
```

This will give one an asynchronous slot (0 – 16), asynchronous port (0 – 512), DS0 slot (0 – 16), DS0 physical port (0 – 32), DS0 virtual port (0 – 32), and channel (0 – 32). The parser has been implemented to explicitly require 32-bit support, or it will fail.

Finally, format **e** is supported for channel-associated signaling (CAS), Primary Rate Interface (PRI), and basic rate interface- (BRI-) based interfaces.

Note This command replaces the **radius-server attribute nas-port extended** command.

Examples

In the following example, a RADIUS server is identified, and the NAS-Port field is set to the PPP extended format:

```
radius-server host 172.31.5.96 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
```

Related Commands

Command	Description
vpdn aaa attribute nas-port vpdn-nas	Enables the LNS to send PPP extended NAS-Port format values to the RADIUS server for accounting.

radius-server authorization missing Service-Type

The **radius-server authorization missing Service-Type** command is replaced by the **radius-server attribute 6** command. See the **radius-server attribute 6** command for more information.

radius-server challenge-noecho

To prevent user responses to Access-Challenge packets from being displayed on the screen, use the **radius-server challenge-noecho** command in global configuration mode. To return to the default condition, use the **no** form of this command.

radius-server challenge-noecho

no radius-server challenge-noecho

Syntax Description

This command has no arguments or keywords.

Defaults

All user responses to Access-Challenge packets are echoed to the screen.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

This command applies to all users. When the **radius-server challenge-noecho** command is configured, user responses to Access-Challenge packets are not displayed unless the Prompt attribute in the user profile is set to *echo* on the RADIUS server. The Prompt attribute in a user profile overrides the **radius-server challenge-noecho** command for the individual user. For more information, see the chapter "Configuring RADIUS" in the *Cisco IOS Security Configuration Guide*.

Examples

The following example stops all user responses from displaying on the screen:

```
radius-server challenge-noecho
```

radius-server configure-nas

To have the Cisco router or access server query the vendor-proprietary RADIUS server for the static routes and IP pool definitions used throughout its domain when the device starts up, use the **radius-server configure-nas** command in global configuration mode. To discontinue the query of the RADIUS server, use the **no** form of this command.

radius-server configure-nas

no radius-server configure-nas

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Use the **radius-server configure-nas** command to have the Cisco router query the vendor-proprietary RADIUS server for static routes and IP pool definitions when the router first starts up. Some vendor-proprietary implementations of RADIUS let the user define static routes and IP pool definitions on the RADIUS server instead of on each individual network access server in the network. As each network access server starts up, it queries the RADIUS server for static route and IP pool information. This command enables the Cisco router to obtain static routes and IP pool definition information from the RADIUS server.

Note Because the **radius-server configure-nas** command is performed when the Cisco router starts up, it will not take effect until you issue a **copy system:running-config nvram:startup-config** command.

Examples

The following example shows how to tell the Cisco router or access server to query the vendor-proprietary RADIUS server for already-defined static routes and IP pool definitions when the device first starts up:

```
radius-server configure-nas
```

Related Commands

Command	Description
radius-server host non-standard	Identifies that the security server is using a vendor-proprietary implementation of RADIUS.

radius-server dead-criteria

To force one or both of the criteria—used to mark a RADIUS server as dead—to be the indicated constant, use the **radius-server dead-criteria** command in global configuration mode. To disable the criteria that were set, use the **no** form of this command.

radius-server dead-criteria *[***time** *seconds] [***tries** *number-of-tries]*

no radius-server dead-criteria *[***time** *seconds] [***tries** *number-of-tries]*

Syntax Description

time *seconds*	(Optional) Minimum amount of time, in seconds, that must elapse from the time that the router last received a valid packet from the RADIUS server to the time the server is marked as dead. If a packet has not been received since the router booted, and there is a timeout, the time criterion will be treated as though it has been met. You can configure the time to be from 1 through 120 seconds. • If the *seconds argument is not configured, the number of seconds will range from 10 to 60 seconds, depending on the transaction rate of the server.* **Note** Both the time criterion and the tries criterion must be met for the server to be marked as dead.
tries *number-of-tries*	(Optional) Number of consecutive timeouts that must occur on the router before the RADIUS server is marked as dead. If the server performs both authentication and accounting, both types of packet will be included in the number. Improperly constructed packets will be counted as though they were timeouts. All transmissions, including the initial transmit and all retransmits, will be counted. You can configure the number of timeouts to be from 1 through 100. • If the *number-of-tries* argument is not configured, the number of consecutive timeouts will range from 10 to 100, depending on the transaction rate of the server and the number of configured retransmissions. **Note** Both the time criterion and the tries criterion must be met for the server to be marked as dead.

Defaults

If the *seconds argument is not configured, the number of seconds will range from 10 to 60 seconds, depending on the transaction rate of the server.*

If the *number-of-tries* argument is not configured, the number of consecutive timeouts will range from 10 to 100, depending on the transaction rate of the server and the number of configured retransmissions.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Note Both the time criterion and the tries criterion must be met for the server to be marked as dead.

The **no** form of this command has the following cases:

- If neither the *seconds* nor the *number-of-tries* argument is indicated, both time and tries will be set to their defaults.
- If either the *seconds* or the *number-of-tries* arguments is indicated, the one indicated (time or tries) will be set to its default. The other will be unchanged.
- If both the *seconds* and the *number-of-tries* arguments are indicated, both time and tries will be set to their defaults.

Examples

The following example shows that the router will be considered dead after 5 seconds and four tries:

```
Router (config)# radius-server dead-criteria time 5 tries 4
```

Related Commands

Command	Description
debug aaa dead-criteria transactions	Displays AAA dead-criteria transaction values.
show aaa dead-criteria	Displays dead-criteria information for a AAA server.
show aaa server-private	Displays the status of all private RADIUS servers.
show aaa servers	Displays information about the number of packets sent to and received from AAA servers.

radius-server deadtime

To improve RADIUS response times when some servers might be unavailable and cause the unavailable servers to be skipped immediately, use the **radius-server deadtime** command in global configuration mode. To set dead-time to 0, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime

Syntax Description

minutes	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).

Defaults

Dead time is set to 0.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command to cause the Cisco IOS software to mark as "dead" any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as "dead" is skipped by additional requests for the duration of *minutes* or unless there are no servers not marked "dead."

When the RADIUS Server Is Marked As Dead

For Cisco IOS versions prior to 12.2(13.7)T, the RADIUS server will be marked as dead if a transaction is transmitted for the configured number of retransmits and a valid response is not received from the server within the configured timeout for any of the RADIUS packet transmissions.

For Cisco IOS versions 12.2(13.7)T and later, the RADIUS server will be marked as dead if both of the following conditions are met:

1. A valid response has not been received from the RADIUS server for any outstanding transaction for at least the timeout period that is used to determine whether to retransmit to that server, and
2. Across all transactions being sent to the RADIUS server, at least the requisite number of retransmits +1 (for the initial transmission) have been sent consecutively without receiving a valid response from the server with the requisite timeout.

Examples

The following example specifies five minutes deadtime for RADIUS servers that fail to respond to authentication requests:

```
radius-server deadtime 5
```

Related Commands

Command	Description
deadtime (server-group configuration)	Configures deadtime within the context of RADIUS server groups.
radius-server host	Specifies a RADIUS server host.
radius-server retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval for which a router waits for a server host to reply.

radius-server directed-request

To allow users logging into a Cisco netword access server (NAS) to select a RADIUS server for authentication, use the **radius-server directed-request** command in global configuration mode. To disable the directed-request feature, use the **no** form of this command.

radius-server directed-request [**restricted**]

no radius-server directed-request [**restricted**]

Syntax Description

restricted	(Optional) Prevents the user from being sent to a secondary server if the specified server is not available.

Defaults

User cannot log into a Cisco NAS to select a RADIUS server for authentication.

Command Modes

Global configuration mode

Command History

Release	Modification
12.0(2)T	This command was introduced.

Usage Guidelines

The **radius-server directed-request** command sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with this command enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Disabling the **radius-server directed-request** command causes the whole string, both before and after the "@" symbol, to be sent to the default RADIUS server. The router queries the list of servers, starting with the first one in the list. It sends the whole string, and accepts the first response that it gets from the server.

Use the **radius-server directed-request restricted** command to limit the user to the RADIUS server identified as part of the username.

The **no radius-server directed-request** command causes the entire username string to be passed to the default RADIUS server.

Note When **no radius-server directed-request restricted** is entered, only the "restricted" flag is removed, and the "directed-request" flag is retained. To disable the directed-request feature, you must also issue the **no radius-server directed-request** command.

Examples

The following example verifies that the RADIUS server is selected based on the directed request:

```
aaa new-model
aaa authentication login default radius
radius-server host 192.168.1.1
radius-server host 172.16.56.103
```

```
radius-server host 172.31.40.1
radius-server directed-request
```

radius-server domain-stripping

To enable Virtual Route Forwarding (VRF)-aware domain-stripping, use the **radius-server domain-stripping** command in global configuration mode. To remove VRF-aware domain-stripping, use the **no** form of this command.

radius-server domain-stripping [**vrf** *vrf-name*]

no radius-server domain-stripping [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Per VRF configuration.

Defaults

This functionality is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)DD	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use the **radius-server domain-stripping** command to strip or truncate the domain from a username. For example, if the username is user1@cisco.com and the **radius-server domain-stripping** command is configured, only “user1” is sent out as the username.

To configure domain-stripping only to a specified VRF, use the **vrf** *vrf-name* option.

Examples

The following example shows a configuration that strips the domain name from the VRF “abc”:

```
radius-server domain-stripping vrf abc
```

radius-server extended-portnames

The **radius-server extended-portnames** command is replaced by the **radius-server attribute nas-port format** command. See the description of the **radius-server attribute nas-port format** command for more information.

radius-server host

To specify a RADIUS server host, use the **radius-server host** command in global configuration mode. To delete the specified RADIUS host, use the **no** form of this command.

radius-server host {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias**{*hostname* | *ip-address*}]

no radius-server host {*hostname* | *ip-address*}

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.
auth-port	(Optional) Specifies the UDP destination port for authentication requests.
port-number	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1645.
acct-port	(Optional) Specifies the UDP destination port for accounting requests.
port-number	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
timeout	(Optional) The time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used. Enter a value in the range 1 to 1000.
seconds	(Optional) Specifies the **timeout** value. Enter a value in the range 1 to 1000. If no **timeout** value is specified, the global value is used.
retransmit	(Optional) The number of times a RADIUS request is re-sent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
retries	(Optional) Specifies the retransmit value. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used.
key	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
string	(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.

Defaults

No RADIUS host is specified; use global **radius-server** command values.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(5)T	This command was modified to add options for configuring timeout, retransmission, and key values per RADIUS server.
12.1(3)T	The **alias** keyword was added on the Cisco AS5300 and AS5800 universal access servers.

Usage Guidelines

You can use multiple **radius-server host** commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

Examples

The following example specifies *host1* as the RADIUS server and uses default ports for both accounting and authentication:

```
radius-server host host1
```

The following example specifies port 1612 as the destination port for authentication requests and port 1616 as the destination port for accounting requests on the RADIUS host named host1:

```
radius-server host host1 auth-port 1612 acct-port 1616
```

Because entering a line resets all the port numbers, you must specify a host and configure accounting and authentication ports on a single line.

The following example specifies the host with IP address 172.29.39.46 as the RADIUS server, uses ports 1612 and 1616 as the authorization and accounting ports, sets the timeout value to 6, sets the retransmit value to 5, and sets “rad123” as the encryption key, matching the key on the RADIUS server:

```
radius-server host 172.29.39.46 auth-port 1612 acct-port 1616 timeout 6 retransmit 5 key
rad123
```

To use separate servers for accounting and authentication, use the zero port value as appropriate.

The following example specifies that RADIUS server host1 be used for accounting but not for authentication, and that RADIUS server host2 be used for authentication but not for accounting:

```
radius-server host host1.example.com auth-port 0
radius-server host host2.example.com acct-port 0
```

The following example specifies four aliases on the RADIUS server with IP address 172.1.1.1:

```
radius-server host 172.1.1.1 acct-port 1645 auth-port 1646
radius-server host 172.1.1.1 alias 172.16.2.1 172.17.3.1 172.16.4.1
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to a user.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies how many times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval a router waits for a server host to reply.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

radius-server host non-standard

To identify that the security server is using a vendor-proprietary implementation of RADIUS, use the **radius-server host non-standard** command in global configuration mode. This command tells the Cisco IOS software to support nonstandard RADIUS attributes. To delete the specified vendor-proprietary RADIUS host, use the **no** form of this command.

radius-server host {*host-name* | *ip-address*} **non-standard**

no radius-server host {*host-name* | *ip-address*} **non-standard**

Syntax Description

host-name	DNS name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.

Defaults

No RADIUS host is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

The **radius-server host non-standard** command enables you to identify that the RADIUS server is using a vendor-proprietary implementation of RADIUS. Although an IETF draft standard for RADIUS specifies a method for communicating information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. This command enables the Cisco IOS software to support the most common vendor-proprietary RADIUS attributes. Vendor-proprietary attributes will not be supported unless you use the **radius-server host non-standard** command.

For a list of supported vendor-specific RADIUS attributes, refer to the appendix "RADIUS Attributes" in the *Cisco IOS Security Configuration Guide*.

Examples

The following example specifies a vendor-proprietary RADIUS server host named *alcatraz*:

```
radius-server host alcatraz non-standard
```

Related Commands

Command	Description
radius-server configure-nas	Allows the Cisco router or access server to query the vendor-proprietary RADIUS server for the static routes and IP pool definitions used throughout its domain when the device starts up.
radius-server host	Specifies a RADIUS server host.

radius-server key

To set the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon, use the **radius-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

radius-server key {***0*** *string* | ***7*** *string* | *string*}

no radius-server key

Syntax Description

0	Specifies that an unencrypted key will follow.
string	The unencrypted (cleartext) shared key.
7	Specifies that a hidden key will follow.
string	The hidden shared key.
string	The unencrypted (cleartext) shared key.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.1(3)T	The *string* argument was modified as follows: • **0** *string* • **7** *string* • *string*

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) authentication with the **aaa new-model** command, you must set the authentication and encryption key using the **radius-server key** command.

Note Specify a RADIUS key after you issue the **aaa new-model** command.

The key entered must match the key used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Examples

The following example sets the authentication and encryption key to “dare to go”:

```
radius-server key dare to go
```

The following example sets the authentication and encryption key to “anykey.” The 7 specifies that a hidden key will follow.

```
service password-encryption
radius-server key 7 anykey
```

After you save your configuration and use the **show-running config** command, an encrypted key will be displayed as follows:

```
Router# show running-config
!
!
 radius-server key 7 19283103834782sda
! The leading 7 indicates that the following text is encrypted.
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server host	Specifies a RADIUS server host.
service password-encryption	Encrypt passwords.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

radius-server local

To enable the access point or wireless-aware router as a local authentication server and to enter into configuration mode for the authenticator, use the **radius-server local** command in global configuration mode. To remove the local RADIUS server configuration from the router or access point, use the **no** form of this command.

radius-server local

no **radius-server local**

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following example shows that the access point is being configured to serve as a local authentication server:

```
Router (config)# radius-server local
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.

Command	Description
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

radius-server optional-passwords

To specify that the first RADIUS request to a RADIUS server be made *without* password verification, use the **radius-server optional-passwords** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server optional-passwords

no radius-server optional-passwords

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When the user enters the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the RADIUS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The RADIUS server must support authentication for users without passwords to make use of this feature.

Examples

The following example configures the first login to not require RADIUS verification:

```
radius-server optional-passwords
```

radius-server retransmit

To specify the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up, use the **radius-server retransmit** command in global configuration mode. To disable retransmission, use the **no** form of this command.

radius-server retransmit *retries*

no radius-server retransmit

Syntax Description

retries	Maximum number of retransmission attempts. The default is 3 attempts.

Defaults

3 attempts

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The Cisco IOS software tries all servers, allowing each one to time out before increasing the retransmit count.

Examples

The following example specifies a retransmit counter value of five times:

```
radius-server retransmit 5
```

radius-server retry method reorder

To specify the reordering of RADIUS traffic retries among a server group, use the **radius-server retry method reorder** command in global configuration mode. To disable the reordering of retries among the server group, use the **no** form of this command.

radius-server retry method reorder

no radius-server retry method reorder

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, RADIUS traffic is not reordered among the server group.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command to reorder RADIUS traffic to another server in the server group when the first server fails in periods of high load. Subsequent to the failure, all RADIUS traffic is directed to the new server. Traffic is switched from the new server to another server in the server group only if the new server also fails. Traffic will not be automatically switched back to the first server.

If the **radius-server retry method reorder** command is not configured, each RADIUS server is used until marked dead. The nondead server that is closest to the beginning of the list is used for the first transmission of a transaction and for the configured number of retransmissions. Each nondead server in the list is thereafter tried in turn.

Examples

The following example shows that RADIUS server retry has been configured:

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 1.2.3.4 key rad123
radius-server host 4.5.6.7 key rad123
```

Related Commands

Command	Description
radius-server transaction max-tries	Specifies the maximum number of transmissions that may be retried per transaction on a RADIUS server.

radius-server source-ports extended

To enable 200 ports in the range from 21645 to 21844 to be used as the source ports for sending out RADIUS requests, use the **radius-server source-ports extended** command in global configuration mode. To return to the default setting, in which ports 1645 and 1646 are used as the source ports for RADIUS requests, use the **no** form of this command.

radius-server source-ports extended

no radius-server source-ports extended

Syntax Description

This command has no arguments or keywords.

Defaults

Ports 1645 and 1646 are used as the source ports for RADIUS requests.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The identifier field of the RADIUS packet is 8 bits long, and yields 256 unique identifiers. A NAS uses one port (1645) as the source port to send out access requests to the RADIUS server and one port (1646) as the source port to send out accounting requests to the RADIUS server. This scheme allows for 256 outstanding access requests and 256 outstanding accounting requests.

If the number of outstanding access requests or accounting requests exceeds 256, the port and ID space will wrap, and all subsequent RADIUS requests will be forced to reuse ports and IDs that are already in use. When the RADIUS server receives a request that uses a port and ID that is already in use, it treats the request as a duplicate. The RADIUS server then drops the request.

The **radius-server source-ports extended** command allows you to configure the NAS to use 200 ports in the range from 21645 to 21844 as the source ports for sending out RADIUS requests. Having 200 source ports allows up to 256*200 authentication and accounting requests to be outstanding at one time. During peak call volume, typically when a router first boots or when an interface flaps, the extra source ports allow sessions to recover more quickly on large-scale aggregation platforms.

Examples

The following example shows how to configure a NAS to use 200 ports in the range from 21645 to 21844 as the source ports for RADIUS requests:

```
Router(config)# radius-server source-ports extended
```

radius-server timeout

To set the interval for which a router waits for a server host to reply, use the **radius-server timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout

Syntax Description

seconds	Number that specifies the timeout interval, in seconds. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command to set the number of seconds a router waits for a server host to reply before timing out.

Examples

The following example changes the interval timer to 10 seconds:

```
radius-server timeout 10
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

radius-server transaction max-tries

To specify the maximum number of transmissions that may be retried per transaction on a RADIUS server, use the **radius-server transaction max-retries** command in global configuration mode. To disable the number of retries that were configured, use the **no** form of this command.

radius-server transaction max-tries *number*

no radius-server transaction max-tries *number*

Syntax Description

number	Total number of transmissions per transaction. The default is eight.

Defaults

Eight transmissions

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command to specify the maximum number of transmissions that may be retried per transaction on a RADIUS server. This command has no meaning if the **radius-server retry method order** command has not been already configured.

Examples

The following example shows that a RADIUS server has been configured for six retries per transaction:

```
aaa new-model
radius-server retry method reordeer
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 1.2.3.4
radius-server host 5.6.7.8
```

Related Commands

Command	Description
radius-server retry method reorder	Specifies the reordering of RADIUS traffic retries among a server group.

radius-server unique-ident

To enable the acct-session-id-count variable containing the unique identifier variable, use the **radius-server unique-ident** command in global configuration mode. To disable the acct-session-id-count variable, use the **no** form of this command.

radius-server unique-ident *id*

no radius-server unique-ident

Syntax Description

id	Unique identifier represented by the first eight bits of the acct-session-id-count variable. Valid values range from 0 to 255.

Defaults

The acct-session-id-count variable is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **radius-server unique-ident** command to increase the size of the accounting session identifier (ID) variable from 32 bits to 56 bits.

RADIUS attribute 44, Accounting Session ID, is a unique accounting identifier that makes it easy to match start and stop records in a log file. Accounting session ID numbers restart at 1 each time the router is power-cycled or the software is reloaded.

The acct-session-id variable is a 32-bit variable that can take on values from 00000000–FFFFFFFF.

The acct-session-id-count variable enabled by the **radius-server unique-ident** command is a 32-bit variable. The first eight bits of the variable are reserved for the unique identifier, an identifier that allows the RADIUS server to identify an accounting session if a reload occurs. The remaining 24 bits of the acct-session-id-count variable acts as a counter variable. When the first acct-session-id variable is assigned, the acct-session-id-count variable is set to 1. The acct-session-id-count variable increments by one every time the acct-session-id variable wraps.

The acct-session-id-count variable can take on values from ##000000–##FFFFFF, where ## represents the eight bits that are reserved for the unique identifier variable.

The acct-session-id-count and acct-session-id variables are concatenated before being sent to the RADIUS server, resulting in the accounting session being represented by the following 56-bit variable:

##000000 00000000–##FFFFFF FFFFFFFF

Examples

The following example shows how to enable the acct-session-id-count variable and sets the unique identifier variable to 5:

```
radius-server unique-ident 5
```

radius-server vsa send

To configure the network access server to recognize and use vendor-specific attributes, use the **radius-server vsa send** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server vsa send [**accounting** | **authentication**]

no radius-server vsa send [**accounting** | **authentication**]

Syntax Description

accounting	(Optional) Limits the set of recognized vendor-specific attributes to only accounting attributes.
authentication	(Optional) Limits the set of recognized vendor-specific attributes to only authentication attributes.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The **radius-server vsa send** command enables the network access server to recognize and use both accounting and authentication vendor-specific attributes. Use the **accounting** keyword with the **radius-server vsa send** command to limit the set of recognized vendor-specific attributes to just accounting attributes. Use the **authentication** keyword with the **radius-server vsa send** command to limit the set of recognized vendor-specific attributes to just authentication attributes.

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string with the following format:

```
protocol : attribute sep value *
```

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization. "Attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes Cisco's "multiple named ip address pools" feature to be activated during IP authorization (during PPP's IPCP address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

The following example causes a “NAS Prompt” user to have immediate access to EXEC commands.

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, refer to RFC 2138, *Remote Authentication Dial-In User Service (RADIUS)*.

Examples

The following example configures the network access server to recognize and use vendor-specific accounting attributes:

```
radius-server vsa send accounting
```

Related Commands

Command	Description
aaa nas port extended	Replaces the NAS-Port attribute with RADIUS IETF attribute 26 and displays extended field information.

reauthentication time

To enter the time limit after which the authenticator should reauthenticate, use the **reauthentication time** command in local RADIUS server group configuration mode. To remove the requirement that users reauthenticate after the specified duration, use the **no** form of this command.

reauthentication time *seconds*

no reauthentication time *seconds*

Syntax Description

seconds	Number of seconds after which reauthentication occurs.

Defaults

The default setting is 0 seconds, which means that group members are not required to reauthenticate.

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following example shows that the time limit after which the authenticator should reauthenticate is 30 seconds:

```
reauthentication time 30
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.

Command	Description
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

redirect (identity policy)

To redirect clients to a particular URL, use the **redirect** command in identity policy configuration mode. To remove the URL, use the **no** form of this command.

redirect url *url*

no redirect url *url*

Syntax Description

url	URL to which clients should be redirected.
url	Valid URL.

Defaults

No default behavior or values

Command Modes

Identity policy configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

When you use this command, an identity policy has to be associated with an Extensible Authentication Protocol over UDP (EAPoUDP) identity profile.

Examples

The following example shows the URL to which clients will be redirected:

```
Router (config)# identity policy p1
Router (config-identity-policy)# redirect url http://www.cisco.com
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

redundancy stateful

To configure stateful failover for tunnels using IP Security (IPSec), use the **redundancy stateful** command in crypto map configuration mode. To disable stateful failover for tunnel protection, use the **no** form of this command.

redundancy *standby-group-name* **stateful**

no redundancy *standby-group-name* **stateful**

Syntax Description

standby-group-name	Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands. Both routers in the standby group are defined by this argument and share the same virtual IP (VIP) address.

Defaults

Stateful failover is not enabled for IPSec tunnels.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **redundancy stateful** command uses an existing IPSec profile (which is specified via the **crypto ipsec profile** command) to configure IPSec stateful failover for tunnel protection. (You do not configure the tunnel interface as you would with a crypto map configuration.) IPSec stateful failover enables you to define a backup IPSec peer (secondary) to take over the tasks of the active (primary) router if the active router is deemed unavailable.

The tunnel source address must be a VIP address, and it must not be an interface name.

Examples

The following example shows how to configure stateful failover for tunnel protection:

```
crypto ipsec profile peer-profile
  redundancy HA-out stateful

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source 209.165.201.3
 tunnel destination 10.0.0.5
 tunnel protection ipsec profile peer-profile
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 name HA-out
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two routers and enters crypto map configuration mode.

regenerate

To enable key rollover with manual certificate enrollment, use the **regenerate** command in ca-trustpoint configuration mode. To disable key rollover, use the **no** form of this command.

regenerate

no regenerate

Syntax Description

This command has no arguments or keywords.

Defaults

Key rollover is not enabled.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **regenerate** command to provide seamless key rollover for manual certificate enrollment. A new key pair is created with a temporary name, and the old certificate and key pair are retained until a new certificate is received from the certification authority (CA). When the new certificate is received, the old certificate and key pair are discarded and the new key pair is renamed with the name of the original key pair.

If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable:

```
! RSA keypair associated with trustpoint is exportable
```

Do not regenerate the keys manually; key rollover will occur when the **crypto ca enroll** command is issued.

Examples

The following example shows how to configure key rollover to regenerate new keys with a manual certificate enrollment from the CA named “trustme2”.

```
crypto ca trustpoint trustme2
 enrollment url http://trustme2.company.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet0
 serial-number none
 regenerate
 password revokeme
 rsakeypair trustme2 2048
 exit
crypto ca authenticate trustme2
crypto ca enroll trustme2
```

Related Commands

Command	Description
crypto ca authenticate	Retrieves the CA certificate and authenticates it.
crypto ca enroll	Requests certificates from the CA for all of your router's RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

reverse-route

To create source proxy information for a crypto map entry, use the **reverse-route** command in crypto map configuration mode. To remove the source proxy information from a crypto map entry, use the **no** form of this command.

reverse-route [**remote-peer** [*ip-address*]]

no reverse-route [**remote-peer** [*ip-address*]]

Syntax Description

remote-peer	(Optional) Routes of public IP addresses and IP security (IPSec) tunnel destination addresses are inserted into the routing table.
ip-address	(Optional) IP address of the next hop destination.

Defaults

No default behavior or values.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.2(13)T	The **remote-peer** keyword was added.
12.3	The *ip-address* argument was added.

Usage Guidelines

This command can be applied on a per-crypto basis.

Reverse route injection (RRI) is a good solution for topologies that require encrypted traffic to be diverted to a Virtual Private Network (VPN) router and all other traffic to a different router. In these scenarios, RRI eliminates the need to manually define static routes on devices. RRI is not required if a single VPN router is used and all traffic passes through the VPN router during its path in and out of the network.

If the user chooses to manually define static routes on the VPN router for remote proxies and have these routes permanently installed in the routing table, RRI should not be enabled on the crypto map instance that covers the same remote proxies. In this case, there is no possibility of user defined static routes being removed by RRI.

Set peer statements in crypto maps must use IP addresses only for this release. Support for host name resolution with RRI is not yet available.

Routing convergence can affect the success of a failover based on the routing protocol used to advertise routes (link state versus periodic update). It is recommended that a link state routing protocol such as Open Shortest Path First (OSPF) be used to help speed convergence time by ensuring that routing updates are sent as soon as a change in routing state is detected.

Examples

The following example shows how all remote VPN gateways connect to the router via 192.168.0.3:

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102

Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
show crypto map (IPSec)	Displays the crypto map configuration.

revocation-check

To check the revocation status of a certificate, use the **revocation-check** command in ca-trustpoint configuration mode. To disable this functionality, use the **no** form of this command.

revocation-check *method1* [*method2*[*method3*]]

no revocation-check *method1* [*method2*[*method3*]]

Syntax Description

method1 [*method2*[*method3*]]	Method used by the router to check the revocation status of the certificate. Available methods are as follows: • **crl**—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • **none**—Certificate checking is not required. • **ocsp**—Certificate checking is performed by an online certificate status protocol (OCSP) server. If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.

Defaults

After a trustpoint is enabled, the default is set to **revocation-check crl**, which means that CRL checking is mandatory.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

Use the **revocation-check** command to ensure that the certificate of a peer has not been revoked.

If your router does not have the applicable CRL and is unable to obtain one or if the OCSP server returns an error, your router will reject the peer's certificate—unless you include the **none** keyword in your configuration. If you use the **none** keyword, your router will check the CRL if it is cached in the router memory, but it will not download the CRL from the CRL distribution point (CDP). If the **none** keyword is configured and a CRL is not available, the certificate will always be accepted. If the **revocation-check none** command is configured, you cannot manually download the CRL via the **crypto ca crl request** command because the manually downloaded CRL may not be deleted after it expires. The expired CRL can cause all certificate verifications to be denied.

Note The **none** keyword replaces the **optional** keyword that is available from the **crl** command. If you enter the **crl optional** command, it will be written back as the **revocation-check none** command.

Also, the **crl** and **none** keywords issued together replace the **best-effort** keyword that is available from the **crl** command. If you enter the **crl best-effort** command, it will be written back as the **revocation-check crl none** command.

Examples

The following example shows how to configure the router to use the OCSP server that is specified in the AIA extension of the certificate:

```
Router(config)# crypto ca trustpoint mytp
Router(ca-trustpoint)# revocation-check ocsp
```

The following example shows how to configure the router to download the CRL from the CDP; if the CRL is unavailable, the OCSP server that is specified in the AIA extension of the certificate will be used. If both options fail, certificate verification will also fail.

```
Router(config)# crypto ca trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocsp
```

The following example shows how to configure your router to use the OCSP server at the HTTP URL "http://myocspserver:81." If the server is down, revocation check will be ignored.

```
Router(config)# crypto ca trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
```

Related Commands

Command	Description
crl	Queries the CRL to ensure that the certificate of the peer has not been revoked.
crypto ca trustpoint	Declares the CA that your router should use.
ocsp url	Enables an OCSP server.

root

To obtain the certification authority (CA) certificate via TFTP, use the **root** command in ca-trustpoint configuration mode. To deconfigure the CA, use the **no** form of this command.

root tftp *server-hostname filename*

no root tftp *server-hostname filename*

Syntax Description

tftp	Defines the TFTP protocol to get the root certificate.
server-hostname filename	Specifies a name for the server and a name for the file that will store the trustpoint CA.

Defaults

A CA certificate is not configured.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

This command allows you to access the CA via the TFTP protocol, which is used to get the CA. You want to configure a CA certificate so that your router can verify certificates issued to peers. Thus, your router does not have to enroll with the CA that issued the certificates the peers.

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which puts you in ca-trustpoint configuration mode.

Note The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to configure the CA certificate named “bar” using TFTP:

```
crypto ca trustpoint bar
 root tftp xxx fff
 crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

root CEP

The **crypto ca trustpoint** command deprecates the **crypto ca trusted-root** command and all related subcommands (all trusted-root configuration mode commands). If you enter a trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

root PROXY

The **root PROXY** command is replaced by the **enrollment http-proxy** command. See the **enrollment http-proxy** command for more information.

root TFTP

The **root TFTP** command is replaced by the **root** command. See the **root** command for more information.

rsakeypair

To specify which key pair to associate with the certificate, use the **rsakeypair** command in ca-trustpoint configuration mode.

rsakeypair *key-label* [*key-size* [*encryption-key-size*]]

Syntax Description

key-label	Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is configured.
key-size	(Optional) Size of the desired Rivest, Shamir, Adelman (RSA) key. If not specified, the existing key size is used. (The specified size must be the same as the size of the *encryption-key-size* argument.)
encryption-key-size	(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates. (The specified size must be the same as the size of the *key-size* argument.)

Defaults

The fully qualified domain name (FQDN) key is used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

When you regenerate a key pair, you are responsible for reenrolling the identities associated with the key pair. Use the **rsakeypair** command to refer back to the named key pair.

Examples

The following example is a sample trustpoint configuration that specifies the RSA key pair "exampleCAkeys":

```
crypto ca trustpoint exampleCAkeys
 enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crl	Generates RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

rsa-pubkey

To define the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signature during Internet Key Exchange (IKE) authentication, use the **rsa-pubkey** command in keyring configuration mode. To remove the manual key that was defined, use the **no** form of this command.

rsa-pubkey{**address** *address* | **name** *fqdn*} [**encryption** | **signature**]

no rsa-pubkey {**address** *address* | **name** *fqdn*} [**encryption** | **signature**]

Syntax Description

address *address*	IP address of the remote peer.
name *fqdn*	Fully qualified domain name (FQDN) of the peer.
encryption	(Optional) The manual key is to be used for encryption.
signature	(Optional) The manual key is to be used for signature.

Defaults

No default behavior or values

Command Modes

Keyring configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use this command to enter public key chain configuration mode. Use this command when you need to manually specify RSA public keys of other IP Security (IPSec) peers. You need to specify the keys of other peers when you configure RSA encrypted nonces as the authentication method in an IKE policy at your peer router.

Examples

The following example shows that the RSA public key of an IPSec peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

save-password

To save your extended authentication (Xauth) password locally on your PC, use the **save-password** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To disable the Save-Password attribute, use the **no** form of this command.

save-password

no save-password

Syntax Description

This command has no arguments or keywords.

Defaults

Your Xauth password is not saved locally on your PC, and the Save-Password attribute is not added to the server group profile.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

Save password control allows you to save your Xauth password locally on your PC so that after you have initially entered the password, the Save-Password attribute is pushed from the server to the client. On subsequent authentications, you can activate the password by using the tick box on the software client or by adding the username and password to the Cisco IOS hardware client profile. The password setting remains until the Save-Password attribute is removed from the server group profile. After the password has been activated, the username and password are sent automatically to the server during Xauth without your intervention.

The save-password option is useful only if your password is static, that is, if it is not a one-time password such as one that is generated by a token.

The Save-Password attribute is configured on a Cisco IOS router or in the RADIUS profile.

To configure save password control, use the **save-password** command.

An example of an attribute-value (AV) pair for the Save-Password attribute is as follows:

```
ipsec:save-password=1
```

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **save-password** command.

Note

- The Save-Password attribute can be applied only by a RADIUS user.
- The attribute can be applied on a per-user basis after the user has been authenticated.
- The attribute can override any similar group attributes.

- User-based attributes are available only if RADIUS is used as the database.

Examples

The following example shows that the Save-Password attribute has been configured:

```
crypto isakmp client configuration group cisco
 save-password
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

secure boot-config

To take a snapshot of the router running configuration and securely archive it in persistent storage, use the **secure boot-config** command in global configuration mode. To remove the secure configuration archive and disable configuration resilience, use the **no** form of this command.

secure boot-config [**restore** *filename*]

no secure boot-config

Syntax Description

restore *filename*	(Optional) Reproduces a copy of the secure configuration archive as the supplied filename.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Without any parameters, this command takes a snapshot of the router running configuration and securely archives it in persistent storage. Like the image, the configuration archive is hidden and cannot be viewed or removed directly from the command-line interface (CLI) prompt . It is recommended that you run this command after the router has been fully configured to reach a steady state of operation and the running configuration is considered complete for a restoration, if required. A syslog message is printed on the console notifying the user of configuration resilience activation. The secure archive uses the time of creation as its filename. For example, .runcfg-20020616-081702.ar was created July 16 2002 at 8:17:02.

The restore option reproduces a copy of the secure configuration archive as the supplied filename (disk0:running-config, slot1:runcfg, and so on). The restore operation will work only if configuration resilience is enabled. The number of restored copies that can be created is unlimited.

The **no** form of this command removes the secure configuration archive and disables configuration resilience. An enable, disable, enable sequence has the effect of upgrading the configuration archive if any changes were made to the running configuration since the last time the feature was disabled.

The configuration upgrade scenario is similar to an image upgrade. The feature detects a different version of Cisco IOS and notifies the user of a version mismatch. The same command can be run to upgrade the configuration archive to a newer version after new configuration commands corresponding to features in the new image have been issued.

The correct sequence of steps to upgrade the configuration archive after an image upgrade is as follows:

- Configure new commands
- Issue the **secure boot-config** command

Examples

The following example shows the command used to securely archive a snapshot of the router running configuration:

```
secure boot-config
```

The following example shows the command used to restore an archived image to the file slot0:rescue-cfg:

```
Router(config)# secure boot-config restore slot0:rescue-cfg
ios resilience:configuration successfully restored as slot0:rescue-cfg
```

Related Commands

Command	Description
secure boot-image	Enables Cisco IOS image resilience.
show secure bootset	Displays the status of image and configuration resilience.

secure boot-image

To enable Cisco IOS image resilience, use the **secure boot-image** command in global configuration mode. To disable Cisco IOS image resilience and release the secured image so that it can be safely removed, use the **no** form of this command.

secure boot-image

no secure boot-image

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command enables or disables the securing of the running Cisco IOS image. The following two possible scenarios exist with this command.

- When turned on for the first time, the running image (as displayed in the **show version** command output) is secured, and a syslog entry is generated. This command will function properly only when the system is configured to run an image from a disk with an Advanced Technology Attachment (ATA) interface. Images booted from a TFTP server cannot be secured. Because this command has the effect of "hiding" the running image, the image file will not be included in any directory listing of the disk. The **no** form of this command releases the image so that it can be safely removed.
- If the router is configured to boot up with Cisco IOS resilience and an image with a different version of Cisco IOS is detected, a message similar to the following is displayed at bootup:

```
ios resilience :Archived image and configuration version 12.2 differs from running
version 12.3.
Run secure boot-config and image commands to upgrade archives to running version.
```

To upgrade the image archive to the new running image, reenter this command from the console. A message will be displayed about the upgraded image. The old image is released and will be visible in the **dir** command output.

Caution Be careful when copying new images to persistent storage because the existing secure image name might conflict with the new image. To verify the name of the secured archive, run the **show secure bootset** command and resolve any name conflicts with the currently secured hidden image.

Note After the Cisco IOS image is secured, the resilient configuration feature will deny any requests to copy, modify, or delete the secure archive and will even survive a disk format operation.

Examples

The following example shows the activation of image resilience.

```
Router(config)# secure boot-image
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
secure boot-config	Saves a secure copy of the router running configuration in persistent storage.
show secure bootset	Displays the status of image and configuration resilience.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

security authentication failure rate

To configure the number of allowable unsuccessful login attempts, use the **security authentication failure rate** command in global configuration mode. To disable this functionality, use the **no** form of this command.

security authentication failure rate *threshold-rate* **log**

no security authentication failure rate *threshold-rate* **log**

Syntax Description

threshold-rate	Number of allowable unsuccessful login attempts. The default is 10.
log	Syslog authentication failures if the rate exceeds the threshold.

Defaults

The default number of failed login attempts before a 15-second delay is 10.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **security authentication failure rate** command provides enhanced security access to the router by generating syslog messages after the number of unsuccessful login attempts exceeds the configured threshold rate. This command ensures that there are not any continuous failures to access the router.

Examples

The following example shows how to configure your router to generate a syslog message after eight failed login attempts:

```
security authentication failure rate 8 log
```

Related Commands

Command	Description
security passwords min-length	Ensures that all configured passwords are at least a specified length.

security ipsec

To apply a previously configured IP Security (IPSec) profile to the redundancy group communications, use the **security ipsec** command in inter-device configuration mode. To remove the IPSec profile from the configuration, use the **no** form of this command.

security ipsec *profile-name*

no security [**ipsec** [*profile-name*]]

Syntax Description

profile-name	Profile name, which was specified via the **crypto ipsec profile** command.

Defaults

The redundancy group is not secured.

Command Modes

Inter-device configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **security ipsec** command allows you to secure a redundancy group via a previously configured IPSec profile. If you are certain that the Stateful Switchover (SSO) traffic between the redundancy group runs on a physically secure interface, you do not have to configure this command.

Note If you configure SSO traffic protection via the **security ipsec** command, the active and standby devices must be directly connected to each other via Ethernet networks.

Examples

The following example shows how to configure SSO traffic protection:

```
crypto ipsec transform-set trans2 ah-md5-hmac esp-aes
!
crypto ipsec profile sso-secure
 set transform-set trans2
!
redundancy inter-device
 scheme standby HA-in
 security ipsec sso-secure
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two IPSec routers.
redundancy inter-device	Enters inter-device configuration mode.

security passwords min-length

To ensure that all configured passwords are at least a specified length, use the **security passwords min-length** command in global configuration mode. To disable this functionality, use the **no** form of this command.

security passwords min-length *length*

no security passwords min-length *length*

Syntax Description

length	Minimum length of a configured password. The default is six characters.

Defaults

Six characters

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **security passwords min-length** command provides enhanced security access to the router by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks, such as “lab” and “cisco.” This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will fail.

Examples

The following example shows both how to specify a minimum password length of six characters and what happens when the password does not adhere to the minimum length:

```
security password min-length 6
enable password lab
% Password too short - must be at least 6 characters. Password not configured.
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
security authentication failure rate	Configures the number of allowable unsuccessful login attempts.

self-identity

To define the identity that the local Internet Key Exchange (IKE) uses to identify itself to the remote peer, use the **self-identity** command in ISAKMP profile configuration mode. To remove the Internet Security Association and Key Management Protocol (ISAKMP) identity that was defined for the IKE, use the **no** form of this command.

self-identity {**address** | **fqdn** | **user-fqdn** *user-fqdn*}

no self-identity {**address** | **fqdn** | **user-fqdn** *user-fqdn*}

Syntax Description

address	The IP address of the local endpoint.
fqdn	The fully qualified domain name (FQDN) of the host.
user-fqdn *user-fqdn*	The user FQDN that is sent to the remote endpoint.

Defaults

If no ISAKMP identity is defined in the ISAKMP profile configuration, global configuration is the default.

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Examples

The following example shows that the IKE identity is the user FQDN “user@vpn.com”:

```
crypto isakmp profile vpnprofile
 self-identity user-fqdn user@vpn.com
```

serial-number (ca-trustpoint)

To specify whether the router serial number should be included in the certificate request, use the **serial-number** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

serial-number [**none**]

no serial-number

Syntax Description

none	(Optional) Specifies that a serial number will not be included in the certificate request.

Defaults

Not configured. You will be prompted for the serial number during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Before you can issue the **serial-number** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

Use this command to specify the router serial number in the certificate request, or use the **none** keyword to specify that a serial number should not be included in the certificate request.

Examples

The following example shows how to omit a serial number from the "root" certificate request:

```
crypto ca trustpoint root
 enrollment url http://10.3.0.7:80
 ip-address none
 fqdn none
 serial-number none
 subject-name CN=jack, OU=PKI, O=Cisco Systems, C=US

crypto ca trustpoint root
 enrollment url http://10.3.0.7:80
 serial-number
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

serial-number (pubkey)

To define the serial number for the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signatures during Internet Key Exchange (IKE) authentication, use the **serial-number** command in pubkey configuration mode. To remove the manual key that was defined, use the **no** form of this command.

serial-number *serial-number*

no serial-number *serial-number*

Syntax Description

serial-number	Device serial number. The value is from 0 through infinity.

Defaults

No default behavior or values

Command Modes

Pubkey configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Examples

The following example shows that the public key of an IP Security (IPSec) peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey-key)# serial-number 1000000
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer that you will manually configure.
key-string (IKE)	Specifies the RSA public key of a remote peer.

server (RADIUS)

To configure the IP address of the RADIUS server for the group server, use the **server** command in server-group configuration mode. To remove the associated server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

no server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

Syntax Description

ip-address	IP address of the RADIUS server host.
auth-port *port-number*	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The port-number argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0.
acct-port *port-number*	(Optional) Specifies the UDP destination port for accounting requests. The port number argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0.

Defaults

If no port attributes are defined, the defaults are as follows:

- Authentication port: 1645
- Accounting port: 1646

Command Modes

Server-group configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(7)T	The following new keywords/arguments were added: • **auth-port** *port-number* • **acct-port** *port-number*

Usage Guidelines

Use the **server** command to associate a particular server with a defined group server. There are two different ways in which you can identify a server, depending on the way you want to offer AAA services. You can identify the server simply by using its IP address, or you can identify multiple host instances or entries using the optional **auth-port** and **acct-port** keywords.

When you use the optional keywords, the network access server identifies RADIUS security servers and host instances associated with a group server on the basis of their IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS host entries providing a specific AAA service. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as failover backup to the first one. Using this

example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

Examples

Configuring Multiple Entries for the Same Server IP Address

The following example shows the network access server configured to recognize several RADIUS host entries with the same IP address. Two different host entries on the same RADIUS server are configured for the same services—authentication and accounting. The second host entry configured acts as fail-over backup to the first one. (The RADIUS host entries are tried in the order in which they are configured.)

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2000
```

Configuring Multiple Entries Using AAA Group Servers

In this example, the network access server is configured to recognize two different RADIUS group servers. One of these groups, group1, has two different host entries on the same RADIUS server configured for the same services. The second host entry configured acts as failover backup to the first one.

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS group server and associates servers
! with it.
aaa group server radius group1
   server 172.20.0.1 auth-port 1000 acct-port 1001
! The following commands define the group2 RADIUS group server and associates servers
! with it.
aaa group server radius group2
   server 172.20.0.1 auth-port 2000 acct-port 2001
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined group servers.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

server (TACACS+)

To configure the IP address of the TACACS+ server for the group server, use the **server** command in TACACS+ group server configuration mode. To remove the IP address of the RADIUS server, use the **no** form of this command.

server *ip-address*

no server *ip-address*

Syntax Description

ip-address	IP address of the selected server.

Defaults

No default behavior or values.

Command Modes

TACACS+ group server configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

You must configure the **aaa group server tacacs** command before configuring this command.

Enter the **server** command to specify the IP address of the TACACS+ server. Also configure a matching **tacacs-server host** entry in the global list. If there is no response from the first host entry, the next host entry is tried.

Examples

The following example shows server host entries configured for the RADIUS server:

```
aaa new-model
aaa authentication ppp default group g1
aaa group server tacacs+ g1
 server 1.0.0.1
 server 2.0.0.1
tacacs-server host 1.0.0.1
tacacs-server host 2.0.0.1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
aaa server group	Groups different server hosts into distinct lists and distinct methods.
tacacs-server host	Specifies a RADIUS server host.

server-private (RADIUS)

To configure the IP address of the private RADIUS server for the group server, use the **server-private** command in server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no server-private *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Syntax Description

ip-address	IP address of the private RADIUS server host.
auth-port *port-number*	(Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port *port-number*	Optional) UDP destination port for accounting requests. The default value is 1646.
non-standard	(Optional) RADIUS server is using vendor-proprietary RADIUS attributes.
timeout *seconds*	(Optional) Time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used.
retransmit *retries*	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
key *string*	(Optional) Authentication and encryption key used between the router and the RADIUS daemon running on the RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used.

Defaults

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between Virtual Route Forwardings (VRFs), private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "radius" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

Examples

The following example shows how to define the sg_water RADIUS group server and associate private servers with it:

```
aaa group server radius sg_water
 server-private 10.1.1.1 timeout 5 retransmit 3 key coke
 server-private 10.2.2.2 timeout 5 retransmit 3 key coke
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

server-private (TACACS+)

To configure the IP address of the private TACACS+ server for the group server, use the **server-private** command in server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]

no server-private

Syntax Description

ip-address	IP address of the private RADIUS or TACACS+ server host.
name	Name of the private RADIUS or TACACS+ server host.
nat	(Optional) Port Network Address Translation (NAT) address of the remote device. This address is sent to the TACACS+ server.
single-connection	(Optional) Maintains a single open connection between the router and the TACACS+ server.
port *port-number*	(Optional) Specifies a server port number. This option overrides the default, which is port 49.
timeout *seconds*	(Optional) Specifies a timeout value. This overrides the global timeout value set with the **tacacs-server timeout** command for this server only.
key [**0** | **7**]	(Optional) Specifies an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command tacacs-server key for this server only. • If no number or 0 is entered, the string that is entered is considered to be plain text. If 7 is entered, the string that is entered is considered to be encrypted text.
string	(Optional) Character string specifying the authentication and encryption key.

Defaults

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes

Server-group configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between virtual route forwardings (VRFs), private servers (servers with private addresses) can be defined within the server group and remain hidden from

other groups, while the servers in the global pool (default "TACACS+" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

Examples

The following example shows how to define the tacacs1 TACACS+ group server and associate private servers with it:

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco

  ip vrf cisco
   rd 100:1

  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
ip tacacs source-interface	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.
tacacs-server host	Specifies a TACACS+ server host.

service password-encryption

To encrypt passwords, use the **service password-encryption** command in global configuration mode. To restore the default, use the **no** form of this command.

service password-encryption

no service password-encryption

Syntax Description

This command has no arguments or keywords.

Defaults

No encryption

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The actual encryption process occurs when the current configuration is written or when a password is configured. Password encryption is applied to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and Border Gateway Protocol neighbor passwords. This command is primarily useful for keeping unauthorized individuals from viewing your password in your configuration file.

When password encryption is enabled, the encrypted form of the passwords is displayed when a **more system:running-config** command is entered.

Caution This command does not provide a high level of network security. If you use this command, you should also take additional network security measures.

Note You cannot recover a lost encrypted password. You must clear NVRAM and set a new password.

Examples

The following example causes password encryption to take place:

```
service password-encryption
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
key-string (authentication)	Specifies the authentication string for a key.
neighbor password	Enables MD5 authentication on a TCP connection between two BGP peers.

set aggressive-mode client-endpoint

To specify the Tunnel-Client-Endpoint attribute within an Internet Security Association Key Management Protocol (ISAKMP) peer configuration, use the **set aggressive-mode client-endpoint** command in ISAKMP policy configuration mode. To remove this attribute from your configuration, use the **no** form of this command.

set aggressive-mode client-endpoint *client-endpoint*

no set aggressive-mode client-endpoint *client-endpoint*

Syntax Description

client-endpoint	One of the following identification types of the initiator end of the tunnel: • ID_IPV4 (IPV4 address) • ID_FQDN (fully qualified domain name, for example "green.cisco.com") • ID_USER_FQDN (e-mail address) The ID type is translated to the corresponding ID type in Internet Key Exchange (IKE).

Defaults

The Tunnel-Client-Endpoint attribute is not defined.

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Before you can use this command, you must enable the **crypto isakmp peer** command.

To initiate an IKE aggressive mode negotiation and specify the RADIUS Tunnel-Client-Endpoint attribute, the **set aggressive-mode client-endpoint** command, along with the **set aggressive-mode password** command, *must* be configured in the ISAKMP peer policy. The Tunnel-Client-Endpoint attribute will be communicated to the server by encoding it in the appropriate IKE identity payload.

Examples

The following example shows how to initiate aggressive mode using RADIUS tunnel attributes:

```
crypto isakmp peer address 10.4.4.1
 set aggressive-mode client-endpoint user-fqdn user@cisco.com
 set aggressive-mode password cisco123
```

Related Commands

Command	Description
crypto isakmp peer	Enables an IPSec peer for IKE querying of AAA for tunnel attributes in aggressive mode.
set aggressive-mode password	Specifies the Tunnel-Password attribute within an ISAKMP peer configuration.

set aggressive-mode password

To specify the Tunnel-Password attribute within an Internet Security Association Key Management Protocol (ISAKMP) peer configuration, use the **set aggressive-mode password** command in ISAKMP policy configuration mode. To remove this attribute from your configuration, use the **no** form of this command.

set aggressive-mode password *password*

no set aggressive-mode password *password*

Syntax Description

password	Password that is used to authenticate the peer to a remote server. The tunnel password is used as the Internet Key Exchange (IKE) preshared key.

Defaults

The Tunnel-Password attribute is not defined.

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(2)T	This command was modified so that output shows that the preshared key is either encrypted or unencrypted.

Usage Guidelines

Before you can use this command, you must enable the **crypto isakmp peer** command.

To initiate an IKE aggressive mode negotiation, the **set aggressive-mode password** command, along with the **set aggressive-mode client-endpoint** command, *must* be configured in the ISAKMP peer policy. The Tunnel-Password attribute will be used as the IKE preshared key for the aggressive mode negotiation.

Output for the **set aggressive-mode password** command will show that the preshared key is either unencrypted or encrypted. An output example for an unencrypted preshared key would be as follows:

```
set aggressive-mode password test123
```

An output example for a type 6 encrypted preshared key would be as follows:

set aggressive-mode password 6 DV’P[aTVWWbcgKU]T\T\QhZAAB

Examples

The following example shows how to initiate aggressive mode using RADIUS tunnel attributes:

```
Router (config)# crypto isakmp peer address 10.4.4.1
Router (config-isakmp-peer)# set aggressive-mode client-endpoint user-fqdn user@cisco.com
Router (config-isakmp-peer)# set aggressive-mode password cisco123
```

Related Commands

Command	Description
crypto isakmp peer	Enables an IPSec peer for IKE querying of AAA for tunnel attributes in aggressive mode.
set aggressive-mode client-endpoint	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.

set ip access-group

To check a preencrypted or postdecrypted packet against an access control list (ACL) without having to use the outside physical interface ACL, use the **set ip access-group** command in crypto map configuration mode. To disable the check, use the **no** form of this command.

set ip access-group {*access-list-number* | *access-list-name*} {**in** | **out**}

no set ip access-group {*access-list-number* | *access-list-name*} {**in** | **out**}

Syntax Description

access-list-number	Number of an access list. Values 100 through 199 are used for IP access lists (extended). The values 2000 through 2699 are used for expanded access lists (extended).
access-list-name	Name of an access list.
in	Sets access control for inbound clear-text packets (after decryption).
out	Sets access control for outbound clear-text packets (prior to encryption).

Defaults

No crypto map access ACLs are defined to filter clear-text packets going through the IPSec tunnel.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **set ip access-group** command is used after the crypto map has been configured.

Examples

The following example shows that a crypto map access ACL has been configured:

```
Router (config)# crypto map map vpn1 10
Router (config-crypto-map)# set ip access-group 151 in
```

Related Commands

Command	Description
crypto map	Assigns a previously defined crypto map set to an interface so that the interface can provide IPSec services.

set isakmp-profile

To set the Internet Security Association and Key Management Protocol (ISAKMP) profile name, use the **set isakmp-profile** command in crypto map configuration mode. To remove the ISAKMP profile name, use the **no** form of this command.

set isakmp-profile *profile-name*

no set isakmp-profile *profile-name*

Syntax Description

profile-name	Name of the ISAKMP profile.

Defaults

If the ISAKMP profile is not specified in the crypto map entry, the default is to the ISAKMP profile that is on the head. If there is no ISAKMP profile on the head, the default is "none."

Command Modes

Crypto map configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command describes the ISAKMP profile to use when you start the Internet Key Exchange (IKE) exchange.

Before configuring an ISAKMP profile on a crypto map, you should set up the ISAKMP profile.

Examples

The following example shows that an ISAKMP profile has been configured on a crypto map:

```
crypto map vpnmap 10 ipsec-isakmp
 set isakmp-profile vpnprofile
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set, which is an acceptable combination of security protocols and algorithms.
crypto map (global)	Creates or modifies a crypto map entry.

set peer (IPSec)

To specify an IP Security (IPSec) peer in a crypto map entry, use the **set peer** command in crypto map configuration mode. To remove an IPSec peer from a crypto map entry, use the **no** form of this command.

set peer {*host-name* [**dynamic**] | *ip-address*}

no set peer {*host-name* [**dynamic**] | *ip-address*}

Syntax Description

host-name	Specifies the IPSec peer by its host name. This is the peer's host name concatenated with its domain name (for example, myhost.example.com).
dynamic	(Optional) The host name of the IPSec peer will be resolved via a domain name server (DNS) lookup right before the router establishes the IPSec tunnel.
ip-address	Specifies the IPSec peer by its IP address.

Defaults

No peer is defined

Command Modes

Crypto map configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(4)T	The **dynamic** keyword was added.

Usage Guidelines

Use this command to specify an IPSec peer for a crypto map.

This command is required for all static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required, and in most cases is not used (because, in general, the peer is unknown).

For crypto map entries created with the **crypto map** *map-name seq-num* **ipsec-isakmp** command, you can specify multiple peers by repeating this command. The peer that packets are actually sent to is determined by the last peer that the router heard from (received either traffic or a negotiation request from) for a given data flow. If the attempt fails with the first peer, Internet Key Exchange (IKE) tries the next peer on the crypto map list.

For crypto map entries created with the **crypto map** *map-name seq-num* **ipsec-manual** command, you can specify only one IPSec peer per crypto map. If you want to change the peer, you must first delete the old peer and then specify the new peer.

You can specify the remote IPSec peer by its host name only if the host name is mapped to the peer's IP address in a DNS or if you manually map the host name to the IP address with the **ip host** command.

The dynamic Keyword

When specifying the host name of a remote IPSec peer via the **set peer** command, you can also issue the **dynamic** keyword, which defers DNS resolution of the host name until right before the IPSec tunnel has been established. Deferring resolution enables the Cisco IOS software to detect whether the IP address of the remote IPSec peer has changed. Thus, the software can contact the peer at the new IP address.

If the **dynamic** keyword is not issued, the host name is resolved immediately after it is specified. So, the Cisco IOS software cannot detect an IP address change and, therefore, attempts to connect to the IP address that it previously resolved.

Examples

The following example shows a crypto map configuration when IKE will be used to establish the security associations (SAs). In this example, an SA could be set up to either the IPSec peer at 10.0.0.1 or the peer at 10.0.0.2.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2\
```

The following example shows how to configure a router to perform real-time DNS resolution with a remote IPSec peer; that is, the host name of peer is resolved via a DNS lookup right before the router establishes a connection (an IPSec tunnel) with the peer.

```
crypto map secure_b 10 ipsec-isakmp
  match address 140
  set peer b.cisco.com dynamic
  set transform-set xset
interface serial1
  ip address 30.0.0.1
  crypto map secure_b
access-list 140 permit ...
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set pfs	Specifies that IPSec should ask for PFS when requesting new SAs for this crypto map entry, or that IPSec requires PFS when receiving requests for new SAs.
set security-association level per-host	Specifies that separate IPSec SAs should be requested for each source/destination host pair.

Command	Description
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec SAs.
set session-key	Specifies the IPSec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

set pfs

To specify that IP Security (IPSec) should ask for perfect forward secrecy (PFS) when requesting new security associations for this crypto map entry, or that IPSec requires PFS when receiving requests for new security associations, use the **set pfs** command in crypto map configuration mode. To specify that IPSec should not request PFS, use the **no** form of this command.

set pfs [**group1** | **group2**]

no set pfs

Syntax Description

group1	(Optional) Specifies that IPSec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group2	(Optional) Specifies that IPSec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

Defaults

By default, PFS is not requested. If no group is specified with this command, **group1** is used as the default.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command is only available for **ipsec-isakmp** crypto map entries and dynamic crypto map entries.

During negotiation, this command causes IPSec to request PFS when requesting new security associations for the crypto map entry. The default (**group1**) is sent if the **set pfs** statement does not specify a group. If the peer initiates the negotiation and the local configuration specifies PFS, the remote peer must perform a PFS exchange or the negotiation will fail. If the local configuration does not specify a group, a default of **group1** will be assumed, and an offer of either **group1** or **group2** will be accepted. If the local configuration specifies **group2**, that group *must* be part of the peer's offer or the negotiation will fail. If the local configuration does not specify PFS it will accept any offer of PFS from the peer.

PFS adds another level of security because if one key is ever cracked by an attacker then only the data sent with that key will be compromised. Without PFS, data sent with other keys could be also compromised.

With PFS, every time a new security association is negotiated, a new Diffie-Hellman exchange occurs. (This exchange requires additional processing time.)

The 1024-bit Diffie-Hellman prime modulus group, **group2**, provides more security than **group1**, but requires more processing time than **group1**.

Examples

The following example specifies that PFS should be used whenever a new security association is negotiated for the crypto map "mymap 10":

```
crypto map mymap 10 ipsec-isakmp
 set pfs group2
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set security-association level per-host	Specifies that separate IPSec security associations should be requested for each source/destination host pair.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

set security-association level per-host

To specify that separate IP Security security associations should be requested for each source/destination host pair, use the **set security-association level per-host** command in crypto map configuration mode. To specify that one security association should be requested for each crypto map access list **permit** entry, use the **no** form of this command.

set security-association level per-host

no set security-association level per-host

Syntax Description

This command has no arguments or keywords.

Defaults

For a given crypto map, all traffic between two IPSec peers matching a single crypto map access list **permit** entry will share the same security association.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command is only available for **ipsec-isakmp** crypto map entries and is not supported for dynamic crypto map entries.

When you use this command, you need to specify that a separate security association should be used for each source/destination host pair.

Normally, within a given crypto map, IPSec will attempt to request security associations at the granularity specified by the access list entry. For example, if the access list entry permits IP protocol traffic between subnet A and subnet B, IPSec will attempt to request security associations between subnet A and subnet B (for any IP protocol), and unless finer-grained security associations are established (by a peer request), all IPSec-protected traffic between these two subnets would use the same security association.

This command causes IPSec to request separate security associations for each source/destination host pair. In this case, each host pairing (where one host was in subnet A and the other host was in subnet B) would cause IPSec to request a separate security association.

With this command, one security association would be requested to protect traffic between host A and host B, and a different security association would be requested to protect traffic between host A and host C.

The access list entry can specify local and remote subnets, or it can specify a host-and-subnet combination. If the access list entry specifies protocols and ports, these values are applied when establishing the unique security associations.

Use this command with care, as multiple streams between given subnets can rapidly consume system resources.

Examples

The following example shows what happens with an access list entry of **permit ip 1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255** and a per-host level:

- A packet from 1.1.1.1 to 2.2.2.1 will initiate a security association request, which would look like it originated via **permit ip host 1.1.1.1 host 2.2.2.1**.
- A packet from 1.1.1.1 to 2.2.2.2 will initiate a security association request, which would look like it originated via **permit ip host 1.1.1.1 host 2.2.2.2**.
- A packet from 1.1.1.2 to 2.2.2.1 will initiate a security association request, which would look like it originated via **permit ip host 1.1.1.2 host 2.2.2.1**.

Without the per-host level, any of the above packets will initiate a single security association request originated via **permit ip 1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255**.

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for PFS when requesting new security associations for this crypto map entry, or that IPSec requires PFS when receiving requests for new security associations.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

set security-association lifetime

To override (for a particular crypto map entry) the global lifetime value, which is used when negotiating IP Security security associations, use the **set security-association lifetime** command in crypto map configuration mode. To reset a crypto map entry's lifetime value to the global value, use the **no** form of this command.

set security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes*}

no set security-association lifetime {**seconds** | **kilobytes**}

Syntax Description

seconds *seconds*	Specifies the number of seconds a security association will live before expiring.
kilobytes *kilobytes*	Specifies the volume of traffic (in kilobytes) that can pass between IPSec peers using a given security association before that security association expires.

Defaults

The crypto map's security associations are negotiated according to the global lifetimes.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command is available only for **ipsec-isakmp** crypto map entries and dynamic crypto map entries.

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the router requests new security associations during security association negotiation, it will specify its crypto map lifetime value in the request to the peer; it will use this value as the lifetime of the new security associations. When the router receives a negotiation request from the peer, it will use the smaller of the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

There are two lifetimes: a "timed" lifetime and a "traffic-volume" lifetime. The session keys/security association expires after the first of these lifetimes is reached.

If you change a lifetime, the change will not be applied to existing security associations, but will be used in subsequent negotiations to establish security associations for data flows supported by this crypto map entry. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command. Refer to the **clear crypto sa** command for more detail.

To change the timed lifetime, use the **set security-association lifetime seconds** form of the command. The timed lifetime causes the keys and security association to time out after the specified number of seconds have passed.

To change the traffic-volume lifetime, use the **set security-association lifetime kilobytes** form of the command. The traffic-volume lifetime causes the key and security association to time out after the specified amount of traffic (in kilobytes) has been protected by the security association's key.

Shorter lifetimes can make it harder to mount a successful key recovery attack, because the attacker has less data encrypted under the same key to work with. However, shorter lifetimes need more CPU processing time.

The lifetime values are ignored for manually established security associations (security associations installed via an **ipsec-manual** crypto map entry).

How These Lifetimes Work

Assuming that the particular crypto map entry does not have lifetime values configured, when the router requests new security associations it will specify its global lifetime values in the request to the peer; it will use this value as the lifetime of the new security associations. When the router receives a negotiation request from the peer, it will use the smaller of either the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

The security association (and corresponding keys) will expire according to whichever occurs sooner, either after the **seconds** time out or after the **kilobytes** amount of traffic is passed.

A new security association is negotiated *before* the lifetime threshold of the existing security association is reached, to ensure that a new security association is ready for use when the old one expires. The new security association is negotiated either 30 seconds before the **seconds** lifetime expires or when the volume of traffic through the tunnel reaches 256 kilobytes less than the **kilobytes** lifetime (whichever occurs first).

If no traffic has passed through the tunnel during the entire life of the security association, a new security association is not negotiated when the lifetime expires. Instead, a new security association will be negotiated only when IPSec sees another packet that should be protected.

Examples

The following example shortens the timed lifetime for a particular crypto map entry, because there is a higher risk that the keys could be compromised for security associations belonging to the crypto map entry. The traffic-volume lifetime is not changed because there is not a high volume of traffic anticipated for these security associations. The timed lifetime is shortened to 2700 seconds (45 minutes).

```
crypto map mymap 10 ipsec-isakmp
 set security-association lifetime seconds 2700
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto ipsec security-association lifetime	Changes global lifetime values used when negotiating IPSec security associations.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.

Command	Description
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for PFS when requesting new security associations for this crypto map entry, or that IPSec requires PFS when receiving requests for new security associations.
set security-association level per-host	Specifies that separate IPSec security associations should be requested for each source/destination host pair.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

set session-key

To manually specify the IP Security session keys within a crypto map entry, use the **set session-key** command in crypto map configuration mode. This command is available only for **ipsec-manual** crypto map entries. To remove IPSec session keys from a crypto map entry, use the **no** form of this command.

Authentication Header (AH) Protocol Syntax

set session-key {**inbound** | **outbound**} **ah** *spi hex-key-string*

no set session-key {**inbound** | **outbound**} **ah**

Encapsulation Security Protocol (ESP) Syntax

set session-key {**inbound** | **outbound**} **esp** *spi cipher hex-key-string* [**authenticator** *hex-key-string*]

no set session-key {**inbound** | **outbound**} **esp**

Syntax Description

inbound	Sets the inbound IPSec session key. (You must set both inbound and outbound keys.)
outbound	Sets the outbound IPSec session key. (You must set both inbound and outbound keys.)
ah	Sets the IPSec session key for the AH protocol. Use when the crypto map entry's transform set includes an AH transform.
esp	Sets the IPSec session key for ESP. Use when the crypto map entry's transform set includes an ESP transform.
spi	Specifies the security parameter index (SPI), a number that is used to uniquely identify a security association. The SPI is an arbitrary number you assign in the range of 256 to 4,294,967,295 (FFFF FFFF). You can assign the same SPI to both directions and both protocols. However, not all peers have the same flexibility in SPI assignment. For a given destination address/protocol combination, unique SPI values must be used. The destination address is that of the router if inbound, the peer if outbound.
hex-key-string	Specifies the session key; enter in hexadecimal format. This is an arbitrary hexadecimal string of 8, 16, or 20 bytes. If the crypto map's transform set includes a DES algorithm, specify at least 8 bytes per key. If the crypto map's transform set includes an MD5 algorithm, specify at least 16 bytes per key. If the crypto map's transform set includes an SHA algorithm, specify 20 bytes per key. Keys longer than the above sizes are simply truncated.
cipher	Indicates that the key string is to be used with the ESP encryption transform.
authenticator	(Optional) Indicates that the key string is to be used with the ESP authentication transform. This argument is required only when the crypto map entry's transform set includes an ESP authentication transform.

Defaults

No session keys are defined by default.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command to define IPSec keys for security associations via **ipsec-manual** crypto map entries. (In the case of **ipsec-isakmp** crypto map entries, the security associations with their corresponding keys are automatically established via the IKE negotiation.)

If the crypto map's transform set includes an AH protocol, you must define IPSec keys for AH for both inbound and outbound traffic. If the crypto map's transform set includes an ESP encryption protocol, you must define IPSec keys for ESP encryption for both inbound and outbound traffic. If your transform set includes an ESP authentication protocol, you must define IPSec keys for ESP authentication for inbound and outbound traffic.

When you define multiple IPSec session keys within a single crypto map, you can assign the same security parameter index (SPI) number to all the keys. The SPI is used to identify the security association used with the crypto map. However, not all peers have the same flexibility in SPI assignment. You should coordinate SPI assignment with your peer's operator, making certain that the same SPI is not used more than once for the same destination address/protocol combination.

Security associations established via this command do not expire (unlike security associations established via IKE).

Session keys at one peer must match the session keys at the remote peer.

If you change a session key, the security association using the key will be deleted and reinitialized.

Examples

The following example shows a crypto map entry for manually established security associations. The transform set "t_set" includes only an AH protocol.

```
crypto ipsec transform-set t_set ah-sha-hmac

crypto map mymap 20 ipsec-manual
 match address 102
 set transform-set t_set
 set peer 10.0.0.21
 set session-key inbound ah 300 1111111111111111111111111111111111111111
 set session-key outbound ah 300 2222222222222222222222222222222222222222
```

The following example shows a crypto map entry for manually established security associations. The transform set "someset" includes both an AH and an ESP protocol, so session keys are configured for both AH and ESP for both inbound and outbound traffic. The transform set includes both encryption and authentication ESP transforms, so session keys are created for both using the **cipher** and **authenticator** keywords.

```
crypto ipsec transform-set someset ah-sha-hmac esp-des esp-sha-hmac

crypto map mymap 10 ipsec-manual
 match address 101
 set transform-set someset
```

```
set peer 10.0.0.1
set session-key inbound ah 300 9876543210987654321098765432109876543210
set session-key outbound ah 300 fedcbafedcbafedcbafedcbafedcbafedcbafedc
set session-key inbound esp 300 cipher 0123456789012345
 authenticator 00001111222233334444555566667777888899999
set session-key outbound esp 300 cipher abcdefabcdefabcd
 authenticator 99998888777766665555444433332222111110000
```

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

set transform-set

To specify which transform sets can be used with the crypto map entry, use the **set transform-set** command in crypto map configuration mode. To remove all transform sets from a crypto map entry, use the **no** form of this command.

set transform-set *transform-set-name* [*transform-set-name2...transform-set-name6*]

no set transform-set

Syntax Description

transform-set-name	Name of the transform set. For an **ipsec-manual** crypto map entry, you can specify only one transform set. For an **ipsec-isakmp** or dynamic crypto map entry, you can specify up to six transform sets.

Defaults

No transform sets are included by default.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command is required for all static and dynamic crypto map entries.

Use this command to specify which transform sets to include in a crypto map entry.

For an **ipsec-isakmp** crypto map entry, you can list multiple transform sets with this command. List the higher priority transform sets first.

If the local router initiates the negotiation, the transform sets are presented to the peer in the order specified in the crypto map entry. If the peer initiates the negotiation, the local router accepts the first transform set that matches one of the transform sets specified in the crypto map entry.

The first matching transform set that is found at both peers is used for the security association. If no match is found, IPSec will not establish a security association. The traffic will be dropped because there is no security association to protect the traffic.

For an **ipsec-manual** crypto map entry, you can specify only one transform set. If the transform set does not match the transform set at the remote peer's crypto map, the two peers will fail to correctly communicate because the peers are using different rules to process the traffic.

If you want to change the list of transform sets, re-specify the new list of transform sets to replace the old list. This change is only applied to crypto map entries that reference this transform set. The change will not be applied to existing security associations, but will be used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command.

Any transform sets included in a crypto map must previously have been defined using the **crypto ipsec transform-set** command.

Examples

The following example defines two transform sets and specifies that they can both be used within a crypto map entry. (This example applies only when IKE is used to establish security associations. With crypto maps used for manually established security associations, only one transform set can be included in a given crypto map entry.)

```
crypto ipsec transform-set my_t_set1 esp-des esp-sha-hmac
crypto ipsec transform-set my_t_set2 ah-sha-hmac esp-des esp-sha-hmac

crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.1
 set peer 10.0.0.2
```

In this example, when traffic matches access list 101, the security association can use either transform set “my_t_set1” (first priority) or “my_t_set2” (second priority) depending on which transform set matches the remote peer’s transform sets.

sgbp aaa authetication

To enable a Stack Group Bidding Protocol (SGBP) authentication list, use the **sgbp aaa authentication** command in global configuration mode. To disable the SGBP authentication list, use the **no** form of this command.

sgbp aaa authentication list *list-name*

no sgbp aaa authentication list *list-name*

Syntax Description

list *list-name*	Name of a list of methods of authentication to use.

Defaults

A SGBP authentication list is not enabled. You must use the same authentication, authorization and accounting (AAA) method list as PPP usersl.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command introduced.

Usage Guidelines

Use the **sgbp aaa authentication** command to create a list different from the AAA list that is used by PPP users.

Examples

The following example shows how to create the AAA list "SGBP" that is to be used by SGBP users:

```
Router(config)# sgbp aaa authentication list SGBP
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
aaa authentication sgbp	Specifies one or more AAA authentication methods for SGBP.
ppp authentication	Enables at least one PPP authentication protocol and to specifies the order in which the protocols are selected on the interface.

show aaa attributes

To display the mapping between an authentication, authorization, and accounting (AAA) attribute number and the corresponding AAA attribute name, use the **show aaa attributes** command in EXEC configuration mode.

show aaa sttributes [**protocol radius**]

Syntax Description

protocol radius	(Optional) Displays the mapping between a RADIUS attribute and a AAA attribute name and number.

Command Modes

EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	The **protocol** and **radius** keywords were added.

Examples

The following example is sample output for the **show aaa attributes** command. In this example, all RADIUS attributes that have been enabled are displayed.

```
Router# show aaa attributes protocol radius

AAA ATTRIBUTE LIST:
    Type=1     Name=disc-cause-ext                Format=Enum
        Protocol:RADIUS
        Non-Standard  Type=195   Name=Ascend-Disconnect-Cau Format=Enum
        Cisco VSA     Type=1     Name=Cisco AVpair          Format=String
    Type=2     Name=Acct-Status-Type              Format=Enum
        Protocol:RADIUS
        IETF          Type=40    Name=Acct-Status-Type      Format=Enum
    Type=3     Name=acl                           Format=Ulong
        Protocol:RADIUS
        IETF          Type=11    Name=Filter-Id             Format=Binary
    Type=4     Name=addr                          Format=IPv4 Address
        Protocol:RADIUS
        IETF          Type=8     Name=Framed-IP-Address     Format=IPv4 Addre
    Type=5     Name=addr-pool                     Format=String
        Protocol:RADIUS
        Non-Standard  Type=218   Name=Ascend-IP-Pool        Format=Ulong
    Type=6     Name=asyncmap                      Format=Ulong
        Protocol:RADIUS
        Non-Standard  Type=212   Name=Ascend-Asyncmap       Format=Ulong
    Type=7     Name=Authentic                     Format=Enum
        Protocol:RADIUS
        IETF          Type=45    Name=Authentic             Format=Enum
    Type=8     Name=autocmd                       Format=String
```

show aaa cache filterserver

To display the cache status, use the **show aaa cache filterserver** command in EXEC mode.

show aaa cache filterserver

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The **show aaa cache filterserver** command shows how many times a particular filter has been referenced or refreshed. This function may be used in administration to determine which filters are actually being used.

Examples

The following is sample output for the **show aaa cache filterserver** command:

```
Router# show aaa cache filterserver

Filter     Server          Age Expires Refresh Access-Control-Lists
-------------------------------------------------------------------------------
aol        1.2.3.4           0    1440     100 ip in icmp drop
                                               ip out icmp drop
                                               ip out forward tcp dstip 1.2.3...
msn        1.2.3.4         N/A   Never       2 ip in tcp drop
msn2       1.2.3.4         N/A   Never       2 ip in tcp drop
vone       1.2.3.4         N/A   Never       0 ip in tcp drop
```

Table 29 describes the significant fields shown in the display.

Table 29 show aaa cache filterserver Command Field Descriptions

Field	Description
Filter	Filter name.
Server	RADIUS server IP address.
Age	When to expire a cache entry.
Expires	Number of minutes in which a cache entry will expire.
Refresh	Number of times a cache has been refreshed.
Access-Control-Lists	Access control list (ACL) of the server.

Related Commands

Command	Description
aaa authorization cache filterserver	Enables AAA authorization caches and the downloading of ACL configurations from a RADIUS filter server.

show aaa dead-criteria

To display dead-criteria detection information for an authentication, authorization, and accounting (AAA) server, use the **show aaa dead-criteria** command in privileged EXEC mode.

show aaa dead-criteria {security-protocol *ip-address}* [**auth-port** *port-number*] [**acct-port** *port-number*] [*server-group-name*]

Syntax Description

security-protocol	Security protocol of the specified AAA server. Currently, the only protocol that is supported is RADIUS.
ip-address	IP address of the specified AAA server.
auth-port	(Optional) Authentication port for the RADIUS server that was specified.
port-number	(Optional) Number of the authentication port. The default is 1645 (for a RADIUS server).
acct-port	(Optional) Accounting port for the RADIUS server that was specified.
port-number	(Optional) Number of the accounting port. The default is 1646 (for a RADIUS server).
server-group-name	(Optional) Server group with which the specified server is associated. The default is “radius” (for a RADIUS server).

Defaults

Currently, the *port-number* argument for the **auth-port** keyword and the *port-number* argument for the **acct-port** keyword default to 1645 and 1646, respectively. The default for the *server-group-name* argument is radius.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(6)	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Multiple RADIUS servers having the same IP address can be configured on a router. The **auth-port** and **acct-port** keywords are used to differentiate the servers. The dead-detect interval of a server that is associated with a specified server group can be obtained by using the **server-group-name** keyword. (The dead-detect interval and retransmit values of a RADIUS server are set on the basis of the server group to which the server belongs. The same server can be part of multiple server groups.)

Examples

The following example shows that dead-criteria-detection information has been requested for a RADIUS server at the IP address 172.19.192.80:

```
Router# show aaa dead-criteria radius 172.19.192.80 radius

RADIUS Server Dead Critieria:
```

```
============================
Server Details:
    Address : 172.19.192.80
    Auth Port : 1645
    Acct Port : 1646
Server Group : radius
Dead Criteria Details:
    Configured Retransmits : 62
    Configured Timeout : 27
    Estimated Outstanding Transactions: 5
    Dead Detect Time : 25s
    Computed Retransmit Tries: 22
    Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 5
Max Computed Dead Detect Time: 25s
Max Computed Retransmits : 22
```

The “Max Computed Dead Detect Time” is displayed in seconds. The other fields shown in the display are self-explanatory.

Related Commands

Command	Description
debug aaa dead-criteria transactions	Displays AAA dead-criteria transaction values.
radius-server dead-criteria	Forces one or both of the criteria—used to mark a RADIUS server as dead—to be the indicated constant.
show aaa server-private	Displays the status of all private RADIUS servers.
show aaa servers	Displays information about the number of packets sent to and received from AAA servers.

show aaa server-private

To display the status of all private RADIUS servers, use the **show aaa server-private** command in user EXEC or privileged EXEC mode.

show aaa server-private

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC or privileged EXEC

Command History

Release	Modification
12.3	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Examples

The following is sample output from the **show aaa server-private** command. Only the first four lines of the display pertain to the status of private RADIUS servers, and the fields in this part of the display are described in Table 30.

```
Router# show aaa server-private

RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645,
acct-port 1646
      State: current UP, duration 18s, previous duration 0s
      Dead: total time 0s, count 0
      Authen: request 0, timeouts 0
              Response: unexpected 0, server error 0, incorrect 0, time 0ms
              Transaction: success 0, failure 0
      Author: request 0, timeouts 0
              Response: unexpected 0, server error 0, incorrect 0, time 0ms
              Transaction: success 0, failure 0
      Account: request 0, timeouts 0
              Response: unexpected 0, server error 0, incorrect 0, time 0ms
              Transaction: success 0, failure 0
      Elapsed time since counters last cleared: 2h1m
```

Table 30 describes the significant fields in the display.

Table 30 show aaa server-private Command Field Descriptions

Field	Description
id	A unique identifier for all AAA servers defined on the router.
priority	The order of use for servers within a group.
host	IP address of the private RADIUS server host.
auth-port	User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port	UDP destination port for accounting requests. The default value is 1646.

Table 30 show aaa server-private Command Field Descriptions

Field	Description
State	Describes the current state of the server; the duration, in seconds, that the server has been in that state; and the duration, in seconds, that the server was in the previous state.
Dead	Indicates the number of times that this server has been marked dead and the cumulative amount of time, in seconds, that it spent in that state.

Related Commands

Command	Description
radius-server dead-criteria	Forces one or both of the criteria—used to mark a RADIUS server as dead—to be the indicated constant.
server-private	Associates a particular private RADIUS server with a defined server group.
show aaa server-private	Displays the status of all private RADIUS servers.
show aaa servers	Displays information about the number of packets sent to and received from AAA servers.

show aaa servers

To display information about the number of packets sent to and received from authentication, authorization, and accounting (AAA) servers, use the **show aaa servers** command in user EXEC and privileged EXEC mode.

show aaa servers

Syntax Description

This command has no arguments or keywords.

Command Modes

User and privileged EXEC

Command History

Release	Modification
12.2(6)T	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Only RADIUS servers are supported by the **show aaa servers** command.

The command displays information about packets sent and received for all AAA transaction types—authentication, authorization, and accounting.

Examples

The following is sample output from the **show aaa servers** command:

```
Router# show aaa servers

RADIUS: id 1, priority 1, host 172.19.192.238, auth-port 2195, acct-port 2196
     State: current UP, duration 323109s, previous duration 0s
     Dead: total time 0s, count 1
     Authen: request 0, timeouts 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
     Author: request 0, timeouts 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
     Account: request 6, timeouts 5
             Response: unexpected 0, server error 0, incorrect 1, time 20ms
             Transaction: success 1, failure 2
     Elapsed time since counters last cleared: 3d17h45m
```

The fields in the output are mapped to Simple Network Management Protocol (SNMP) objects in the Cisco AAA-SERVER-MIB and are used in SNMP reporting. The first line of the report is mapped to the Cisco AAA-SERVER-MIB as follows:

- id maps to casIndex
- priority maps to casPriority
- host maps to casAddress
- auth-port maps to casAuthenPort

- acct-port maps to casAcctPort

Mapping the following set of objects listed in the Cisco AAA-SERVER-MIB map to fields displayed by the **show aaa servers** command is more straightforward. For example, the casAuthenRequests field corresponds to the Authen: request portion of the report, casAuthenRequestTimeouts corresponds to the Authen: timeouts portion of the report, and so on.

```
casStatisticsGroup OBJECT-GROUP
    OBJECTS{
        casAuthenRequests,
        casAuthenRequestTimeouts,
        casAuthenUnexpectedResponses,
        casAuthenServerErrorResponses,
        casAuthenIncorrectResponses,
        casAuthenResponseTime,
        casAuthenTransactionSuccesses,
        casAuthenTransactionFailures,
        casAuthorRequests,
        casAuthorRequestTimeouts,
        casAuthorUnexpectedResponses,
        casAuthorServerErrorResponses,
        casAuthorIncorrectResponses,
        casAuthorResponseTime,
        casAuthorTransactionSuccesses,
        casAuthorTransactionFailures,
        casAcctRequests,
        casAcctRequestTimeouts,
        casAcctUnexpectedResponses,
        casAcctServerErrorResponses,
        casAcctIncorrectResponses,
        casAcctResponseTime,
        casAcctTransactionSuccesses,
        casAcctTransactionFailures,
        casState,
        casCurrentStateDuration,
        casPreviousStateDuration,
        casTotalDeadTime,
        casDeadCount
    }
```

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:
http://www.cisco.com/go/mibs

Table 31 describes the significant fields in the display.

Table 31 show aaa servers Command Field Descriptions

Field	Description
id	An identifier that uniquely identifies the server on the router.
priority	The priority by which the server will be tried within the server group.
host	The IP address of the AAA server.
auth-port	The port on the AAA server that is used for authentication and authorization requests.
acct-port	The port on the AAA server that is used for accounting requests.

Table 31 show aaa servers Command Field Descriptions

Field	Description
State	Indicates the assumed state of the AAA server. The following states are possible: • UP—Indicates that the server is currently considered alive and attempts will be made to communicate with it. • DEAD—Indicates that the server is currently presumed dead and, in the case of failovers, this server will be skipped unless it is the last server in the group. • duration—Is the amount of time the server is assumed to be in the current state, either UP or DEAD. • previous duration—Is the amount of time the server was considered to be in the previous state.
Dead	Indicates the number of times that this server has been marked dead, and the cumulative amount of time, in seconds, that it spent in that state.

Table 31 show aaa servers Command Field Descriptions

Field	Description
Authen	Provides information about authentication packets that were sent to and received from the server, and authentication transactions that were successful or that failed. The following information may be reported in this field: • request—Number of authentication requests that were sent to the AAA server. • timeouts—Number of timeouts (no responses) that were observed, when a transmission was sent to this server. • Response—Provides statistics about responses that were observed from this server and includes the following reports: – unexpected—Number of unexpected responses. A response is considered unexpected when it is received *after* the timeout period for the packet has expired. This may happen if the link to the server is severely congested, for example. An unexpected response can also be produced when a server generates a response for no apparent reason. – server error—Number of server errors. This category is a catch-all for error packets that do not fall into one of the previous categories. – incorrect—Number of incorrect responses. A response is considered incorrect if it is of the wrong format expected by the protocol. This frequently happens when an incorrect server key is configured on the router. • Transaction: These fields provide information about authentication, authorization, and accounting transactions related to the server. A transaction is defined as a request for authentication, authorization, or accounting information that is sent by the AAA module, or by an AAA client (such as PPP) to an AAA protocol (RADIUS or TACACS+), which may involve multiple packet transmissions and retransmissions. Transactions may require packet retransmissions to one or more servers in a single server group, to verify success or failure. Success or failure is reported to AAA by the RADIUS and TACACS+ protocols, as follows – success—Incremented when a transaction is successful. – failure—Incremented when a transaction fails (for example, packet retransmissions to another server in the server group failed due to failover or did not succeed. (A negative response to an Access-Request, such as Access-Reject, is considered to be a *successful* transaction).
Author	The fields in this category are similar to those in the Authen: fields. An important difference, however, is that because authorization information is carried in authentication packets for the RADIUS protocol, these fields are not incremented when using RADIUS.

Table 31 show aaa servers Command Field Descriptions

Field	Description
Account	The fields in this category are similar to those in the Authen: fields, but provide accounting transaction and packet statistics.
Elapsed time since counters last cleared	Displays the amount of time in days, hours, and minutes that have passed since the counters were last cleared.

Related Commands

Command	Description
show aaa server-private	Displays the status of all private RADIUS servers.

show aaa user

To display attributes related to an authentication, authorization, and accounting (AAA) session, use the **show aaa user** command in privileged EXEC mode.

show aaa user {all | *unique id***}**

Syntax Description

all	Displays information about all users for which AAA currently has knowledge.
unique id	Displays information for only this user.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

When a user logs into a Cisco router and uses AAA, a unique ID is assigned to the session. Throughout the life of the session, various attributes that are related to the session are collected and stored internally within a AAA database. These attributes can include the IP address of the user, the protocol being used to access the router (such as PPP or Serial Line Internet Protocol [SLIP]), the speed of the connection, and the number of packets or bytes that are received or transmitted.

The output of this command provides a snapshot of various subdatabases that are associated with a AAA unique ID. Some of the more important ones are listed in Table 32.

The output also shows various AAA call events that are associated with a particular session. For example, when a session comes up, the events generally recorded are CALL START, NET UP, and IP Control Protocol UP (IPCP UP).

In addition, the output provides a snapshot of the dynamic attributes that are associated with a particular session. (Dynamic attributes are those that keep changing values throughout the life of the session.) Some of the more important ones are listed in Table 32.

The unique ID of a session can be obtained from the output of the **show aaa sessions** command.

Note This command does not provide information for all users who are logged into a device, but for only those who have been authenticated or authorized using AAA or for only those whose sessions are being accounted for by the AAA module.

Note Using the **all** keyword can produce a large amount of output, depending on the number of users who are logged into the device at any given time.

Examples

The following example shows that information is requested for all users:

```
Router# show aaa user all
```

The following example shows that information is requested for user 5:

```
Router# show aaa user 5
```

The following is sample output from the **show aaa user** command. The session information displayed is for a PPP over Ethernet over Ethernet (PPPoEoE) session.

```
Router# show aaa user 3

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *20:32:49.199 PST Wed Dec 17
2003

  Unique id 3 is currently in use.
  Accounting:
    log=0x20C201
    Events recorded :
      CALL START
      NET UP
      IPCP_PASS
      INTERIM START
      VPDN NET UP
  update method(s) :
    NONE
  update interval = 0
  Outstanding Stop Records : 0
  Dynamic attribute list:
    63CCF138 0 00000001 connect-progress(30) 4 LAN Ses Up
    63CCF14C 0 00000001 pre-session-time(239) 4 3(3)
    63CCF160 0 00000001 nas-tx-speed(337) 4 102400000(61A8000)
    63CCF174 0 00000001 nas-rx-speed(33) 4 102400000(61A8000)
    63CCF188 0 00000001 elapsed_time(296) 4 2205(89D)
    63CCF19C 0 00000001 bytes_in(97) 4 6072(17B8)
    63CCF1B0 0 00000001 bytes_out(223) 4 6072(17B8)
    63CCF1C4 0 00000001 pre-bytes-in(235) 4 86(56)
    63CCF1D8 0 00000001 pre-bytes-out(236) 4 90(5A)
    63CCF1EC 0 00000001 paks_in(98) 4 434(1B2)
    63CCF244 0 00000001 paks_out(224) 4 434(1B2)
    63CCF258 0 00000001 pre-paks-in(237) 4 7(7)
    63CCF26C 0 00000001 pre-paks-out(238) 4 9(9)
  No data for type EXEC
  No data for type CONN
  NET: Username=peer1
    Session Id=00000003 Unique Id=00000003
    Start Sent=1 Stop Only=N
    stop_has_been_sent=N
    Method List=63B4A10C : Name = default
    Attribute list:
    63CCF138 0 00000001 session-id(293) 4 3(3)
    63CCF14C 0 00000001 Framed-Protocol(62) 4 PPP
    63CCF160 0 00000001 protocol(241) 4 ip
    63CCF174 0 00000001 addr(5) 4 70.0.0.1
  No data for type CMD
  No data for type SYSTEM
  No data for type RM CALL
  No data for type RM VPDN
  No data for type AUTH PROXY
  No data for type IPSEC-TUNNEL
  No data for type RESOURCE
  No data for type 10
  No data for type CALL
Debg: No data available
Radi: 641AACAC
```

```
Interface:
  TTY Num = -1
  Stop Received = 0
  Byte/Packet Counts till Call Start:
    Start Bytes In = 106      Start Bytes Out = 168
    Start Paks    In = 3      Start Paks  Out = 4
  Byte/Packet Counts till Service Up:
    Pre Bytes In = 192      Pre Bytes Out = 258
    Pre Paks  In = 10      Pre Paks  Out = 13
  Cumulative Byte/Packet Counts :
    Bytes In = 6264      Bytes Out = 6330
    Paks  In = 444      Paks  Out = 447
  StartTime = 19:56:01 PST Dec 17 2003
  AuthenTime = 19:56:04 PST Dec 17 2003
  Component = PPoE
Authen: service=PPP type=CHAP method=RADIUS
Kerb: No data available
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000003
  Session Id = 00000003
  Attribute List:
    63CCF180 0 00000001 port-type(156) 4 PPP over Ethernet
    63CCF194 0 00000009 interface(152) 7 0/0/0/0
PerU: No data available
```

Table 32 lists the significant fields shown in the display.

Table 32 show aaa user Field Descriptions

Field	Description
EXEC	Exec-Accounting database
NET	Network Accounting database
CMD	Command Accounting database
Pre Bytes In	Bytes that were received before the call was authenticated
Pre Bytes Out	Bytes that were transmitted before the call was authenticated
Pre Paks In	Packets that were received before the call was authenticated
Pre Paks Out	Packets that were transmitted before the call was authenticated
Bytes In	Bytes that were received after the call was authenticated
Bytes Out	Bytes that were transmitted after the call was authenticated
Paks In	Packets that were received after the call was authenticated
Paks Out	Packets that were transmitted after the call was authenticated
Authen	Authentication database

Field	Description
General	General database
PerU	Per-User database

Related Commands

Command	Description
show aaa sessions	Displays information about AAA sessions as seen in the AAA Session MIB.

show accounting

The **show accounting** command is replaced by the **show aaa user** command. See the **show aaa user** command for more information.

show auto secure config

To display AutoSecure configurations, use the **show auto secure config** command in privileged EXEC mode.

show suto secure config

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following sample output from the **show auto secure config** command shows what has been enabled and disabled via the **auto secure** command:

```
Router# show auto secure config

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$CZ6G$GkGOnHdNJCO3CjNHHyTUA.
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
ip domain-name cisco.com

crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
```

```
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
interface FastEthernet1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
interface FastEthernet1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
interface FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
ip cef
access-list compiled
ip access-list extended autosec_iana_reserved_block
 deny ip 1.0.0.0 0.255.255.255 any
 deny ip 2.0.0.0 0.255.255.255 any
 deny ip 5.0.0.0 0.255.255.255 any
 deny ip 7.0.0.0 0.255.255.255 any
 deny ip 23.0.0.0 0.255.255.255 any
 deny ip 27.0.0.0 0.255.255.255 any
 deny ip 31.0.0.0 0.255.255.255 any
 deny ip 36.0.0.0 0.255.255.255 any
 deny ip 37.0.0.0 0.255.255.255 any
 deny ip 39.0.0.0 0.255.255.255 any
 deny ip 41.0.0.0 0.255.255.255 any
 deny ip 42.0.0.0 0.255.255.255 any
 deny ip 49.0.0.0 0.255.255.255 any
 deny ip 50.0.0.0 0.255.255.255 any
 deny ip 58.0.0.0 0.255.255.255 any
 deny ip 59.0.0.0 0.255.255.255 any
 deny ip 60.0.0.0 0.255.255.255 any
 deny ip 70.0.0.0 0.255.255.255 any
 deny ip 71.0.0.0 0.255.255.255 any
```

```
 deny ip 72.0.0.0 0.255.255.255 any
 deny ip 73.0.0.0 0.255.255.255 any
 deny ip 74.0.0.0 0.255.255.255 any
 deny ip 75.0.0.0 0.255.255.255 any
 deny ip 76.0.0.0 0.255.255.255 any
 deny ip 77.0.0.0 0.255.255.255 any
 deny ip 78.0.0.0 0.255.255.255 any
 deny ip 79.0.0.0 0.255.255.255 any
 deny ip 83.0.0.0 0.255.255.255 any
 deny ip 84.0.0.0 0.255.255.255 any
 deny ip 85.0.0.0 0.255.255.255 any
 deny ip 86.0.0.0 0.255.255.255 any
 deny ip 87.0.0.0 0.255.255.255 any
 deny ip 88.0.0.0 0.255.255.255 any
 deny ip 89.0.0.0 0.255.255.255 any
 deny ip 90.0.0.0 0.255.255.255 any
 deny ip 91.0.0.0 0.255.255.255 any
 deny ip 92.0.0.0 0.255.255.255 any
 deny ip 93.0.0.0 0.255.255.255 any
 deny ip 94.0.0.0 0.255.255.255 any
 deny ip 95.0.0.0 0.255.255.255 any
 deny ip 96.0.0.0 0.255.255.255 any
 deny ip 97.0.0.0 0.255.255.255 any
 deny ip 98.0.0.0 0.255.255.255 any
 deny ip 99.0.0.0 0.255.255.255 any
 deny ip 100.0.0.0 0.255.255.255 any
 deny ip 101.0.0.0 0.255.255.255 any
 deny ip 102.0.0.0 0.255.255.255 any
 deny ip 103.0.0.0 0.255.255.255 any
 deny ip 104.0.0.0 0.255.255.255 any
 deny ip 105.0.0.0 0.255.255.255 any
 deny ip 106.0.0.0 0.255.255.255 any
 deny ip 107.0.0.0 0.255.255.255 any
 deny ip 108.0.0.0 0.255.255.255 any
 deny ip 109.0.0.0 0.255.255.255 any
 deny ip 110.0.0.0 0.255.255.255 any
 deny ip 111.0.0.0 0.255.255.255 any
 deny ip 112.0.0.0 0.255.255.255 any
 deny ip 113.0.0.0 0.255.255.255 any
 deny ip 114.0.0.0 0.255.255.255 any
 deny ip 115.0.0.0 0.255.255.255 any
 deny ip 116.0.0.0 0.255.255.255 any
 deny ip 117.0.0.0 0.255.255.255 any
 deny ip 118.0.0.0 0.255.255.255 any
 deny ip 119.0.0.0 0.255.255.255 any
 deny ip 120.0.0.0 0.255.255.255 any
 deny ip 121.0.0.0 0.255.255.255 any
 deny ip 122.0.0.0 0.255.255.255 any
 deny ip 123.0.0.0 0.255.255.255 any
 deny ip 124.0.0.0 0.255.255.255 any
 deny ip 125.0.0.0 0.255.255.255 any
 deny ip 126.0.0.0 0.255.255.255 any
 deny ip 197.0.0.0 0.255.255.255 any
 deny ip 201.0.0.0 0.255.255.255 any
 permit ip any any
remark This acl might not be up to date.
Visit www.iana.org/assignments/ipv4-add ress-space for update list
ip access-list extended autosec_private_block

 deny ip 10.0.0.0 0.255.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 192.168.0.0 0.0.255.255 any
 permit ip any any
ip access-list extended autosec_complete_bogon
```

```
deny ip 1.0.0.0 0.255.255.255 any
deny ip 2.0.0.0 0.255.255.255 any
deny ip 5.0.0.0 0.255.255.255 any
deny ip 7.0.0.0 0.255.255.255 any
deny ip 23.0.0.0 0.255.255.255 any
deny ip 27.0.0.0 0.255.255.255 any
deny ip 31.0.0.0 0.255.255.255 any
deny ip 36.0.0.0 0.255.255.255 any
deny ip 37.0.0.0 0.255.255.255 any
deny ip 39.0.0.0 0.255.255.255 any
deny ip 41.0.0.0 0.255.255.255 any
deny ip 42.0.0.0 0.255.255.255 any
deny ip 49.0.0.0 0.255.255.255 any
deny ip 50.0.0.0 0.255.255.255 any
deny ip 58.0.0.0 0.255.255.255 any
deny ip 59.0.0.0 0.255.255.255 any
deny ip 60.0.0.0 0.255.255.255 any
deny ip 70.0.0.0 0.255.255.255 any
deny ip 71.0.0.0 0.255.255.255 any
deny ip 72.0.0.0 0.255.255.255 any
deny ip 73.0.0.0 0.255.255.255 any
deny ip 74.0.0.0 0.255.255.255 any
deny ip 75.0.0.0 0.255.255.255 any
deny ip 76.0.0.0 0.255.255.255 any
deny ip 77.0.0.0 0.255.255.255 any
deny ip 78.0.0.0 0.255.255.255 any
deny ip 79.0.0.0 0.255.255.255 any
deny ip 83.0.0.0 0.255.255.255 any
deny ip 84.0.0.0 0.255.255.255 any
deny ip 85.0.0.0 0.255.255.255 any
deny ip 86.0.0.0 0.255.255.255 any
deny ip 87.0.0.0 0.255.255.255 any
deny ip 88.0.0.0 0.255.255.255 any
deny ip 89.0.0.0 0.255.255.255 any
deny ip 90.0.0.0 0.255.255.255 any
deny ip 91.0.0.0 0.255.255.255 any
deny ip 92.0.0.0 0.255.255.255 any
deny ip 93.0.0.0 0.255.255.255 any
deny ip 94.0.0.0 0.255.255.255 any
deny ip 95.0.0.0 0.255.255.255 any
deny ip 96.0.0.0 0.255.255.255 any
deny ip 97.0.0.0 0.255.255.255 any
deny ip 98.0.0.0 0.255.255.255 any
deny ip 99.0.0.0 0.255.255.255 any
deny ip 100.0.0.0 0.255.255.255 any
deny ip 101.0.0.0 0.255.255.255 any
deny ip 102.0.0.0 0.255.255.255 any
deny ip 103.0.0.0 0.255.255.255 any
deny ip 104.0.0.0 0.255.255.255 any
deny ip 105.0.0.0 0.255.255.255 any
deny ip 106.0.0.0 0.255.255.255 any
deny ip 107.0.0.0 0.255.255.255 any
deny ip 108.0.0.0 0.255.255.255 any
deny ip 109.0.0.0 0.255.255.255 any
deny ip 110.0.0.0 0.255.255.255 any
deny ip 111.0.0.0 0.255.255.255 any
deny ip 112.0.0.0 0.255.255.255 any
deny ip 113.0.0.0 0.255.255.255 any
deny ip 114.0.0.0 0.255.255.255 any
deny ip 115.0.0.0 0.255.255.255 any
deny ip 116.0.0.0 0.255.255.255 any
deny ip 117.0.0.0 0.255.255.255 any
deny ip 118.0.0.0 0.255.255.255 any
deny ip 119.0.0.0 0.255.255.255 any
```

```
 deny ip 120.0.0.0 0.255.255.255 any
 deny ip 121.0.0.0 0.255.255.255 any
 deny ip 122.0.0.0 0.255.255.255 any
 deny ip 123.0.0.0 0.255.255.255 any
 deny ip 124.0.0.0 0.255.255.255 any
 deny ip 125.0.0.0 0.255.255.255 any
 deny ip 126.0.0.0 0.255.255.255 any
 deny ip 197.0.0.0 0.255.255.255 any
 deny ip 201.0.0.0 0.255.255.255 any

 deny ip 10.0.0.0 0.255.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 192.168.0.0 0.0.255.255 any

 deny ip 224.0.0.0 15.255.255.255 any
 deny ip 240.0.0.0 15.255.255.255 any
 deny ip 0.0.0.0 0.255.255.255 any
 deny ip 169.254.0.0 0.0.255.255 any
 deny ip 192.0.2.0 0.0.0.255 any
 deny ip 127.0.0.0 0.255.255.255 any
 permit ip any any
remark This acl might not be up to date.
Visit www.iana.org/assignments/ipv4-address-space for update list
interface FastEthernet0/0
 ip verify unicast reverse-path
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
access-list 100 deny ip any any
interface FastEthernet0/0
 ip inspect autosec_inspect out
 ip access-group 100 in
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.

show call admission statistics

To monitor the global Call Admission Control (CAC) configuration parameters and the behavior of CAC, use the **show call admission statistics** command in user EXEC or privileged EXEC mode.

show call admission statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from the **show call admission statistics** command:

```
Router# show call admission statistics

Total Call admission charges: 0, limit 25
Total calls rejected 12, accepted 51
Load metric: charge 0, unscaled 0
```

Table 33 describes the significant fields shown in the display.

Table 33 show call admission statistics Field Descriptions

Field	Description
Total call admission charges	Percentage of system resources being charged to the system. If you configured a resource limit, SA requests are dropped when this field is equal to that limit.
limit	Maximum allowed number of total call admission charges. Valid values are 0 to 100000.
Total calls rejected	Number of SA requests that were not accepted.
accepted	Number of SA requests that were accepted.
unscaled	Not related to IKE. This value always is 0.

Related Commands

Command	Description
call admission limit	Instructs IKE to drop calls when a specified percentage of system resources are being consumed.
crypto call admission limit	Specifies the maximum number of IKE SA requests allowed before IKE begins rejecting new IKE SA requests.

show crypto ca certificates

Note This command was replaced by the **show crypto pki certificates** command effective with Cisco IOS Release 12.3(7)T.

To display information about your certificate, the certification authority certificate, and any registration authority certificates, use the **show crypto ca certificates** command in EXEC mode.

show crypto ca certificates

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command shows information about the following certificates:

- Your certificate, if you have requested one from the CA (see the **crypto pki enroll** command)
- The certificate of the CA, if you have received the CA's certificate (see the **crypto pki authenticate** command)
- RA certificates, if you have received RA certificates (see the **crypto pki authenticate** command)

Examples

The following is sample output from the **show crypto ca certificates** command after you authenticated the CA by requesting the CA's certificate and public key with the **crypto pki authenticate** command:

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The CA certificate might show Key Usage as "Not Set."

The following is sample output from the **show crypto ca certificates** command, and shows the router's certificate and the CA's certificate. In this example, a single, general purpose RSA key pair was previously generated, and a certificate was requested but not received for that key pair.

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
    Serial Number: 04806682
  Status: Pending
  Key Usage: General Purpose
    Fingerprint: 428125BD A3419600 3F6C7831 6CD8FA95 00000000
```

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

Note that in the previous sample, the router's certificate Status shows "Pending." After the router receives its certificate from the CA, the Status field changes to "Available" in the **show** output.

The following is sample output from the **show crypto ca certificates** command, and shows two router's certificates and the CA's certificate. In this example, special usage RSA key pairs were previously generated, and a certificate was requested and received for each key pair.

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 428125BDA34196003F6C78316CD8FA95
  Key Usage: Signature

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: AB352356AFCD0395E333CCFD7CD33897
  Key Usage: Encryption

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The following is sample output from the **show crypto ca certificates** command when the CA supports an RA. In this example, the CA and RA certificates were previously requested with the **crypto ca authenticate** command.

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set

RA Signature Certificate
  Status: Available
  Certificate Serial Number: 34BCF8A0
  Key Usage: Signature

RA KeyEncipher Certificate
  Status: Available
  Certificate Serial Number: 34BCF89F
  Key Usage: Encryption
```

Related Commands

Command	Description
crypto pki authenticate	Authenticates the CA (by obtaining the certificate of the CA).
crypto pki enroll	Obtains the certificates of your router from the CA.
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the route.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.

show crypto ca crls

Note This command was replaced by the **show crypto pki crls** command effective with Cisco IOS Release 12.3(7)T.

To display the current certificate revocation list (CRL) on router, use the **show crypto ca crls** command in EXEC mode.

show crypto ca crls

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.1	This command was introduced.

Examples

The following is sample output of the **show crypto ca crls** command:

```
Router# show crypto ca crls

          CRL Issuer Name:
              OU = sjvpn, O = cisco, C = us
              LastUpdate: 16:17:34 PST Jan 10 2002
              NextUpdate: 17:17:34 PST Jan 11 2002
              Retrieved from CRL Distribution Point:
                LDAP: CN = CRL1, OU = sjvpn, O = cisco, C = us
```

Related Commands

Command	Description
crypto pki crl request	Requests that a new CRL be obtained immediately from the CA.

show crypto ca roots

The **show crypto ca roots** command is replaced by the **show crypto pki trustpoints** command. See the **show crypto pki trustpoints** command for more information.

show crypto ca timers

Note This command was replaced by the **show crypto pki timers** command effective with Cisco IOS Release 12.3(8)T.

To display the status of the managed timers that are maintained by Cisco IOS for public key infrastructure (PKI), use the **show crypto ca timers** command in EXEC mode.

show crypto ca timers

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

For each timer, this command displays the time remaining before the timer expires. It also associates trustpoint certification authorities (CAs), except for certificate revocation list (CRL) timers, by displaying the CRL distribution point.

Examples

The following example is sample output for the **show crypto ca timers** command:

```
Router# show crypto ca timers

PKI Timers
| 4d15:13:33.144
 | 4d15:13:33.144  CRL http://msca-root.cisco.com/CertEnroll/msca-root.crl
 |328d11:56:48.372  RENEW msroot
 | 6:43.201  POLL verisign
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crypto pki trustpoint	Declares the CA that your router should use.

show crypto ca trustpoints

Note This command was replaced by the **show crypto pki trustpoints** command effective with Cisco IOS Release 12.3(7)T.

To display the trustpoints that are configured in the router, use the **show crypto pki trustpoints** command in privileged EXEC or user EXEC mode.

show crypto ca trustpoints

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC mode
User EXEC mode

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

This command replaces the **show crypto ca roots** command. If you enter the **show crypto ca roots** command, the output will be written back as the **show crypto pki trustpoints** command.

Examples

The following is sample output from the **show crypto ca trustpoints** command:

```
Router# show crypto ca trustpoints

Trustpoint bo:
    Subject Name:
    CN = bomborra Certificate Manager
     O = cisco.com
     C = US
          Serial Number:01
    Certificate configured.
    CEP URL:http://bomborra
    CRL query url:ldap://bomborra
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

show crypto call admission statistics

To monitor Crypto Call Admission Control (CAC) statistics, use the **show crypto call admission statistics** command in user EXEC or privileged EXEC mode.

show crypto call admission statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Enter this command to display information about the Crypto CAC configuration parameters and their history, including statistics regarding the current security association (SA) count, SAs being negotiated, total new SA requests, the number of Internet Key Exchange (IKE) SA requests accepted and rejected, and details regarding why requests were rejected.

Examples

The following example shows sample output from the **show crypto call admission statistics** command:

```
Router# show crypto call admission statistics

Crypto Call Admission Control Statistics
------------------------------------------------------------
System Resource Limit: 0    Max IKE SAs 0
Total IKE SA Count:    0    active:     0   negotiating: 0
Incoming IKE Requests: 0    accepted:   0   rejected:    0
Outgoing IKE Requests: 0    accepted:   0   rejected:    0
Rejected IKE Requests: 0    rsrc low:   0   SA limit:    0
```

Table 34 describes the significant fields shown in the display.

Table 34 show crypto call admission statistics Field Descriptions

Field	Description
System resource limit	Percentage of system resources that the router can be using before IKE starts dropping all SA requests.
Max IKE SAs	Number of active IKE SA requests allowed on the router.
Total IKE SA Count	Number of IKE SAs.
active	Number of active SAs.
negotiating	Number of SA requests being negotiated.
Incoming IKE Requests	Number of incoming IKE SA requests.

Table 34 show crypto call admission statistics Field Descriptions (continued)

Field	Description
Incoming IKE Requests accepted	Number of accepted IKE SA requests.
Incoming IKE Requests rejected	Number of rejected incoming IKE SA requests.
Outgoing IKE Requests	Number of outgoing IKE SA requests.
Outgoing IKE requests accepted	Number of accepted outgoing IKE SA requests.
Outgoing IKE requests rejected	Number of rejected outgoing IKE SA requests.
Rejected IKE Requests	Number of IKE requests that were rejected.
rsrc low	Number of IKE requests that were rejected because system resources were low or the preconfigured system resource limit was exceeded.
SA limit	Number of IKE SA requests that were rejected because the SA limit has been reached.

Related Commands

Command	Description
clear crypto call admission statistics	Clears the counters that track the number of accepted and rejected IKE SA requests.

show crypto debug-condition

To display crypto debug conditions that have already been enabled in the router, use the **show crypto debug-condition** command in privileged EXEC mode.

show crypto debug-condition {[**peer**] [**connid**] [**spi**] [**fvrf**] [**ivrf**] [**unmatched**]}

Syntax Description

peer	(Optional) Displays debug conditions related to the peer. Possible conditions can include peer IP address, subnet mask, host name, username, and group key.
connid	(Optional) Displays debug conditions related to the connection ID.
spi	(Optional) Displays debug conditions related to the security parameter index (SPI).
fvrf	(Optional) Displays debug conditions related to the front-door virtual private network (VPN) routing and forwarding (FVRF) instance.
ivrf	(Optional) Displays debug conditions related to the inside VRF (IVRF) instance.
unmatched	(Optional) Displays debug messages related Internet Key Exchange (IKE), IP Security (IPSec), or the crypto engine, depending on what was specified via the **debug crypto condition unmatched** [**isakmp** | **ipsec** | **engine**] command.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

You can specify as many filter values as specified via the **debug crypto condition** command. (You cannot specify a filter value that you did not use in the **debug crypto condition** command.) If no keywords are specified, all configured crypto conditions will be shown.

Examples

The following example shows how to display debug messages when the peer IP address is 10.1.1.1, 10.1.1.2, or 10.1.1.3 and when the connection ID 2000 of crypto engine 0 is used. This example also shows how to enable global debug crypto CLIs and enable the **show crypto debug-condition** command to verify conditional settings.

```
Router# debug crypto condition connid 2000 engine-id 1
Router# debug crypto condition peer ipv4 10.1.1.1
Router# debug crypto condition peer ipv4 10.1.1.2
Router# debug crypto condition peer ipv4 10.1.1.3
Router# debug crypto condition unmatched
! Verify crypto conditional settings.
Router# show crypto debug-condition

Crypto conditional debug currently is turned ON
```

```
IKE debug context unmatched flag:ON
IPsec debug context unmatched flag:ON
Crypto Engine debug context unmatched flag:ON

IKE peer IP address filters:
10.1.1.1  10.1.1.2   10.1.1.3

Connection-id filters:[connid:engine_id]2000:1,
! Enable global crypto CLIs to start conditional debugging.
Router# debug crypto isakmp
Router# debug crypto ipsec
Router# debug crypto engine
```

The following example shows how to disable all crypto conditional settings via the **reset** keyword:

```
Router# debug crypto condition reset
! Verify that all crypto conditional settings have been disabled.
Router# show crypto debug-condition

Crypto conditional debug currently is turned OFF
IKE debug context unmatched flag:OFF
IPsec debug context unmatched flag:OFF
Crypto Engine debug context unmatched flag:OFF
```

Related Commands

Command	Description
debug crypto condition	Defines conditional debug filters.
debug crypto condition unmatched	Displays crypto conditional debug messages when context information is unavailable to check against debug conditions.

show crypto dynamic-map

To display a dynamic crypto map set, use the **show crypto dynamic-map** command in EXEC mode.

show crypto dynamic-map [**tag** *map-name*]

Syntax Description

tag *map-name*	(Optional) Displays only the crypto dynamic map set with the specified *map-name*.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use the **show crypto dynamic-map** command to view a dynamic crypto map set.

Examples

The following is sample output for the **show crypto dynamic-map** command:

```
Router# show crypto dynamic-map

Crypto Map Template"vpn1" 1
        ISAKMP Profile: vpn1-ra
        No matching address list set.
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                vpn1,
```

The following partial configuration was in effect when the above **show crypto dynamic-map** command was issued:

```
crypto dynamic-map vpn1 1
 set transform-set vpn1
 set isakmp-profile vpn1-ra
 reverse-route
```

Related Commands

Command	Description
show crypto map	Views the crypto map configuration.

show crypto engine

To display a summary of the configuration information for the crypto engines, use the **show crypto engine** command in privileged EXEC mode.

show crypto engine [**accelerator** | **brief** | **configuration** | **connections** | **qos**]

Syntax Description

accelerator	(Optional) Displays crypto accelerator information.
brief	(Optional) Displays a summary of the configuration information for the crypto engine.
configuration	(Optional) Displays the version and configuration information for the crypto engine.
connections	(Optional) Displays information about the crypto engine connections.
qos	(Optional) Displays quality of service (QoS) information.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced on the Cisco 7200, RSP7000, and 7500 series routers.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

This command displays all crypto engines and displays the AIM-VPN product name.

Examples

The following example of **show crypto engine brief** shows typical crypto engine information:

```
Router# show crypto engine brief

crypto engine name: Virtual Private Network (VPN) Module
crypto engine type: hardware

VPN Module in slot: 1
Product Name: AIM-VPN/EPII
Software Serial #: 55AA
Device ID: 0014
Vendor ID: 13A3
VSK revision: 0
Boot version: 255
DPU version: 0
HSP version: 2.0(0x0) (PRODUCTION)

Time running: 0 Seconds
```

```
Compression: Yes
DES: Yes
3 DES: Yes
AES CBC: Yes (128,192,256)
AES CNTR: No
Maximum buffer length: 4096
Maximum DH index: 2000
Maximum SA index: 2000
Maximum Flow index: 4000
Maximum RSA key size: 2048
crypto engine in slot: 1

crypto engine name: unknown
crypto engine type: software
serial number: 0DDC7C0D
crypto engine state: installed
crypto engine in slot: N/A
```

Table 35 describes significant fields shown in the display.

Table 35 show crypto engine Command Field Descriptions

Field	Description
crypto engine name	Name of the crypto engine as assigned with the key-name argument in the crypto key generate dss command.
crypto engine type	If “software” is listed, the crypto engine resides in either the Route Switch Processor (RSP) (the Cisco IOS crypto engine) or in a second-generation Versatile Interface Processor (VIP2). If “crypto card” or “ESA” is listed, the crypto engine is associated with an Encryption Service Adapter (ESA).
crypto engine state	The state “installed” indicates that a crypto engine is located in the given slot, but it is not configured for encryption. The state “dss key generated” indicates the crypto engine found in that slot has DSS keys already generated.
crypto firmware version	Version number of the crypto firmware running on the ESA.
crypto lib version	Version number of the crypto library running on the router.
crypto engine in slot	Chassis slot number of the crypto engine. For the Cisco IOS crypto engine, this is the chassis slot number of the Route Switch Processor (RSP).

Related Commands

Command	Description
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.

show crypto engine accelerator logs

To display information about the last 32 CryptoGraphics eXtensions (CGX) Library packet processing commands and associated parameters sent from the VPN module driver to the VPN module hardware, use the **show crypto engine accelerator logs** command in privileged EXEC mode.

show crypto engine accelerator logs

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)XC	This command was introduced on the Cisco 1720 and Cisco 1750 platforms.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command when encrypted traffic is sent to the router and a problem with the encryption module is suspected. Use the **debug crypto engine accelerator logs** command to enable command logging *before* using this command.

Note The **show crypto engine accelerator logs** command is intended only for Cisco Systems TAC personnel to collect debugging information.

Examples

The following is sample output for the **show crypto engine accelerator logs** command:

```
Router# show crypto engine accelerator logs

Contents of packet log (current index = 20):

tag = 0x5B02, cmd = 0x5000
param[0] = 0x000E, param[1] = 0x57E8
param[2] = 0x0008, param[3] = 0x0000
param[4] = 0x0078, param[5] = 0x0004
param[6] = 0x142C, param[7] = 0x142C
param[8] = 0x0078, param[9] = 0x000C
tag = 0x5B03, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x583C
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C
tag = 0x5C00, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x57BC
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C
```

```
.
.
.
tag = 0x5A01, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x593C
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C

Contents of cgx log (current index = 12):

cmd = 0x0074 ret = 0x0000
param[0] = 0x0010, param[1] = 0x028E
param[2] = 0x0039, param[3] = 0x0D1E
param[4] = 0x0100, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
cmd = 0x0062 ret = 0x0000
param[0] = 0x0035, param[1] = 0x1BE0
param[2] = 0x0100, param[3] = 0x0222
param[4] = 0x0258, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
cmd = 0x0063 ret = 0x0000
param[0] = 0x0222, param[1] = 0x0258
param[2] = 0x0000, param[3] = 0x0000
param[4] = 0x0000, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x020A
param[8] = 0x002D, param[9] = 0x0000
.
.
.
cmd = 0x0065 ret = 0x0000
param[0] = 0x0222, param[1] = 0x0258
param[2] = 0x0010, param[3] = 0x028E
param[4] = 0x00A0, param[5] = 0x0008
param[6] = 0x0001, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
```

Related Commands

Command	Description
debug crypto engine acclerator logs	Enables logging of commands and associated parameters sent from the VPN module driver to the VPN module hardware using a debug flag.

show crypto engine accelerator ring

To display the contents and status of the control command, transmit packets, and receive packet rings used by the hardware accelerator crypto engine, use the **show crypto engine accelerator ring** command in privileged EXEC mode.

show crypto engine accelerator ring [**control** | **packet** | **pool**]

Syntax Description

control	(Optional) Number of control commands that are queued for execution by the hardware accelerator crypto engine are displayed.
packet	(Optional) Contents and status information for the transmit packet rings that are used by the hardware accelerator crypto engine are displayed.
pool	(Optional) Contents and status information for the receive packet rings that are used by the hardware accelerator crypto engine are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XL	This command was introduced for the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

Usage Guidelines

This command displays the command ring information.

If there were valid data in any of the rings, the ring entry would be printed.

Examples

The following example shows the command ring information:

```
Router# show crypto engine accelerator ring packet

PPQ RING:

cmd ring:head = 10 tail =10

result ring:head = 10 tail =10

destination ring:head = 10 tail =10
```

```
source ring:head = 10 tail =10

free ring:head = 0 tail =255
        00000000  071A96C5
        00000000  071A96C5
        00000001  071A9465
        00000001  071A9465
        00000002  071A9205
        00000002  071A9205
.
.
.
```

Related Commands

Command	Description
clear crypto engine accelerator counter	Resets the statistical and error counters for the hardware accelerator to zero.
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.
crypto ipsec	Defines the IPSec SAs and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine SA database.
show crypto engine accelerator statistic	Displays the current run-time statistics and error counters for the crypto engine.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

show crypto engine accelerator sa-database

To display active (in-use) entries in the platform-specific virtual private network (VPN) module database, use the **show crypto engine accelerator sa-database** command in privileged EXEC mode.

show crypto engine accelerator sa-database

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)XC	This command was introduced on the Cisco 1720 and Cisco 1750 platforms.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command when encrypted traffic is sent to the router and a problem with the encryption module is suspected.

Note The **show crypto engine accelerator sa-database** command is intended only for Cisco Systems TAC personnel to collect debugging information.

Examples

The following is sample output for the **show crypto engine accelerator sa-database** command:

```
Router# show crypto engine accelerator sa-database

Flow Summary
        Index   Algorithms
        005      tunnel inbound  esp-md5-hmac esp-des ah-sha-hmac
        006      tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
        007      tunnel inbound  esp-md5-hmac esp-des ah-sha-hmac
        008      tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
        009      tunnel inbound  esp-md5-hmac esp-des ah-sha-hmac
        010      tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
SA Summary:
        Index   DH-Index        Algorithms
        003     001(deleted)    DES SHA
        004     002(deleted)    DES SHA
DH Summary
        Index Group Config
```

Related Commands

Command	Description
debug crypto engine acclerator logs	Enables logging of commands and associated parameters sent from the VPN module driver to the VPN module hardware using a debug flag.

show crypto engine accelerator statistic

To display the statistics and error counters for the onboard hardware accelerator of the router for IP Security (IPSec) encryption, use the **show crypto engine accelerator statistic** command in privileged EXEC mode.

show crypto engine accelerator statistic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)XC	This command was introduced for the Cisco 1700 series router and other Cisco routers that support hardware accelerators for IPSec encryption.
12.1(3)XL	This command was implemented on the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745. In addition, the show output for this command was enhanced to display compression statistics.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

Examples

The following example displays compression statistics:

```
Router# show crypto engine accelerator statistic

     Statistics for Hardware VPN Module:
         ds: 8235C3D8        idb: 82359A64
     Statistics for Encryption Module:
                 0 packets in                          0 packets out
                 0 packet overruns                     0 output packets dropped
                 0 packets decompressed                0 packets compressed
                 0 compressed bytes in                 0 encompassed bytes in
                 0 packets bypass compression          0 packet abort compression
                 0 packets fail compression
                4:1 compression ratio                  2:1 overall compression ratio
                 0 decompressed bytes out              0 compressed bytes out
                 0 packets decrypted                   0 packets encrypted
                 0 bytes decrypted                     0 bytes encrypted
                 0 bytes before decrypt                0 bytes after encrypt
```

```
   0 paks/sec in                                0 paks/sec out
   0 Kbits/sec decrypted                        0 Kbits/sec encrypted
   0 packet overruns
rx_no_endp:      0   rx_hi_discards:  0     fw_failure:         0
invalid_sa:      0   invalid_flow:    0     cgx_errors          0
fw_qs_filled:    0   fw_resource_lock:0     lotx_full_err:      0
null_ip_error:   0   pad_size_error:  0     out_bound_dh_acc:   0
esp_auth_fail:   0   ah_auth_failure: 0     crypto_pad_error:   0
ah_prot_absent:  0   ah_seq_failure:  0     ah_spi_failure:     0
esp_prot_absent:0    esp_seq_fail:    0     esp_spi_failure:    0
obound_sa_acc:   0   invalid_sa:      0     out_bound_sa_flow:  0
invalid_dh:      0   bad_keygroup:    0     out_of_memory:      0
no_sh_secret:    0   no_skeys:        0     invalid_cmd:        0
dsp_coproc_err:  0   comp_unsupported:0     pak_too_big:        0
null packets: 0
pak_mp_length_spec_fault: 0
tx_lo_queue_size_max 0  cmd_unimplemented: 0
219 seconds since last clear of counters
Interrupts: 4          Immed: 3          HiPri ints:  0
LoPri ints: 0          POST Errs: 0         Alerts: 1
Unk Cmds: 0          UnexpCmds: 0
cgx_cmd_pending:0    packet_loop_max: 0  packet_loop_limit: 0
```

Table 36 describes significant fields shown in the display.

Table 36 show crypto engine accelerator statistic Command Field Descriptions

Counter	Description
packets decompressed	Number of packets that were decompressed by the interface.
packets compressed	Number of packets that were compressed by the interface.
compressed bytes in	Number of compressed bytes that were presented to the compression algorithm from the input interface on decrypt.
encompassed bytes in	Number of uncompressed bytes (payload) that were presented to the compression algorithm from Cisco IOS on encrypt.
packets bypass compression	Number of packets that were not compressed because they were too small (<128 bytes).
packet abort compression	Number of packets that were not compressed because the packets are expanded rather than compressed.
packets fail compression	Number of packets that were not compressed because of problems in the compression algorithm.
compression ratio	Ratio of compression and decompression of packets presented to the compression algorithm that were successfully compressed or decompressed. This statistic measures the efficiency of the algorithm for all packets that were compressed or decompressed.
overall compression ratio	Ratio of compression and decompression of packets presented to the compression algorithm, including those that were not compressed due to expansion, too small. This ratio indicates whether the data traffic on this interface is suitable for compression. A ratio of 1:1 would imply that no successful compression is being performed on this data traffic.

Table 36 show crypto engine accelerator statistic Command Field Descriptions

Counter	Description
decompressed bytes out	Number of decompressed bytes that were sent to Cisco IOS by the compression algorithm on decrypt.
compressed bytes out	Number of compressed bytes that were forwarded to Cisco IOS by the algorithm on encrypt.

The following sample output displays a typical output of the current statistics and error counters for the hardware accelerator of the router:

```
Router# show crypto engine accelerator statistic

Virtual Private Network (VPN) Module in slot :0
        Statistics for Hardware VPN Module since the last clear
         of counters 1379 seconds ago
            167874 packets in                167874 packets out
         201596210 bytes in                201596059 bytes out
               121 paks/sec in                   121 paks/sec out
              1169 Kbits/sec in                 1169 Kbits/sec out
                 0 packets decrypted               0 packets encrypted
                 0 bytes before decrypt            0 bytes encrypted
                 0 bytes decrypted                 0 bytes after encrypt
                 0 packets decompressed            0 packets compressed
                 0 bytes before decomp             0 bytes before comp
                 0 bytes after decomp              0 bytes after comp
                 0 packets bypass decompr          0 packets bypass compres
                 0 bytes bypass decompres          0 bytes bypass compressi
                 0 packets not decompress          0 packets not compressed
                 0 bytes not decompressed          0 bytes not compressed
             1.0:1 compression ratio           1.0:1 overall
                20 commands out                   20 commands acknowledged
        Last 5 minutes:
             46121 packets in                  46121 packets out
               153 paks/sec in                   153 paks/sec out
           1667834 Kbits/sec in              1667836 Kbits/sec out
                 0 bytes decrypted                 0 bytes encrypted
                 0 Kbits/sec decrypted             0 Kbits/sec encrypted
             1.0:1 compression ratio           1.0:1 overall

        Errors:
        ppq full errors       :       0 ppq rx errors         :       0
        cmdq full errors      :       0 cmdq rx errors        :       0
        no buffer             :       0 replay errors         :       0
        dest overflow         :       0 authentication errors :       0
        Out of memory         :       0 Access denied         :       0
        Out of handles        :       0 Bad function code     :       0
        Invalid parameter     :       0 Bad handle value      :       0
        Output buffer overrun :       0 Input Underrun        :       0
        Input Overrun         :       0 Invalid Key           :       0
        Invalid Packet        :       0 Decrypt Failure       :       0
        Verification Fail     :       0 Bad Attribute         :       0
        Invalid attrribute val:       0 Missing attribute     :       0
        Unwrappable object    :       0 Hash Miscompare       :       0
        DF Bit set            :       0 RNG self test fail    :       0
        Other error           :       0
        sessions              :       0

        Warnings:
        sessions_expired:0        packets_fragmented:0
        general:         0
```

Tip In Cisco IOS Release 12.2(8)T and later releases, you can add a time stamp to show commands using the **exec prompt timestamp** command in line configuration mode.

Related Commands

Command	Description
clear crypto engine accelerator counter	Resets the statistical and error counters for the hardware accelerator to zero.
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
crypto engine accelerator	Enables the use of the onboard hardware accelerator of the Cisco uBR905 and Cisco uBR925 routers for IPSec encryption.
crypto ipsec	Defines the IPSec SAs and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator ring	Displays the contents of command and transmit rings for the crypto engine.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine security association (SA) database.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

show crypto ha

To display all virtual IP (VIP) addresses that are currently in use by IP Security (IPSec) and Internet Key Exchange (IKE), use the **show crypto ha** command in privileged EXEC mode.

show crypto ha

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced.

Examples

The following output from the **show crypto ha** command shows all VIP addresses that are being used by IPSec and IKE:

```
Router# show crypto ha

IKE VIP: 209.165.201.3
  stamp: 74 BA 70 27 9C 4F 7F 81 3A 70 13 C9 65 22 E7 76
IKE VIP: 255.255.255.253
  stamp: Not set
IKE VIP: 255.255.255.254
  stamp: Not set
IPSec VIP: 209.165.201.3
IPSec VIP: 255.255.255.253
IPSec VIP: 255.255.255.254
```

show crypto ipsec client ezvpn

To display the Cisco Easy VPN Remote configuration, use the **show crypto ipsec client ezvpn** command in privileged EXEC mode.

show crypto ipsec client ezvpn

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)YA	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Examples

The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an active Virtual Private Network (VPN) connection when the router is in client mode:

```
Router# show crypto ipsec client ezvpn

Tunnel name: hw1
Inside interface list: FastEthernet0/0, Serial1/0,
Outside interface: Serial0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 209.165.201.0
Mask: 255.255.255.224
DNS Primary: 209.165.201.1
DNS Secondary: 209.165.201.2
NBMS/WINS Primary: 209.165.201.3
NBMS/WINS Secondary: 209.165.201.4
Default Domain: cisco.com
```

The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an active VPN connection when the router is in network-extension mode:

```
Router# show crypto ipsec client ezvpn

Tunnel name: hw1
Inside interface list: FastEthernet0/0, Serial1/0,
Outside interface: Serial0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 209.165.202.128
Mask: 255.255.255.224
Default Domain: cisco.com

Split Tunnel List: 1
       Address    : 209.165.200.225
       Mask       : 255.255.255.224
```

```
        Protocol   : 0x0
        Source Port: 0
        Dest Port  : 0
```

The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an inactive VPN connection:

```
Router# show crypto ipsec client ezvpn

Current State: IDLE
Last Event: REMOVE INTERFACE CFG
Router#
```

Table 37 describes significant fields shown by the **show crypto ipsec client ezvpn** command:

Table 37 show crypto ipsec client ezvpn Field Descriptions

Field	Description
Current State	Displays whether the VPN tunnel connection is active or idle. Typically, when the tunnel is up, the current state is IPSEC ACTIVE.
Last Event	Displays the last event performed on the VPN tunnel. Typically, the last event before a tunnel is created is SOCKET UP.
Address	Displays the IP address used on the outside interface.
Mask	Displays the subnet mask used for the outside interface.
DNS Primary	Displays the primary domain name system (DNS) server provided by the Dynamic Host Configuration Protocol (DHCP) server.
DNS Secondary	Displays the secondary DNS server provided by the DHCP server.
Domain Name	Displays the domain name provided by the DHCP server.
NBMS/WINS Primary	Displays the primary NetBIOS Microsoft Windows Name Server provided by the DHCP server.
NBMS/WINS Secondary	Displays the secondary NetBIOS Microsoft Windows Name Server provided by the DHCP server.

Related Commands

Command	Description
show crypto ipsec transform	Displays the specific configuration for one or all transformation sets.

show crypto ipsec sa

To display the settings used by current security associations (SAs), use the **show crypto ipsec sa** command in privileged EXEC mode.

show crypto ipsec sa [**map** *map-name* | **address** | **identity** | **interface** *interface* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name*] [**detail**]

IPSec and IKE Stateful Failover Syntax

show crypto ipsec sa [**active** | **standby**]

Syntax Description

map *map-name*	(Optional) Any existing SAs that were created for the crypto map set named *map-name* are displayed.
address	(Optional) All existing SAs are displayed, sorted by the destination address (either the local address or the address of the IP Security (IPSec) remote peer) and then by protocol (Authentication Header [AH] or Encapsulation Security Protocol [ESP]).
identity	(Optional) Only the flow information is displayed. It does not show the SA information.
interface *interface*	(Optional) All existing SAs created for an interface that is named *interface* are displayed.
peer [**vrf** *fvrf-name*] **address**	(Optional) All existing SAs with the peer address. If the peer address is in the Virtual Routing and Forwarding (VRF), specify **vrf** and the *fvrf-name*.
vrf *ivrf-name*	(Optional) All existing SAs whose inside virtual routing and forwarding (IVRF) is the same as the *ivrf-name*.
detail	(Optional) Detailed error counters are displayed. (The default is the high-level send or receive error counters.)
active	(Optional) All existing SAs that are in an active state are displayed.
standby	(Optional) All existing SAs that are in standby state are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(13)T	The “remote crypto endpt” and “in use settings” fields were modified to support Network Address Translation (NAT) traversal.
12.2(15)T	The **interface** keyword and *interface* argument were added. The **peer** keyword, the **vrf** keyword, and the *fvrf-name* argument were added. In addition, the **address** keyword was added to the **peer** keyword string. The **vrf** keyword and *ivrf-name* argument were added.
12.3(11)T	The **active** and **standby** keywords were added.

Usage Guidelines

If no keyword is used, all SAs are displayed. They are sorted first by interface, and then by traffic flow (for example, source or destination address, mask, protocol, or port). Within a flow, the SAs are listed by protocol (ESP or AH) and direction (inbound or outbound).

Examples

The following is sample output for the **show crypto ipsec sa** command:

```
Router# show crypto ipsec sa vrf vpn2

interface: Ethernet1/2
    Crypto map tag: ra, local addr. 172.16.1.1

   protected vrf: vpn2
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.4.1.4/255.255.255.255/0/0)
   current_peer: 10.1.1.1:500
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.1.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: 50110CF8

     inbound esp sas:
      spi: 0xA3E24AFD(2749516541)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5127, flow_id: 7, crypto map: ra
        sa timing: remaining key lifetime (k/sec): (4603517/3503)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x50110CF8(1343294712)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5128, flow_id: 8, crypto map: ra
        sa timing: remaining key lifetime (k/sec): (4603517/3502)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

The following configuration was in effect when the above **show crypto ipsec sa vrf** command was issued. The IPSec remote access tunnel was “UP” when this command was issued.

```
crypto dynamic-map vpn1 1
 set transform-set vpn1
 set isakmp-profile vpn1-ra
 reverse-route
!
```

```
crypto dynamic-map vpn2 1
 set transform-set vpn2
 set isakmp-profile vpn2-ra
 reverse-route
!
!
crypto map ra 1 ipsec-isakmp dynamic vpn1
crypto map ra 2 ipsec-isakmp dynamic vpn2
```

IPSec and IKE Stateful Failover Examples

The following sample output shows the IPSec SA status of only the active device:

```
Router# show crypto ipsec sa active

interface: Ethernet0/0
    Crypto map tag: to-peer-outside, local addr 209.165.201.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.16.0.1/255.255.255.255/0/0)
   current_peer 209.165.200.225 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 209.165.201.3, remote crypto endpt.: 209.165.200.225
     path mtu 1500, media mtu 1500
     current outbound spi: 0xD42904F0(3559458032)

     inbound esp sas:
      spi: 0xD3E9ABD0(3555306448)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: 6, crypto map: to-peer-outside
        sa timing: remaining key lifetime (k/sec): (4586265/3542)
             HA last key lifetime sent(k): (4586267)
        ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
```

The following sample output shows the IPSec SA status of only the standby device:

```
Router# show crypto ipsec sa standby

interface: Ethernet0/0
    Crypto map tag: to-peer-outside, local addr 209.165.201.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.16.0.1/255.255.255.255/0/0)
   current_peer 209.165.200.225 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0

 local crypto endpt.: 209.165.201.3, remote crypto endpt.: 209.165.200.225
 path mtu 1500, media mtu 1500
 current outbound spi: 0xD42904F0(3559458032)

 inbound esp sas:
  spi: 0xD3E9ABD0(3555306448)
    transform: esp-3des ,
    in use settings ={Tunnel, }
    conn id: 2012, flow_id: 12, crypto map: to-peer-outside
    sa timing: remaining key lifetime (k/sec): (4441561/3486)
         HA last key lifetime sent(k): (4441561)
    ike_cookies: 00000000 00000000 00000000 00000000
    IV size: 8 bytes
    replay detection support: Y
    Status: STANDBY

 inbound ah sas:
  spi: 0xF3EE3620(4092474912)
    transform: ah-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2012, flow_id: 12, crypto map: to-peer-outside
    sa timing: remaining key lifetime (k/sec): (4441561/3486)
         HA last key lifetime sent(k): (4441561)
    ike_cookies: 00000000 00000000 00000000 00000000
    replay detection support: Y
    Status: STANDBY

 inbound pcp sas:

 outbound esp sas:
  spi: 0xD42904F0(3559458032)
    transform: esp-3des ,
    in use settings ={Tunnel, }
    conn id: 2011, flow_id: 11, crypto map: to-peer-outside
    sa timing: remaining key lifetime (k/sec): (4441561/3485)
         HA last key lifetime sent(k): (4441561)
    ike_cookies: 00000000 00000000 00000000 00000000
    IV size: 8 bytes
    replay detection support: Y
    Status: STANDBY

 outbound ah sas:
  spi: 0x75251086(1965363334)
    transform: ah-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2011, flow_id: 11, crypto map: to-peer-outside
    sa timing: remaining key lifetime (k/sec): (4441561/3485)
         HA last key lifetime sent(k): (4441561)
    ike_cookies: 00000000 00000000 00000000 00000000
    replay detection support: Y
    Status: STANDBY

 outbound pcp sas:
```

show crypto ipsec security-association lifetime

To display the security association (SA) lifetime value configured for a particular crypto map entry, use the **show crypto ipsec security-association lifetime** command in EXEC mode.

show crypto ipsec security-association lifetime

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.

Examples

The following is sample output for the **show crypto ipsec security-association lifetime** command:

```
Router# show crypto ipsec security-association lifetime

Security-association lifetime: 4608000 kilobytes/120 seconds
```

The following configuration was in effect when the previous **show crypto ipsec security-association lifetime** command was issued:

```
crypto ipsec security-association lifetime seconds 120
```

show crypto ipsec transform-set

To display the configured transform sets, use the **show crypto ipsec transform-set** command in EXEC mode.

show crypto ipsec transform-set [**tag** *transform-set-name*]

Syntax Description

tag *transform-set-name*	(Optional) Only the transform sets with the specified *transform-set-name* are displayed.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(13)T	The command output was expanded to include a warning message for users who try to configure an IP Security (IPSec) transform that the hardware does not support.

Examples

The following is sample output for the **show crypto ipsec transform-set** command:

```
Router# show crypto ipsec transform-set

Transform set combined-des-sha: {esp-des esp-sha-hmac}
   will negotiate = { Tunnel,  },

Transform set combined-des-md5: {esp-des esp-md5-hmac}
   will negotiate = { Tunnel,  },

Transform set t1: {esp-des esp-md5-hmac}
   will negotiate = {Tunnel,},

Transform set t100: {ah-sha-hmac}
   will negotiate = {Transport,},

Transform set t2: {ah-sha-hmac}
   will negotiate = {Tunnel,},
   { esp-des  }
   will negotiate = {Tunnel,},
```

The following configuration was in effect when the previous **show crypto ipsec transform-set** command was issued:

```
crypto ipsec transform-set combined-des-sha esp-des esp-sha-hmac
crypto ipsec transform-set combined-des-md5 esp-des esp-md5-hmac
crypto ipsec transform-set t1 esp-des esp-md5-hmac
crypto ipsec transform-set t100 ah-sha-hmac
 mode transport
crypto ipsec transform-set t2 ah-sha-hmac esp-des
```

The following sample output from the s**how crypto ipsec transform-set** command displays a warning message after a user tries to configure an IPSec transform that the hardware does not support:

```
Router# show crypto ipsec transform-set

Transform set transform-1:{ esp-256-aes esp-md5-hmac  }
   will negotiate = { Tunnel,  },

WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

show crypto isakmp key

To list the keyrings and their preshared keys, use the **show crypto isakmp key** command in EXEC mode.

show crypto isakmp key

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.

Examples

The following is sample output for the **show crypto isakmp key** command:

```
Router# show crypto isakmp key

Hostname/Address       Preshared Key
vpn1                   : 172.61.1.1          vpn1
vpn2                   : 10.1.1.1            vpn2
```

The following configuration was in effect when the above **show crypto isakmp key** command was issued:

```
crypto keyring vpn1
  pre-shared-key address 172.16.1.1 key vpn1
crypto keyring vpn2
  pre-shared-key address 10.1.1.1 key vpn2
```

Table 38 describes significant fields in the **show crypto isakmp key** profile.

Table 38 show crypto isakmp key Field Descriptions

Field	Description
Hostname/Address	The preshared key host name or address.
Preshared Key	The preshared key.
keyring	Name of the crypto keyring. The global keys are listed in the default keyring.
VRF string	The virtual route forwarding (VRF) of the keyring. If the keyring does not have a VRF, an empty string is printed.

show crypto isakmp peer

To display peer descriptions, use the **show crypto isakmp peer** command in privileged EXEC mode.

show crypto isakmp peer

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following output example shows information about the peer named "This-is-another-peer-at-10-1-1-3":

```
Router# show crypto isakmp peer

Peer: 10.1.1.3 Port: 500
 Description: This-is-another-peer-at-10-1-1-3
 Phase1 id: 10.1.1.3
```

Table 39 describes the significant fields shown in the display.

Table 39 show crypto isakmp peer Field Descriptions

Field	Description
Phase1 id	Internet Key Exchange (IKE) ID

Related Commands

Command	Description
clear crypto session	Deletes crypto sessions (IPSec and IKE) SAs.
description	Adds a description for an IKE peer.
show crypto session	Displays status information for active crypto sessions in a router.

show crypto isakmp policy

To display the parameters for each Internet Key Exchange (IKE) policy, use the **show crypto isakmp policy** command in EXEC mode.

show crypto isakmp policy

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(13)T	The command output was expanded to include a warning message for users who try to configure an IKE encryption method that the hardware does not support.

Examples

The following is sample output from the **show crypto isakmp policy** command, after two IKE policies have been configured (with priorities 15 and 20, respectively):

```
Router# show crypto isakmp policy

Protection suite priority 15
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys)
        hash algorithm:  Message Digest 5
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman Group:    #2 (1024 bit)
        lifetime:      5000 seconds, no volume limit
Protection suite priority 20
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys)
        hash algorithm: Secure Hash Standard
        authentication method:   preshared Key
        Diffie-Hellman Group:    #1 (768 bit)
        lifetime:      10000 seconds, no volume limit
Default protection suite
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys)
        hash algorithm: Secure Hash Standard
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman Group:    #1 (768 bit)
        lifetime:      86400 seconds, no volume limit
```

Note Although the output shows "no volume limit" for the lifetimes, you can currently configure only a time lifetime (such as 86,400 seconds); volume limit lifetimes are not used.

The following sample output from the **show crypto isakmp policy** command displays a warning message after a user tries to configure an IKE encryption method that the hardware does not support:

```
Router# show crypto isakmp policy

Protection suite of priority 1
```

```
        encryption algorithm:  AES - Advanced Encryption Standard (256 bit keys).
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
        hash algorithm:        Secure Hash Standard
        authentication method: Pre-Shared Key
        Diffie-Hellman group:  #1 (768 bit)
        lifetime:              3600 seconds, no volume limit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the DH group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.

show crypto isakmp profile

To list all the Internet Security Association and Key Management Protocol (ISAKMP) profiles that are defined on a router, use the **show crypto isakmp profile** command in EXEC mode.

show crypto isakmp profile

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.

Examples

The following is sample output for the **show crypto isakmp profile** command:

```
Router# show crypto isakmp profile

ISAKMP PROFILE vpn1-ra
   Identities matched are:
group vpn1-ra
   Identity presented is: ip-address
```

Table 40 describes significant fields in the display.

Table 40 show crypto isakmp profile Command Field Descriptions

Field	Description
ISAKMP PROFILE	Name of the ISAKMP profile.
Identities matched are:	Lists all identities that the ISAKMP profile will match.
Identity presented is:	The identity that the ISAKMP profile will present to the remote endpoint.

The following configuration was in effect when the above **show crypto isakmp profile** command was issued:

```
crypto isakmp profile vpn1-ra
 vrf vpn1
 self-identity address
 match identity group vpn1-ra
 client authentication list aaa-list
 isakmp authorization list aaa
 client configuration address initiate
 client configuration address respond
```

Related Commands

Command	Description
show crypto isakmp key	Lists the keyrings and their preshared keys.

show crypto isakmp sa

To display current Internet Key Exchange (IKE) security associations (SAs), use the **show crypto isakmp sa** command in privileged EXEC mode.

show crypto isakmp sa [**active** | **standby**]

Syntax Description

active	(Optional) All existing IKE SAs that are in an active state are displayed.
standby	(Optional) All existing IKE SAs that are in standby state are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(11)T	The **active** and **standby** keywords were added.

Usage Guidelines

If neither the **active** keyword nor the **standby** keyword are specified, current SAs for all configured routers will be shown.

Examples

The following sample output shows the SAs of both the active and standby devices:

```
Router# show crypto isakmp sa

dst             src             state          conn-id slot status
209.165.201.3   209.165.200.225 QM_IDLE              2    0 STDBY
10.0.0.1        10.0.0.2        QM_IDLE              1    0 ACTIVE
```

The following sample output shows the SAs of only the active device:

```
Router# show crypto isakmp sa active

dst             src             state          conn-id slot status
209.165.201.3   209.165.200.225 QM_IDLE              5    0 ACTIVE
```

The following sample output shows the SAs of only the standby device:

```
Router# show crypto isakmp sa standby

dst             src             state          conn-id slot status
209.165.201.3   209.165.200.225 QM_IDLE              5    0 STDBY
209.165.201.3   209.165.200.225 QM_IDLE              1    0 STDBY
```

Table 41 through Table 44 show the various states that may be displayed in the output of the **show crypto isakmp sa** command. When an Internet Security Association and Key Management Protocol (ISAKMP) SA exists, it will most likely be in its quiescent state (QM_IDLE). For long exchanges, some of the MM_xxx states may be observed.

Table 41 States in Main Mode Exchange

State	Explanation
MM_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is “larval” at this stage—there is no state.
MM_SA_SETUP	The peers have agreed on parameters for the ISAKMP SA.
MM_KEY_EXCH	The peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated.
MM_KEY_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE, and a Quick Mode exchange begins.

Table 42 States in Aggressive Mode Exchange

State	Explanation
AG_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is “larval” at this stage—there is no state.
AG_INIT_EXCH	The peers have done the first exchange in aggressive mode, but the SA is not authenticated.
AG_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE, and a quick mode exchange begins.

Table 43 States in Quick Mode Exchange

State	Explanation
QM_IDLE	The ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent quick mode exchanges. It is in a quiescent state.

Table 44 show crypto isakmp sa Field Descriptions

Field	Description
f_vrf/i_vrf	The front door virtual routing and forwarding (FVRF) and the inside VRF (IVRF) of the IKE SA. If the FVRF is global, the output shows f_vrf as an empty field.

Related Commands

Command	Description
crypto isakmp policy	Defines an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.

show crypto key mypubkey rsa

To display the RSA public keys of your router, use the **show crypto key mypubkey rsa** command in privileged EXEC mode.

show crypto key mypubkey rsa

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(7)T	The show output was modified to display whether an RSA key is protected (encrypted) and locked or unlocked.

Usage Guidelines

This command displays your router's RSA public keys.

Examples

The following is sample output from the **show crypto key mypubkey rsa** command. Special usage RSA keys were previously generated for this router using the **crypto key generate rsa** command.

```
% Key pair was generated at: 06:07:49 UTC Jan 13 1996
Key name: myrouter.example.com
 Usage: Signature Key
 Key Data:
  005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
  04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
  BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001

% Key pair was generated at: 06:07:50 UTC Jan 13 1996
Key name: myrouter.example.com
 Usage: Encryption Key
 Key Data:
  00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5
  18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB
  07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

The following example shows how to encrypt the RSA key "pki1-72a.cisco.com." Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the RSA key is encrypted (protected) and unlocked.

```
Router(config)# crypto key encrypt rsa name pki1-72a.cisco.com passphrase cisco1234
Router(config)# exit
Router# show crypto key mypubkey rsa

% Key pair was generated at:00:15:32 GMT Jun 25 2003
Key name:pki1-72a.cisco.com
Usage:General Purpose Key
*** The key is protected and UNLOCKED. ***
```

```
Key is not exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E0CC9A 1D23B52C
CD00910C ABD392AE BA6D0E3F FC47A0EF 8AFEE340 0EC1E62B D40E7DCC
23C4D09E
03018B98 E0C07B42 3CFD1A32 2A3A13C0 1FF919C5 8DE9565F 1F020301 0001
% Key pair was generated at:00:15:33 GMT Jun 25 2003
Key name:pki1-72a.cisco.com.server
Usage:Encryption Key
Key is exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D3491E 2A21D383
854D7DA8 58AFBDAC 4E11A7DD E6C40AC6 66473A9F 0C845120 7C0C6EC8 1FFF5757
3A41CE04 FDCB40A4 B9C68B4F BC7D624B 470339A3 DE739D3E F7DDB549 91CD4DA4
DF190D26 7033958C 8A61787B D40D28B8 29BCD0ED 4E6275C0 6D020301 0001
Router#
```

The following example shows how to lock the key "pki1-72a.cisco.com." Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the key is protected (encrypted) and locked.

```
Router# crypto key lock rsa name pki1-72a.cisco.com passphrase cisco1234
!
Router# show crypto key mypubkey rsa

% Key pair was generated at:20:29:41 GMT Jun 20 2003
Key name:pki1-72a.cisco.com
Usage:General Purpose Key
*** The key is protected and LOCKED. ***
Key is exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D7808D C5FF14AC
0D2B55AC 5D199F2F 7CB4B355 C555E07B 6D0DECBE 4519B1F0 75B12D6F 902D6E9F
B6FDAD8D 654EF851 5701D5D7 EDA047ED 9A2A619D 5639DF18 EB020301 0001
```

Related Commands

Command	Description
crypto key encrypt rsa	Encrypts the RSA private key.
crypto key generate rsa (IKE)	Generates RSA key pairs.
crypto key lock rsa	Locks the RSA private key in a router.

show crypto key pubkey-chain rsa

To display the RSA public keys of the peer that are stored on your router, use the **show crypto key pubkey-chain rsa** command in EXEC mode.

show crypto key pubkey-chain rsa [**name** *key-name* | **address** *key-address*]

Syntax Description

name *key-name*	(Optional) The name of a particular public key to view.
address *key-address*	(Optional) The address of a particular public key to view.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command shows RSA public keys stored on your router. This includes peers' RSA public keys manually configured at your router and keys received by your router via other means (such as by a certificate, if certification authority support is configured).

If a router reboots, any public key derived by certificates will be lost. This is because the router will ask for certificates again, at which time the public key will be derived again.

Use the **name** or **address** keywords to display details about a particular RSA public key stored on your router.

If no keywords are used, this command displays a list of all RSA public keys stored on your router.

Examples

The following is sample output from the **show crypto key pubkey-chain rsa** command:

```
Router# show crypto key pubkey-chain rsa

Codes: M - Manually Configured, C - Extracted from certificate

Code  Usage        IP-address     Name
M     Signature    10.0.0.1       myrouter.example.com
M     Encryption   10.0.0.1       myrouter.example.com
C     Signature    172.16.0.1     routerA.example.com
C     Encryption   172.16.0.1     routerA.example.com
C     General      192.168.10.3   routerB.domain1.com
```

This sample shows manually configured special usage RSA public keys for the peer "somerouter." This sample also shows three keys obtained from peers' certificates: special usage keys for peer "routerA" and a general purpose key for peer "routerB."

Certificate support is used in the above example; if certificate support was not in use, none of the peers' keys would show "C" in the code column, but would all have to be manually configured.

The following is sample output when you issue the command **show crypto key pubkey rsa name somerouter.example.com**:

```
Router# show crypto key pubkey rsa name somerouter.example.com

Key name: somerouter.example.com
Key address: 10.0.0.1
 Usage: Signature Key
 Source: Manual
 Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
  04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
  BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001

Key name: somerouter.example.com
Key address: 10.0.0.1
 Usage: Encryption Key
 Source: Manual
 Data:
  00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5
  18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB
  07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

Note The Source field in the above example indicates "Manual," meaning that the keys were manually configured on the router, not received in the peer's certificate.

The following is sample output when you issue the command **show crypto key pubkey rsa address 192.168.10.3**:

```
Router# show crypto key pubkey rsa address 192.168.10.3

Key name: routerB.example.com
Key address: 192.168.10.3
 Usage: General Purpose Key
 Source: Certificate
 Data:
  0738BC7A 2BC3E9F0 679B00FE 53987BCC 01030201 42DD06AF E228D24C 458AD228
  58BB5DDD F4836401 2A2D7163 219F882E 64CE69D4 B583748A 241BED0F 6E7F2F16
  0DE0986E DF02031F 4B0B0912 F68200C4 C625C389 0BFF3321 A2598935 C1B1
```

The Source field in the above example indicates "Certificate," meaning that the keys were received by the router by way of the other router's certificate.

show crypto map (IPSec)

To display the crypto map configuration, use the **show crypto map** command in privileged EXEC or user EXEC mode.

show crypto map [**interface** *interface* | **tag** *map-name*]

Syntax Description

interface *interface*	(Optional) Displays only the crypto map set that is applied to the specified interface.
tag *map-name*	(Optional) Displays only the crypto map set with the specified *map-name*.

Defaults

No crypto maps are shown.

Command Modes

Privileged EXEC
User EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.3(8)T	Output has been modified to display the crypto input and output access control lists (ACLs) that have been configured.

Usage Guidelines

The **show crypto map** command provides output that is IP specific, and it allows you to specify a particular crypto map.

Examples

The following example shows that crypto input and output ACLs have been configured:

```
Router# show crypto map

Crypto Map "test" 10 ipsec-isakmp
 Peer
 Extended IP access list ipsec_acl
  access-list ipsec_acl permit ip 192.168.2.0 0.0.0.255 192.168.102.0 0.0.0.255
 Extended IP access check IN list 110
  access-list 110 permit ip host 192.168.102.47 192.168.2.0 0.0.0.15
  access-list 110 permit ip host 192.168.102.47 192.168.2.32 0.0.0.15
  access-list 110 permit ip host 192.168.102.47 192.168.2.64 0.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.0 0.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.32 0.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.64 0.0.0.15
 Extended IP access check OUT list 120
  access-list 120 permit ip 192.168.2.0 0.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.32 0.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.64 0.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.0 0.0.0.15 host 192.168.102.57
  access-list 120 permit ip 192.168.2.32 0.0.0.15 host 192.168.102.57
  access-list 120 permit ip 192.168.2.64 0.0.0.15 host 192.168.102.57
```

```
Current peer: 10.0.0.2
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets=test
Interfaces using crypto map test:
 Serial0/1
```

Table 45 describes the output in the display.

Table 45 show crypto map Command Field Descriptions

Field	Description
Peer	Possible peers that are configured for this crypto map entry.
Extended IP access list	Access list that is used to define which data packets are to be encrypted. Packets that are denied by this access list are forwarded but not encrypted. The “reverse” of this access list is used to check the inbound return packets, which are also encrypted. Packets that are denied by the “reverse” access list are dropped because they should have been encrypted but were not.
Extended IP access list check	Access lists that are used to more finely control which data packets are allowed into or out of the IPSec tunnel. Packets that are allowed by the “Extended IP access list” ACL but denied by the “Extended IP access list check” ACL are dropped.
Current peer	Current peer that is being used for this crypto map entry.
Security association lifetime	Number of bytes that are allowed to be encrypted or decrypted or the age of the security association before new encryption keys must be negotiated.
PFS	(Perfect Forward Secrecy) If “Yes,” the Internet Security Association (ISAKMP) SKEYID-d key is also renegotiated each time IPSec security association (SA) encryption keys are renegotiated (requires another Diffie-Hillman calculation). Otherwise, the same ISAKMP SKEYID-d key is used when renegotiating IPSec SA encryption keys. ISAKMP keys are renegotiated on a separate schedule, with a default time of 24 hours.
Transform sets	List of transform sets (encryption, authentication, and compression algorithms) that can be used with this crypto map.
Interfaces using crypto map test	Interfaces to which this crypto map is applied. Packets that are leaving from this interface are subject to the rules of this crypto map for encryption. Encrypted packets may enter the router on any interface, and they will be decrypted. Nonencrypted packets that are entering the router through this interface are subject to the “reverse” crypto access list check.

show crypto mib ipsec flowmib history failure size

To display the size of the IP Security (IPSec) failure history table, use the **show crypto mib ipsec flowmib history failure size** command in privileged EXEC mode.

show crypto mib ipsec flowmib history failure size

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.

Examples

The following is sample output from the **show crypto mib ipsec flowmib history failure size** command:

```
Router# show crypto mib ipsec flowmib history failure size

IPSec Failure Window size: 140
```

Related Commands

Command	Description
crypto mib ipsec flowmib history failure size	Changes the size of the IPSec failure history table.
show crypto mib ipsec flowmib version	Displays the IPSec Flow MIB version used by the router.

show crypto mib ipsec flowmib history tunnel size

To display the size of the IP Security (IPSec) tunnel history table, use the **show crypto mib ipsec flowmib history tunnel size** command in privileged EXEC mode.

show crypto mib ipsec flowmib history tunnel *size*

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.

Examples

The following is sample output from the **show crypto mib ipsec flowmib history tunnel size** command:

```
Router# show crypto mib ipsec flowmib history tunnel size

IPSec History Window Size: 130
```

Related Commands

Command	Description
crypto mib ipsec flowmib history tunnel size	Changes the size of the IPSec tunnel history table.
show crypto mib ipsec flowmib version	Displays the IPSec Flow MIB version used by the router.

show crypto mib ipsec flowmib version

To display the IP Security (IPSec) MIB version used by the router, use the **show crypto mib ipsec flowmib version** command in privileged EXEC mode.

show crypto mib ipsec flowmib version

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.

Usage Guidelines

Use the **show crypto mib ipsec flowmib version** command to display the MIB version used by the management applications to identify the feature set.

Note The MIB version can also be obtained by querying the MIB element cipSecMibLevel using Simple Network Management Protocol (SNMP).

Examples

The following is sample output from the **show crypto mib ipsec flowmib version** command:

```
Router# show crypto mib ipsec flowmib version

IPSec Flow MIB version: 1
```

Related Commands

Command	Description
show crypto mib ipsec flowmib history failure size	Displays the size of the IPSec failure history table.
show crypto mib ipsec flowmib history tunnel size	Displays the size of the IPSec tunnel history table.

show crypto pki certificates

To display information about your certificate, the certification authority certificate, and any registration authority certificates, use the **show crypto pki certificates** command in EXEC mode.

show crypto pki certificates [*trustpoint-name* **[verbose]]**

Syntax Description

trustpoint-name	(Optional) Name of the trustpoint. Using this argument indicates that only certificates that are related to the trustpoint are to be displayed.
verbose	(Optional) More detailed information is to be displayed. **Note** The **verbose** keyword can be used only if a trustpoint name is entered.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	The **show crypto ca certificates** command was introduced.
12.2(13)T	The *trustpoint-name* argument was added.
12.3(7)T	This command replaced the **show crypto ca certificates** command.
12.3(8)T	The **verbose** keyword was added.

Usage Guidelines

This command shows information about the following certificates:

- Your certificate, if you have requested one from the CA (see the **crypto pki enroll** command)
- The certificate of the CA, if you have received the certificate of the CA (see the **crypto pki authenticate** command)
- RA certificates, if you have received RA certificates (see the **crypto pki authenticate** command)

Examples

The following is sample output from the **show crypto pki certificates** command after you authenticated the CA by requesting the certificate of the CA and public key with the **crypto pki authenticate** command:

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The CA certificate might show Key Usage as “Not Set.”

The following is sample output from the **show crypto pki certificates** command, and it shows the certificate of the router and the certificate of the CA. In this example, a single, general-purpose Rivest, Shamir, and Adelman (RSA) key pair was previously generated, and a certificate was requested but not received for that key pair.

```
Certificate
  Subject Name
```

```
    Name: myrouter.example.com
    IP Address: 10.0.0.1
    Serial Number: 04806682
  Status: Pending
  Key Usage: General Purpose
    Fingerprint: 428125BD A3419600 3F6C7831 6CD8FA95 00000000

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

Note that in the previous sample, the certificate status of the router shows "Pending." After the router receives its certificate from the CA, the Status field changes to "Available" in the **show** output.

The following is sample output from the **show crypto pki certificates** command, and it shows the certificates of two routers and the certificate of the CA. In this example, special-usage RSA key pairs were previously generated, and a certificate was requested and received for each key pair.

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 428125BDA34196003F6C78316CD8FA95
  Key Usage: Signature

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: AB352356AFCD0395E333CCFD7CD33897
  Key Usage: Encryption

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The following is sample output from the **show crypto pki certificates** command when the CA supports an RA. In this example, the CA and RA certificates were previously requested with the **crypto pki authenticate** command.

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set

RA Signature Certificate
  Status: Available
  Certificate Serial Number: 34BCF8A0
  Key Usage: Signature

RA KeyEncipher Certificate
  Status: Available
  Certificate Serial Number: 34BCF89F
  Key Usage: Encryption
```

The following is sample output from the **show crypto pki certificates** command using the optional *trustpoint-name* argument and **verbose** keyword. The output shows the certificate of a router and the certificate of the CA. In this example, general-purpose RSA key pairs were previously generated, and a certificate was requested and received for the key pair.

```
Certificate
   Status: Available
   Version: 3
   Certificate Serial Number: 18C1EE03000000004CBD
   Certificate Usage: General Purpose
   Issuer:
     cn=msca-root
     ou=pki msca-root
     o=cisco
     l=santa cruz2
     st=CA
     c=US
     ea=user@example.com
   Subject:
     Name: myrouter.example.com
     hostname=myrouter.example.com
   CRL Distribution Points:
     http://msca-root/CertEnroll/msca-root.crl
   Validity Date:
     start date: 19:50:40 GMT Oct 5 2004
     end   date: 20:00:40 GMT Oct 12 2004
   Subject Key Info:
     Public Key Algorithm: rsaEncryption
     RSA Public Key: (360 bit)
   Signature Algorithm: SHA1 with RSA Encryption
   Fingerprint MD5: 2B5F53E6 E3E892E6 3A9D3706 01261F10
   Fingerprint SHA1: 315D127C 3AD34010 40CE7F3A 988BBDA5 CD528824
   X509v3 extensions:
     X509v3 Key Usage: A0000000
       Digital Signature
       Key Encipherment
     X509v3 Subject Key ID: D156E92F 46739CBA DFE66D2D 3559483E B41ECCF4
     X509v3 Authority Key ID: 37F3CC61 AF5E7C0B 434AB364 CF9FA0C1 B17C50D9
     Authority Info Access:
   Associated Trustpoints: msca-root
   Key Label: myrouter.example.com

CA Certificate
   Status: Available
   Version: 3
   Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
   Certificate Usage: Signature
   Issuer:
     cn=msca-root
     ou=pki msca-root
     o=cisco
     l=santa cruz2
     st=CA
     c=US
     ea=user@example.com
   Subject:
     cn=msca-root
     ou=pki msca-root
     o=cisco
     l=santa cruz2
     st=CA
     c=US
     ea=user@example.com
   CRL Distribution Points:
     http://msca-root.example.com/CertEnroll/msca-root.crl
   Validity Date:
     start date: 22:19:29 GMT Oct 31 2002
     end   date: 22:27:27 GMT Oct 31 2017
```

```
Subject Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (512 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: 84E470A2 38176CB1 AA0476B9 C0B4F478
Fingerprint SHA1: 0F57170C 654A5D7D 10973553 EFB0F94F 2FAF9837
X509v3 extensions:
  X509v3 Key Usage: C6000000
    Digital Signature
    Non Repudiation
    Key Cert Sign
    CRL Signature
  X509v3 Subject Key ID: 37F3CC61 AF5E7C0B 434AB364 CF9FA0C1 B17C50D9
  X509v3 Basic Constraints:
      CA: TRUE
  Authority Info Access:
Associated Trustpoints: msca-root
```

Related Commands

Command	Description
crypto pki authenticate	Authenticates the CA (by obtaining the certificate of the CA).
crypto pki enroll	Obtains the certificates of your router from the CA.
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the route.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.

show crypto pki crls

To display the current certificate revocation list (CRL) on router, use the **show crypto pki crls** command in EXEC mode.

show crypto pki crls

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.1	The **show crypto ca crls** command was introduced.
12.3(7)T	This command replaced the **show crypto ca crls** command.

Examples

The following is sample output of the **show crypto pki crls** command:

```
Router# show crypto pki crls

          CRL Issuer Name:
              OU = sjvpn, O = cisco, C = us
              LastUpdate: 16:17:34 PST Jan 10 2002
              NextUpdate: 17:17:34 PST Jan 11 2002
              Retrieved from CRL Distribution Point:
                LDAP: CN = CRL1, OU = sjvpn, O = cisco, C = us
```

Related Commands

Command	Description
crypto pki crl request	Requests that a new CRL be obtained immediately from the CA.

show crypto pki server

To display the current state and configuration of the certificate server, use the **show crypto pki server** command in privileged EXEC mode.

show crypto pki server

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

At startup, the certificate server must check the current configuration before issuing any certificates. As it starts up, the certificate server transitions through the states defined in Table 46. Use the **show crypto pki server** command to display the state of the certificate server.

Table 46 States of the Certificate Server

Certificate Server State	Description
configured	The server is available and has generated the certificate server certificates.
storage configuration incomplete	The server is verifying that the configured storage location is available.
waiting for HTTP server	The server is verifying that the HTTP server is running.
waiting for time setting	The server is verifying that the time has been set.

Examples

The following example is sample output for the **show crypto pki server** command:

```
Router# show crypto pki server

Certificate Server status: disabled, storage configuration incomplete
    Granting mode is: manual
    Last certificate issued serial number: 0
    CA certificate expiration timer: 21:29:38 GMT Jun 5 2006
    CRL NextUpdate timer: 21:31:39 GMT Jun 6 2003
    Current storage dir: ftp://myftpserver
    Database Level: Minimum - no cert data written to storage
```

Table 47 describes the significant fields shown in the display.

Table 47 show crypto pki server Field Descriptions

Field	Description
Granting mode is	Specifies whether certificate enrollment requests should be granted manually (which is the default) or automatic (via the **grant automatic** command). **Note** The **grant automatic** command should be used *only* when testing and building simple networks. This command *must* be disabled before the network is accessible by the Internet.
Last certificate issued serial number	The serial number of the latest certificate. (To specify the distinguished name (DN) as the certification authority (CA) issuer name, use the **issuer-name** command.)
CA certificate expiration timer	The expiration date for the CA certificate. (To specify the expiration date, use the **lifetime** command.)
CRL NextUpdate timer	The next time the certificate revocation list (CRL) will be updated. (To specify the CRL lifetime, in hours, use the **lifetime crl** command.
Current storage dir	The location where all database entries for the certificate server will be written out. (To specify a location, use the **database url** command.)
Database Level	The type of data that is stored in the certificate enrollment database—minimal, names, or complete. (To specify the data type to be stored, use **database level** command.)

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enter certificate server configuration mode.

show crypto pki timers

To display the status of the managed timers that are maintained by Cisco IOS for public key infrastructure (PKI), use the **show crypto pki timers** command in EXEC mode.

show crypto pki timers

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(8)T	The **show crypto ca timers** command was introduced.
12.3(7)T	This command replaced the **show crypto ca timers** command.

Usage Guidelines

For each timer, this command displays the time remaining before the timer expires. It also associates trustpoint certification authorities (CAs), except for certificate revocation list (CRL) timers, by displaying the CRL distribution point.

Examples

The following example is sample output for the **show crypto pki timers** command:

```
Router# show crypto pki timers

PKI Timers
| 4d15:13:33.144
 | 4d15:13:33.144  CRL http://msca-root.cisco.com/CertEnroll/msca-root.crl
 |328d11:56:48.372  RENEW msroot
 | 6:43.201  POLL verisign
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crypto pki trustpoint	Declares the CA that your router should use.

show crypto pki trustpoints

To display the trustpoints that are configured in the router, use the **show crypto pki trustpoints** command in privileged or user EXEC mode.

show crypto pki trustpoints [**status** | *label* [**status**]]

Syntax Description

status	(Optional) Trustpoint status.
label	(Optional) Trustpoint name.

Defaults

If the *label* argument (trustpoint name) is not specified, command output is displayed for all trustpoints.

Command Modes

Privileged EXEC mode
User EXEC mode

Command History

Release	Modification
12.2(8)T	The **show crypto ca trustpoints** command was introduced.
12.3(7)T	This command replaced the **show crypto ca trustpoints** command.
12.3(11)T	The **status** keyword and *label* argument were added.

Usage Guidelines

If you enter the **show crypto ca roots** command, it will have the same effect as entering the **show crypto pki trustpoints** command.

Examples

The following is sample output from the **show crypto pki trustpoints** command:

```
Router# show crypto pki trustpoints

Trustpoint bo:
    Subject Name:
    CN = bomborra Certificate Manager
     O = cisco.com
     C = US
          Serial Number:01
    Certificate configured.
    CEP URL:http://bomborra
    CRL query url:ldap://bomborra
```

The following output using the **status** keyword shows that the trustpoint is configured in query mode and is currently trying to query the certificates (the CA certificate and the router certificate are both pending):

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate pending:
    Subject Name:
```

```
    cn=nsca-r1 Cert Manager,ou=pki,o=cisco.com,c=US
   Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router certificate pending:
   Subject Name:
    hostname=trance.cisco.com,o=cisco.com
  Next query attempt:
   52 seconds
```

The following output using the **status** keyword shows that the trustpoint has been authenticated:

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=nsca-r1 Cert Manager,ou=pki,o=cisco.com,c=US
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  State:
    Keys generated ..... No
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... None
```

The following output using the **status** keyword shows that the trustpoint is enrolling and that two of the certificate requests are pending (Signature and Encryption):

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=nsca-r1 Cert Manager,ou=pki,o=cisco.com,c=US
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router Signature certificate pending:
    Requested Subject Name:
     hostname=trance.cisco.com
    Request Fingerprint: FAE0D74E BB844EA1 54B26698 56AB42EC
    Enrollment polling: 1 times (9 left)
    Next poll: 32 seconds
  Router Encryption certificate pending:
    Requested Subject Name:
     hostname=trance.cisco.com
    Request Fingerprint: F4E815DB D9D9B60F 9B5B1724 3E155DBF
    Enrollment polling: 1 times (9 left)
    Next poll: 44 seconds
  Last enrollment status: Pending
  State:
    Keys generated ..... Yes (Signature, Encryption)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Pending
```

The following output using the **status** keyword shows that enrollment has succeeded and that two router certificates have been granted (Signature and Encryption):

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=nsca-r1 Cert Manager,ou=pki,o=cisco.com,c=US
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router Signature certificate configured:
    Subject Name:
     hostname=trance.cisco.com,o=cisco.com
    Fingerprint: 8A370B8B 3B6A2464 F962178E 8385E9D6
```

```
  Router Encryption certificate configured:
    Subject Name:
     hostname=trance.cisco.com,o=cisco.com
    Fingerprint: 43A03218 C0AFF844 AE0C162A 690B414A
  Last enrollment status: Granted
  State:
    Keys generated ..... Yes (Signature, Encryption)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes
```

The following output using the **status** keyword shows that trustpoint enrollment has been rejected:

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=nsca-r1 Cert Manager,ou=pki,o=cisco.com,c=US
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Last enrollment status: Rejected
  State:
    Keys generated ..... Yes (General Purpose)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... None
```

The following output using the **status** keyword shows that enrollment has succeeded and that the router is configured for autoenrollment using a regenerated key. In addition, the running configuration has been modified so that it will not be saved automatically after autoenrollment.

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=nsca-r1 Cert Manager,ou=pki,o=cisco.com,c=US
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router General Purpose certificate configured:
    Subject Name:
     hostname=trance.cisco.com,o=cisco.com
    Fingerprint: FC365F95 E24D4B55 81347510 10FFE331
  Last enrollment status: Granted
  Next enrollment attempt:
    01:58:25 PST Feb 14 2004
    * A new key will be generated *
    * Configuration will not be saved after enrollment *
  State:
    Keys generated ..... Yes (General Purpose)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes
```

Table 48 describes the significant fields shown in the display.

Table 48 show crypto ca trustpoints Field Descriptions

Field	Description
Trustpoint	Name of the trustpoint.
Issuing CA certificate pending	The certification authority (CA) certificate is being retrieved (query mode).
Issuing CA certificate [not] configured	A CA certificate is [not] configured.
Subject Name	Subject name of the indicated certificate.

Table 48 show crypto ca trustpoints Field Descriptions (continued)

Field	Description
Next query attempt	Time until the next query attempt (query mode).
Router certificate pending/Router [key usage] certificate pending	The trustpoint is attempting to obtain the certificate from the CA server (through query mode or enrollment).
Router [key usage] certificate configured	Certificate of the specified key usage is configured.
Requested Subject Name	Subject name used in the enrollment request (Public Key Cryptography Standards 10 [PKCS10]).
Fingerprint MD5/SHA1	Fingerprint of the indicated certificate (Message Digest 5 [MD5] or Secure Hash Algorithm 1 [SHA]1).
Request Fingerprint MD5/SHA1	Fingerprint of the PKCS10 enrollment request (MD5/SHA1).
Enrollment polling: [polled] times ([remaining] left)/Next poll: in seconds	Number of Simple Certificate Enrollment Protocol (SCEP) polling attempts that have been made and that remain before the router gives up/Time until the next polling attempt.
Last enrollment status: Pending/Granted/Rejected/Failed	Last enrollment attempt status (pending, granted, rejected, or failed).
Next enrollment attempt: *time* (Optional) A new key will be generated. (Optional) Configuration will not be saved after enrollment.	The trustpoint is configured to do auto-enrollment and the auto-enrollment will happen at *time.* (Optional) The trustpoint is configured to generate a new key when auto-enrollment occurs. (Optional) The running configuration is “dirty,” so the configuration will not be saved automatically after autoenrollment.
State	Current state of the trustpoint.
Keys generated	“Yes or No” and the key usage (General Purpose or Signature, Encryption).
Issuing CA authenticated	“Yes or No” if crypto CA authentication has been done successfully.
Certificate request(s)	Progress of current enrollment: “Pending,” “Yes,” (complete), or “None” (not in progress).

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

show crypto session

To display status information for active crypto sessions, use the **show crypto session** command in privileged EXEC mode.

show crypto session [detail] | [local *ip-address* **[port** *local-port***] [remote** *ip-address* **[port** *remote-port***]] [detail]] | [fvfr** *vrf-name***] [ivrf** *vrf-name***] [detail]**

IPSec and IKE Stateful Failover Syntax

show crypto session [active | standby]

Syntax Description

detail	(Optional) **Provides more detailed information about the session, such as the capability of the Internet Key Exchange (IKE) security association (SA), connection ID, remaining lifetime of the IKE SA, inbound or outbound encrypted or decrypted packet number of the IP Security (IPSec) flow, dropped packet number, and kilobyte-per-second lifetime of the IPSec SA.**
local *ip-address*	(Optional) Displays status information about crypto sessions of a local crypto endpoint. • *The ip-address* value is the IP address of the local crypto endpoint.
port *local-port*	(Optional) Port of the local crypto endpoint. • *The local-port* value can be 1 through 65535. The default value is 500.
remote *ip-address*	(Optional) Displays status information about crypto sessions of a remote session. • *The ip-address* value is the IP address of the remote crypto endpoint.
port *remote-port*	(Optional) Displays status information about crypto sessions of a remote crypto endpoint. • *The remote-port* value can be 1 through 65535. The default value is 500.
fvfr *vrf-name*	(Optional) Displays status information about the front door virtual routing and forwarding (FVRF) session.
ivrf *vrf-name*	(Optional) Displays status information about the inside VRF (IVRF) session.
active	(Optional) Displays all crypto sessions in the active state.
standby	(Optional) Displays all crypto sessions that are in the standby state.

Defaults

If the **show crypto session** command is entered without any keywords, all existing sessions will be displayed. Port default values are 500.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(11)T	The **active** and **standby** keywords were added.

Usage Guidelines

You can get a list of all the active Virtual Private Network (VPN) sessions and of the IKE and IPSec SAs for each VPN session by entering the **show crypto session** command. The listing will include the following:

- Interface
- IKE peer description, if available
- IKE SAs that are associated with the peer by whom the IPSec SAs are created
- IPSec SAs serving the flows of a session

Multiple IKE or IPSec SAs may be established for the same peer (for the same session), in which case IKE peer descriptions will be repeated with different values for the IKE SAs that are associated with the peer and for the IPSec SAs that are serving the flows of the session.

Examples

The following example shows active VPN sessions:

```
Router# show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication

Interface: Ethernet1/0
Session status: UP-NO-IKE
Peer: 10.2.80.179/500 fvrf: (none) ivrf: (none)
      Desc: My-manual-keyed-peer
      Phase1_id: 10.2.80.179
  IPSEC FLOW: permit ip host 10.2.80.190 host 10.2.80.179
        Active SAs: 4, origin: manual-keyed crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

Interface: Ethernet1/2
Session status: DOWN
Peer: 10.1.1.1/500 fvrf: (none) ivrf: (none)
      Desc: SJC24-2-VPN-Gateway
      Phase1_id: 10.1.1.1
  IPSEC FLOW: permit ip host 10.2.2.3 host 10.2.2.2
        Active SAs: 0, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
  IPSEC FLOW: permit ip 10.2.0.0/255.255.0.0 10.4.0.0/255.255.0.0
        Active SAs: 0, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

Interface: Serial2/0.17
Session status: UP-ACTIVE
Peer: 10.1.1.5/500 fvrf: (none) ivrf: (none)
      Desc: (none)
      Phase1_id: 10.1.1.5
  IKE SA: local 10.1.1.5/500 remote 10.1.1.5/500 Active
```

```
        Capabilities:(none) connid:1 lifetime:00:59:51
IPSEC FLOW: permit ip host 10.1.1.5 host 10.1.2.5
      Active SAs: 2, origin: dynamic crypto map
      Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 20085/171
      Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 20086/171
```

Table 49 describes the significant fields shown in the display.

Table 49 show crypto session Field Descriptions

Field	Description
Interface	Interface to which the crypto session is related.
Session status	Current status of the crypto (VPN) sessions. See Table 50 for the status of the IKE SA, IPSec SA, and tunnel as shown in the display.
IKE SA	Information is provided about the IKE SA, such as local and remote address and port, SA status, SA capabilities, crypto engine connection ID, and remaining lifetime of the IKE SA.
IPSEC FLOW	A snapshot of information about the IPSec-protected traffic flow, such as what the flow is (for example, permit ip host 10.1.1.5 host 10.1.2.5); how many IPSec SAs there are; the origin of the SA, such as manual keyed, dynamic, or static crypto map; the number of encrypted or decrypted packets or dropped packets; and the IPSec SA remaining lifetime in kilobytes per second.

Table 50 provides an explanation of the current status of the VPN sessions shown in the display.

Table 50 Current Status of the VPN Sessions

IKE SA	IPSec SA	Tunnel Status
Exist, active	Exist (flow exists)	UP-ACTIVE
Exist, active	None (flow exists)	UP-IDLE
Exist, active	None (no flow)	UP-IDLE
Exist, inactive	Exist (flow exists)	UP-NO-IKE
Exist, inactive	None (flow exists)	DOWN-NEGOTIATING
Exist, inactive	None (no flow)	DOWN-NEGOTIATING
None	Exist (flow exists)	UP-NO-IKE
None	None (flow exists)	DOWN
None	None (no flow)	DOWN

Note IPSec flow may not exist if a dynamic crypto map is being used.

The following sample output shows all crypto sessions that are in the standby state:

```
Router# show crypto session standby
Crypto session current status
```

```
Interface: Ethernet0/0
Session status: UP-STANDBY
Peer: 209.165.200.225 port 500
  IKE SA: local 209.165.201.3/500 remote 209.165.200.225/500 Active
  IKE SA: local 209.165.201.3/500 remote 209.165.200.225/500 Active
  IPSEC FLOW: permit ip host 192.168.0.1 host 172.16.0.1
        Active SAs: 4, origin: crypto map
```

Related Commands

Command	Description
clear crypto session	Deletes crypto sessions (IPSec and IKE SAs).
description	Adds a description for an IKE peer.
show crypto isakmp peer	Displays peer descriptions.

show crypto session group

To display groups that are currently active on the Virtual Private Network (VPN) device, use the **show crypto session group** command in privileged EXEC mode.

show crypto session group

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

If the **crypto isakmp client configuration group** command and **max-users** keyword have not been enabled in any VPN group profile, this command will yield a blank result.

Examples

The following example shows that at least one session is active for the group Connections:

```
Router# show crypto session group
 Group: Connections
 cisco: 1
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
show crypto session summary	Displays groups that are currently active on the VPN device and the users that are connected for each of those groups.

show crypto session summary

To display groups that are currently active on the Virtual Private Network (VPN) device and the users that are connected for each of those groups, use the **show crypto session summary** command in privileged EXEC mode.

show crypto session summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

If the **crypto isakmp client configuration group** command and **max-users** keyword are not enabled in any VPN group profile and the **crypto isakmp client configuration group** command and **max-logins** keyword are not enabled, this command will yield a blank result.

Examples

The following example shows that the group “cisco” is active and that it has one user connected, green, who is connected one time. The number in parentheses (1) is the number of simultaneous logins for that user.

```
Router# show crypto session summary

 Group cisco has 1 connections
  User (Logins)
  green (1)
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
show crypto session group	Displays groups that are currently active on the VPN device.

show dnsix

To display state information and the current configuration of the DNSIX audit writing module, use the **show dnsix** command in privileged EXEC mode.

show dnsix

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show dnsix** command:

```
Router# show dnsix

Audit Trail Enabled with Source 192.168.2.5
          State: PRIMARY
          Connected to 192.168.2.4
          Primary 192.168.2.4
          Transmit Count 1
          DMDP retries 4
          Authorization Redirection List:
               192.168.2.4
          Record count: 0
          Packet Count: 0
          Redirect Rcv: 0
```

show dot1x

To show details for an identity profile, use the **show dot1x** command in privileged EXEC mode.

show dot1x [interface *interface-name* [**details**]]

Syntax Description

interface *interface-name*	(Optional) Name of the interface.
details	(Optional) Displays 802.1X details for the specified interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(11)T	The PAE, HeldPeriod, StartPeriod, and MaxStart fields were added to the **show dot1x** command output.

Examples

The following is sample output for the **show dot1x** command:

```
Router# show dot1x

Sysauthcontrol  = Disabled
Dot1x Version   = 1

Dot1x Info for interface Ethernet0
----------------------------------------
PortControl       = AUTO
ReAuthentication  = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
QuietWhile        = 120 Seconds
MaxReq            = 2

Dot1x Info for interface Ethernet1
----------------------------------------
PortControl       = AUTO
ReAuthentication  = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
QuietWhile        = 120 Seconds
MaxReq            = 2
```

The following is sample output for the **show dot1x** command using the **interface** and **details** keywords. The clients are authenticated in this output example.

```
Router# show dot1x interface ethernet 0 details

PortControl       = AUTO
```

```
ReAuthentication  = Enabled
ReAuthPeriod      = 36000 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
QuietWhile        = 120 Seconds
MaxReq            = 2


Dot1x Client List
-----------------------------------
MAC Address         State
-----------------------------------
0000.1111.0001      AUTHENTICATED
0000.1111.0002      UNAUTHENTICATED
```

The following **show dot1x** sample output shows information for all three possible interface configurations (that is, as an authenticator, as a supplicant, and as an authenticator and supplicant).

```
Router# show dot1x

Sysauthcontrol     = Enabled
Dot1x Version      = 1

Dot1x Information for interface Ethernet0
----------------------------------------
PortControl        = AUTO
PAE                = AUTHENTICATOR
ReAuthentication   = Enabled
ReAuthPeriod       = 60 Seconds
ServerTimeout      = 30 Seconds
SuppTimeout        = 30 Seconds
QuietWhile         = 120 Seconds
MaxReq             = 2

Dot1x Information for interface Ethernet1
----------------------------------------
PortControl        = AUTO
PAE                = SUPPLICANT
AuthPeriod         = 30
HeldPeriod         = 60 Seconds
StartPeriod        = 30 Seconds
MaxStart           = 2

Dot1x Information for interface Ethernet2
----------------------------------------
PortControl        = AUTO
PAE                = BOTH
ReAuthentication   = Enabled
ReAuthPeriod       = 60 Seconds
ServerTimeout      = 30 Seconds
SuppTimeout        = 30 Seconds
QuietWhile         = 120 Seconds
MaxReq             = 2
AuthPeriod         = 30
HeldPeriod         = 60 Seconds
StartPeriod        = 30 Seconds
MaxStart           = 2
```

The following is sample output for the **show dot1x** command using the **interface** and **details** keywords.

```
Router# show dot1x interface ethernet0

PortControl        = AUTO
PAE                = AUTHENTICATOR
```

```
ReAuthentication    = Enabled
ReAuthPeriod        = 60 Seconds
ServerTimeout       = 30 Seconds
SuppTimeout         = 30 Seconds
QuietWhile          = 120 Seconds
MaxReq              = 2

Router# show dot1x interface ethernet0 details

PortControl         = AUTO
PAE                 = SUPPLICANT
ReAuthentication    = Enabled
ReAuthPeriod        = 60 Seconds
ServerTimeout       = 30 Seconds
SuppTimeout         = 30 Seconds
QuietWhile          = 120 Seconds
MaxReq              = 2


Dot1x Client List
-------------------------------------
MAC Address          State
-------------------------------------
0001.f380.87ce       AUTHENTICATED
0001.87ce.f380       AUTHENTICATING
0010.a7b4.97af       UNAUTHENTICATED


Dot1x List of Supplicant Instances
-----------------------------------------
MAC Address           State
-----------------------------------------
0180.c200.0003        AUTHORIZED
```

Table 51 describes the significant fields shown in the displays.

Table 51 show dot1x Field Descriptions

Field	Description
Sysauthcontrol	802.1X port-based authentication is enabled or disabled.
PortControl	Port control value. • AUTO—the authentication status of the client PC is being determined by the authentication process. • Force-authorize—all the client PCs on the interface are being authorized. • Force-unauthorized—all the client PCs on the interface are being unauthorized.
PAE	Port Access Entity. Defines the role of an interface (as a supplicant, as an authenticator, or as an authenticator and supplicant).
ReAuthentication	Periodic reauthentication of client PCs on the interface has been enabled or disabled.
ReAuthPeriod	Time after which an automatic reauthentication will be initiated.

Table 51 show dot1x Field Descriptions (continued)

Field	Description
ServerTimeout	Timeout that has been set for RADIUS retries. If an 802.1X packet is sent to the server and the server does not send a response, the packet will be sent again after the number of seconds that are shown.
SuppTimeout	Time that has been set for supplicant (client PC) retries. If an 802.1X packet is sent to the supplicant and the supplicant does not send a response, the packet will be sent again after the number of seconds that are shown.
QuietWhile	After authentication fails for a client, the authentication gets restarted after the quiet period that is shown.
RateLimit	The period that EAP-start packets are throttled from misbehaving supplicants.
MaxReq	Maximum number of times that the router sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client PC before concluding that the client PC does not support 802.1X.
HeldPeriod	Interval for which the supplicant (client PC) will wait before trying to send its credentials after being unauthenticated by the authenticator.
StartPeriod	Interval between two successive Extensible Authentication Protocol over LAN- (EAPOL-) start messages (when they are being retransmitted).
MaxStart	Number of EAPOL-start messages that the supplicant (client PC) sends before the supplicant assumes that the other end is not 802.1X capable.
Dot1x Client List	Table providing information regarding MAC addresses and the state of the PCs. This list displays in the output if the interface is configured only as an authenticator or as an authenticator and a supplicant. If the interface is configured as a supplicant, a separate list is displayed.
Dot1x List of Supplicant Instances	Table providing information regarding MAC addresses and the state of the PCs. This list displays in the output if the interface is configured only as a supplicant.
MAC Address	List of MAC addresses (for example, the MAC address of the PC or of any 802.1X client).
State	The state of the PC can be authenticated or unauthenticated.

Related Commands

Command	Description
clear dot1x	Clears 802.1X interface information.

Command	Description
debug dot1x	Displays 802.1X debugging information.
identity profile	Creates an identity profile.

show dot1x (EtherSwitch)

To display the 802.1X statistics, administrative status, and operational status for the Ethernet switch network module or for the specified interface, use the **show dot1x** command in privileged EXEC mode.

show dot1x [statistics] [interface *interface-type interface-number*]

Syntax Description

statistics	(Optional) Displays 802.1X statistics.
interface *interface-type interface-number*	(Optional) Specifies the slot and port number of the interface to reauthenticate.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

If you do not specify an interface, global parameters and a summary appear. If you specify an interface, details for that interface appear.

If you specify an interface with the **statistics** keyword, statistics appear for all physical ports.

Examples

The following is sample output from the **show dot1x** command:

```
Router# show dot1x

Global 802.1X Parameters
    reauth-enabled               no
    reauth-period              3600
    quiet-period                 60
    tx-period                    30
    supp-timeout                 30
    server-timeout               30
    reauth-max                    2
    max-req                       2

802.1X Port Summary
    Port Name               Status      Mode                Authorized
    Gi0/1                   disabled    n/a                 n/a
    Gi0/2                   enabled     Auto (negotiate)    no

    802.1X Port Details
    802.1X is disabled on GigabitEthernet0/1
```

```
802.1X is enabled on GigabitEthernet0/2
      Status                Unauthorized
      Port-control          Auto
      Supplicant            0060.b0f8.fbfb
      Multiple Hosts        Disallowed
      Current Identifier    2

      Authenticator State Machine
        State               AUTHENTICATING
        Reauth Count        1

      Backend State Machine
        State               RESPONSE
        Request Count       0
        Identifier (Server) 2

      Reauthentication State Machine
        State               INITIALIZE
```

Table 52 describes the significant fields shown in the display.

Table 52 show dot1x Field Descriptions

Field	Description
reauth-enabled	Periodic reauthentication of client PCs on the interface has been enabled or disabled.
reauth-period	Time, in seconds, after which an automatic reauthentication will be initiated.
quiet-period	After authentication fails for a client, the authentication gets restarted after this quiet period shown in seconds.
tx-period	Time, in seconds, that the device waits for a response from a client to an Extensible Authentication Protocol (EAP) request or identity frame before retransmitting the request.
supp-timeout	Time, in seconds, that has been set for supplicant (client PC) retries. If an 802.1X packet is sent to the supplicant and the supplicant does not send a response, the packet will be sent again after the number of seconds that are shown.
server-timeout	Timeout, in seconds, that has been set for RADIUS retries. If an 802.1X packet is sent to the server and the server does not send a response, the packet will be sent again after the number of seconds that are shown.
reauth-max	The maximum number of times that the device tries to authenticate the client without receiving any response before the switch resets the port and restarts the authentication process.
max-req	Maximum number of times that the router sends an EAP request/identity frame (assuming that no response is received) to the client PC before concluding that the client PC does not support 802.1X.
Port Name	Interface type and slot/port numbers.
Status	Displays the 802.1X status of the port as either enabled or disabled.

Table 52 show dot1x Field Descriptions (continued)

Field	Description
Mode	Operational status of the port: • Auto—The port control value has been configured to be Force-unauthorized but the port has not changed to that state. • n/a—802.1X is disabled.
Authorized	Authorization state of the port.
Status	Status of the port (authorized or unauthorized). The status of a port appears as authorized if the **dot1x port-control** interface configuration command is set to **auto**, and authentication was successful.
Port-control	Setting of the **dot1x port-control** interface configuration command. The port control value is one of the following: • Auto—The authentication status of the client PC is being determined by the authentication process. • Force-authorize—All the client PCs on the interface are being authorized. • Force-unauthorized—All the client PCs on the interface are being unauthorized.
Supplicant	Ethernet MAC address of the client, if one exists. If the device has not discovered the client, this field displays *Not set*.
Multiple Hosts	Setting of the **dot1x multiple-hosts** interface configuration command (allowed or disallowed).
Current Identifier	Each exchange between the device and the client includes an identifier, which matches requests with responses. This number is incremented with each exchange and can be reset by the authentication server. **Note** This field and the remaining fields in the output show internal state information. For a detailed description of these state machines and their settings, refer to the IEEE 802.1X standard.

The following is sample output from the **show dot1x interface gigabitethernet0/2** privileged EXEC command. Table 52 describes the fields in the output.

```
Router# show dot1x interface gigabitethernet0/2

802.1X is enabled on GigabitEthernet0/2
  Status                Authorized
  Port-control          Auto
  Supplicant            0060.b0f8.fbfb
  Multiple Hosts        Disallowed
  Current Identifier    3

  Authenticator State Machine
    State               AUTHENTICATED
    Reauth Count        0
```

```
  Backend State Machine
    State               IDLE
    Request Count       0
    Identifier (Server) 2

Reauthentication State Machine
    State               INITIALIZE
```

The following is sample output from the **show dot1x statistics interface gigiabitethernet0/1** command. Table 53 describes the fields in the example.

```
Router# show dot1x statistics interface gigabitethernet0/1

GigabitEthernet0/1

    Rx: EAPOL     EAPOL     EAPOL     EAPOL     EAP       EAP       EAP
        Start     Logoff    Invalid   Total     Resp/Id   Resp/Oth  LenError
        0         0         0         21        0         0         0

        Last      Last
        EAPOLVer  EAPOLSrc
        1         0002.4b29.2a03

    Tx: EAPOL     EAP       EAP
        Total     Req/Id    Req/Oth
        622       445       0
```

Table 53 show dot1x statistics Field Descriptions

Field	Description
Rx EAPOL Start	Number of valid EAPOL-start frames that have been received. **Note** EAPOL = Extensible Authentication Protocol over LAN
Rx EAPOL Logoff	Number of EAPOL-logoff frames that have been received.
Rx EAPOL Invalid	Number of EAPOL frames that have been received and have an unrecognized frame type.
Rx EAPOL Total	Number of valid EAPOL frames of any type that have been received.
Rx EAP Resp/ID	Number of EAP-response/identity frames that have been received.
Rx EAP Resp/Oth	Number of valid EAP-response frames (other than response/identity frames) that have been received.
Rx EAP LenError	Number of EAPOL frames that have been received in which the packet body length field is invalid.
Last EAPOLVer	Protocol version number carried in the most recently received EAPOL frame.
LAST EAPOLSrc	Source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	Number of EAPOL frames of any type that have been sent.
Tx EAP Req/Id	Number of EAP-request/identity frames that have been sent.
Tx EAP Req/Oth	Number of EAP-request frames (other than request/identity frames) that have been sent.

Related Commands

Command	Description
dot1x default	Resets the global 802.1X parameters to their default values.

show eou

To display information about Extensible Authentication Protocol over UDP (EAPoUDP) global values or EAPoUDP session cache entries, use the **show eou** command in privileged EXEC mode.

show eou {all | authentication {clientless | eap | static} | interface {*interface-type***} | ip {***ip-address***} | mac {***mac-address***} | posturetoken {***name***}}**

Syntax Description

all	Displays EAPoUDP information about all clients.
authentication	Authentication type.
clientless	Authentication type is clientless.
eap	Authentication type is EAP.
static	Authentication type is static.
interface	Provides information about the interface.
interface-type	Type of interface (see Table 54 for the interface types that may be shown).
ip	Specifies an IP address.
ip-address	IP address of the client device.
mac	Specifies a MAC address.
mac-address	The 48-bit address of the client device.
posturetoken	Displays information about a posture token name.
name	Name of the posture token.

Defaults

If no keywords are listed, all global EAPoUDP global values are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Table 54 lists the interface types that may be used for the *interface-type* argument.

Table 54 Description of Interface Types

Interface Type	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	Code division multiple access Internet exchange (CDMA Ix) interface
CTunnel	Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface

Table 54 Description of Interface Types

Interface Type	Description
Dialer	Dialer interface
Ethernet	IEEE 802.3 standard interface
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink frame relay bundle interface
Multilink	Multilink-group interface
Null	Null interface
Serial	Serial interface
Tunnel	Tunnel interface
Vif	Pragmatic General Multicast (PGM) Multicase Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following output displays information about a global EAPoUDP configuration. The default values can be changed or customized using the **eou default**, **eou max-retry**, **eou revalidate**, or **eou timeout** commands, depending on whether you configure them globally or as interface specific.

```
Router# show eou

Global EAPoUDP Configuration

---------------------------

EAPoUDP Version     = 1

EAPoUDP Port        = 0x5566

Clientless Hosts    = Disabled

IP Station ID       = Disabled

Revalidation        = Enabled

Revalidation Period = 36000 Seconds

ReTransmit Period   = 3 Seconds

StatusQuery Period  = 300 Seconds

Hold Period         = 180 Seconds

AAA Timeout         = 60 Seconds

Max Retries         = 3

EAPoUDP Logging     = Disabled
```

```
Clientless Host Username = clientless

Clientless Host Password = clientless


Interface Specific EAPoUDP Configurations

----------------------------------------

Interface Ethernet2/1
```

No interface specific configuration

Table 55 describes the significant fields shown in the display.

Table 55 show eou Field Descriptions

Field	Description
EAPoUDP Version	EAPoUDP protocol version.
EAPoUDP Port	EAPoUDP port number.
Clientless Hosts	Clientless hosts are enabled or disabled.
IP Station ID	Specifies whether the IP address is allowed in the AAA station-id field. By default, it is disabled.
Revalidation	Revalidation is enabled or disabled.
Revalidation Period	Specifies whether revalidation of hosts is enabled. By default, it is disabled.
ReTransmit Period	Specifies the EAPoUDP packet retransmission interval. The default is 3 seconds.
StatusQuery Period	Specifies the EAPoUDP status query interval for validated hosts. The default is 300 seconds.
Hold Period	Hold period following a failed authentication.
AAA Timeout	AAA timeout period.
Max Retries	Maximum number of allowable retransmissions.
EAPoUDP Logging	Logging is enabled or disabled.
Clientless Host Username	Username of the clientless host.
Clientless Host Password	Password of the clientless host.

Related Commands

Command	Description
eou	Displays information about EAPoUDP.

show ip admission

To display the network admission control cache entries or the running network admission control configuration, use the **show ip admission** command in privileged EXEC mode.

show ip admission {[**cache**] [**configuration**] [**eapoudp**]}

Syntax Description

cache	Displays the current list of network admission entries.
configuration	Displays the running network admission control configuration.
eapoudp	Displays the Extensible Authentication Protocol over UDP (EAPoUDP) network admission control entries.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This **command was introduced**.

Usage Guidelines

Use this command to display either the IP admission control entries or the running IP admission control configuration. Use **show ip admission cache eapoudp** to list the host IP addresses, the session timeout, and the posture state. If the posture statue is POSTURE ESTAB, the host validation was successful.

Examples

The following output displays all the IP admission control rules that are configured on the router:

```
Router# show ip admission configuration

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name avrule
    eapoudp list not specified auth-cache-time 60 minutes
```

The following output displays the host IP addresses, the session timeout, and the posture states:

```
Router# show ip admission cache eapoudp

Posture Validation Proxy Cache
Total Sessions: 3 Init Sessions: 1
 Client IP 10.0.0.112, timeout 60, posture state POSTURE ESTAB
 Client IP 10.0.0.142, timeout 60, posture state POSTURE INIT
 Client IP 10.0.0.205, timeout 60, posture state POSTURE ESTAB
```

The field descriptions in the display are self-explanatory.

Related Commands

Command	Description
clear ip admission cache	Clears IP admission cache entries from the router.
ip admission name	Creates a Layer 3 network admission control rule.

show ip auth-proxy

To display the authentication proxy entries or the running authentication proxy configuration, use the **show ip auth-proxy** command in privileged EXEC mode.

show ip auth-proxy {**cache** | **configuration**}

Syntax Description

cache	Displays the current list of the authentication proxy entries.
configuration	Displays the running authentication proxy configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **show ip auth-proxy** to display either the authentication proxy entries or the running authentication proxy configuration. Use the **cache** keyword to list the host IP address, the source port number, the timeout value for the authentication proxy, and the state for connections using authentication proxy. If authentication proxy state is HTTP_ESTAB, the user authentication was successful.

Use the **configuration** keyword to display all authentication proxy rules configured on the router.

Examples

The following example shows sample output from the **show ip auth-proxy cache** command after one user authentication using the authentication proxy:

```
Router# show ip auth-proxy cache

Authentication Proxy Cache
    Client IP 192.168.25.215 Port 57882, timeout 1, state HTTP_ESTAB
```

The following example shows how the **show ip auth-proxy configuration** command displays the information about the authentication proxy rule **pxy**. The global idle timeout value is 60 minutes. The idle timeouts value for this named rule is 30 minutes. No host list is specified in the rule, meaning that all connection initiating HTTP traffic at the interface is subject to the authentication proxy rule.

```
Router# show ip auth-proxy configuration

Authentication cache time is 60 minutes
Authentication Proxy Rule Configuration
Auth-proxy name pxy
http list not specified auth-cache-time 30 minutes
```

Related Commands

Command	Description
clear ip auth-proxy cache	Clears authentication proxy entries from the router.
ip auth-proxy	Sets the authentication proxy idle timeout value (the length of time an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity).
ip auth-proxy (interface configuration)	Applies an authentication proxy rule at a firewall interface.
ip auth-proxy name	Creates an authentication proxy rule.

show ip inspect

To display Context-Based Access Control (CBAC) configuration and session information, use the **show ip inspect** command in privileged EXEC mode.

show ip inspect {**name** *inspection-name* | **config** | **interfaces** | **session** [**detail**] | **all**}

Syntax Description

name *inspection-name*	Displays the configured inspection rule with the name *inspection-name*.
config	Displays the complete CBAC inspection configuration.
interfaces	Displays the interface configuration with respect to applied inspection rules and access lists.
session [**detail**]	Displays existing sessions that are currently being tracked and inspected by CBAC. The optional **detail** keyword allows additional details about these sessions to be shown.
all	Displays all CBAC configuration and all existing sessions that are currently being tracked and inspected by CBAC.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(4)T	The output for the **show ip inspect session detail** command was enhanced to support dynamic access control list (ACL) bypass.

Usage Guidelines

Use this command to view the CBAC configuration and session information.

ACL Bypass Functionality

ACL bypass allows a packet to avoid redundant ACL checks by allowing the firewall to permit the packet on the basis of existing inspection sessions instead of dynamic ACLs. Because input and output dynamic ACLs have been eliminated from the firewall configuration, the **show ip inspect session detail** command output no longer shows dynamic ACLs. Instead, the output displays the matching inspection session for each packet that is permitted through the firewall.

Examples

The following example shows sample output for the **show ip inspect name myinspectionrule** command, where the inspection rule "myinspectionrule" is configured. In this example, the output shows the protocols that should be inspected by CBAC and the corresponding idle timeouts for each protocol.

```
Router# show ip inspect name myinspectionrule

Inspection Rule Configuration
 Inspection name myinspectionrule
    tcp timeout 3600
    udp timeout 30
```

```
    ftp timeout 3600
```

The following is sample output for the **show ip inspect config** command. In this example, the output shows CBAC configuration, including global timeouts, thresholds, and inspection rules.

```
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
```

The following is sample output for the **show ip inspect interfaces** command:

```
Interface Configuration
 Interface Ethernet0
  Inbound inspection rule is myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
```

The following is sample output for the **show ip inspect session** command. In this example, the output shows the source and destination addresses and port numbers (separated by colons), and it indicates that the session is an FTP session.

```
Router# show ip inspect session

Established Sessions
 Session 25A3318 (10.0.0.1:20)=>(10.1.0.1:46068) ftp-data SIS_OPEN
 Session 25A6E1C (10.1.0.1:46065)=>(10.0.0.1:21) ftp SIS_OPEN
```

The following is sample output for the **show ip inspect all** command:

```
Router# show ip inspect all

Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name all
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
Interface Configuration
 Interface Ethernet0
  Inbound inspection rule is all
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
  Outgoing inspection rule is not set
```

```
  Inbound access list is not set
  Outgoing access list is not set
 Established Sessions
 Session 25A6E1C (30.0.0.1:46065)=>(40.0.0.1:21) ftp SIS_OPEN
 Session 25A34A0 (40.0.0.1:20)=>(30.0.0.1:46072) ftp-data SIS_OPEN
```

The following is sample output from the **show ip inspect session detail** command, which shows that an outgoing ACL and an inbound ACL (dynamic ACLs) have been created to allow return traffic:

```
Router# show ip inspect session detail

Established Sessions
 Session 80E87274 (192.168.1.116:32956)=>(192.168.101.115:23) tcp SIS_OPEN
   Created 00:00:08, Last heard 00:00:04
   Bytes sent (initiator:responder) [140:298] acl created 2
   Outgoing access-list 102 applied to interface FastEthernet0/0
   Inbound access-list 101 applied to interface FastEthernet0/1
```

The following is sample output from the **show ip inspect session detail** command, which shows related ACL information (such as session identifiers [SID]), but does not show dynamic ACLs, which are no longer created:

```
Router# show ip inspect session detail

Established Sessions
 Session 814063CC (192.168.1.116:32955)=>(192.168.101.115:23) tcp SIS_OPEN
  Created 00:00:10, Last heard 00:00:06
  Bytes sent (initiator:responder) [140:298]
  In  SID 192.168.101.115[23:23]=>192.168.1.117[32955:32955] on ACL 101 (15 matches)
```

Out SID 192.168.101.115[23:23]=>192.168.1.116[32955:32955] on ACL 102

show ip ips

To display Intrusion Prevention System (IPS) information such as configured sessions and signatures, use the **show ip ips** command in privileged EXEC mode.

show ip ips {[**all**] [**configuration**] [**interfaces**] [**name** *name*] [**statistics** [**reset**]] [**sessions** [**details**]] [**signatures** [**details**]]}

Syntax Description

all	Displays all available IPS information.
configuration	Displays additional configuration information, including default values that may not be displayed using the **show running-config** command.
interfaces	Displays the interface configuration.
statistics [**reset**]	Displays information such as the number of packets audited and the number of alarms sent. The optional **reset** keyword resets sample output to reflect the latest statistics.
name *name*	Displays information only for the specified IPS rule.
sessions [**details**]	Displays IPS session-related information. The optional **details** keyword shows detailed session information.
signatures [**details**]	Displays signature information, such as which signatures are disabled and marked for deletion. The optional **details** keyword shows detailed signature information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from **show ip audit** to **show ip ips**. Also, all **show ip ips** commands were combined into a single command.

Usage Guidelines

Use the **show ip ips configuration** EXEC command to display additional configuration information, including default values that may not be displayed using the **show running-config** command.

Examples

Sample Output for the show ip ips configuration Command

The following example displays the output of the **show ip ips configuration** command:

```
Event notification through syslog is enabled
Event notification through Net Director is enabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 25
PostOffice:HostID:5 OrgID:100 Addr:10.2.7.3 Msg dropped:0
HID:1000 OID:100 S:218 A:3 H:14092 HA:7118 DA:0 R:0
    CID:1 IP:172.21.160.20 P:45000 S:ESTAB (Curr Conn)
```

```
Audit Rule Configuration
 Audit name AUDIT.1
    info actions alarm
```

Sample Output for the show ip ips interface Command

The following example displays the output of the **show ip ips interface** command:

```
Interface Configuration
 Interface Ethernet0
  Inbound IPS audit rule is AUDIT.1
    info actions alarm
  Outgoing IPS audit rule is not set
 Interface Ethernet1
  Inbound IPS audit rule is AUDIT.1
    info actions alarm
  Outgoing IPS audit rule is AUDIT.1
    info actions alarm
```

Sample Output for the show ip ips statistics Command

The following displays the output of the **show ip ips statistics** command:

```
Signature audit statistics [process switch:fast switch]
  signature 2000 packets audited: [0:2]
  signature 2001 packets audited: [9:9]
  signature 2004 packets audited: [0:2]
  signature 3151 packets audited: [0:12]
Interfaces configured for audit 2
Session creations since subsystem startup or last reset 11
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [2:1:0]
Last session created 19:18:27
Last statistic reset never

HID:1000 OID:100 S:218 A:3 H:14085 HA:7114 DA:0 R:0
```

Related Commands

Command	Description
clear ip ips statistics	Resets statistics on packets analyzed and alarms sent.

show ip port-map

To display the Port to Application Mapping (PAM) information, use the **show ip port-map** command in privileged EXEC mode.

show ip port-map [*appl-name* | **port** *port-num*]

Syntax Description

appl-name	(Optional) Specifies the name of the application to which to apply the port mapping.
port *port-num*	(Optional) Specifies the alternative port number that maps to the application.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use this command to display the port mapping information at the firewall, including the system-defined and user-defined information. Include the application name to display the list of entries by application. Include the port number to display the entries by port.

Examples

The following is sample output for the **show ip port-map** command, including system-defined mapping information:

```
Router# show ip port-map

Default mapping: vdolive          port 7000               system defined
Default mapping: sunrpc           port 111                system defined
Default mapping: netshow          port 1755               system defined
Default mapping: cuseeme          port 7648               system defined
Default mapping: tftp             port 69                 system defined
Default mapping: real-audio-video port 7070               system defined
Default mapping: streamworks      port 1558               system defined
Default mapping: ftp              port 21                 system defined
Default mapping: h323             port 1720               system defined
Default mapping: smtp             port 25                 system defined
Default mapping: http             port 80                 system defined
Default mapping: msrpc            port 135                system defined
Default mapping: exec             port 512                system defined
Default mapping: login            port 513                system defined
Default mapping: sql-net          port 1521               system defined
Default mapping: tftp             port 70                 user defined
Host specific:   ftp              port 1000   in list 10  user defined
Host specific:   netshow          port 70     in list 10  user defined
Host specific:   smtp             port 70     in list 50  user defined
```

The following example shows the port mapping information for file transfer protocol services:

```
show ip port-map ftp
```

```
Default mapping: ftp             port 21                  system defined
Host specific:   ftp             port 1000   in list 10   user defined
```

The following example shows the ports associated with the NetShow application, including both the default and host-specific port mapping information:

```
show ip port-map netshow
Default mapping: netshow         port 1755                system defined
Host specific:   netshow         port 21     in list 10   user defined
```

The following example shows the applications associated with port 69, including both the default and host-specific port mapping information:

```
show ip port-map port 69
Default mapping: tftp            port 69                  user defined
Host specific:   netshow         port 69     in list 50   user defined
Host specific:   smtp            port 69     in list 10   user defined
```

Related Commands

Command	Description
ip port-map	Establishes PAM.

show ip sdee

To display Security Device Event Exchange (SDEE) notification information, use the **show ip sdee** command in privileged EXEC mode.

show ip sdee {[**alerts**] [**all**] [**errors**] [**events**] [**configuration**] [**status**] [**subscriptions**]}

Syntax Description

alerts	Displays the Intrusion Detection System (IDS) alert buffer.
all	Displays all information available for IDS SDEE notifications.
errors	Displays IDS SDEE error messages.
events	Displays IDS SDEE events.
configuration	Displays SDEE configuration parameters.
status	Displays the status events that are currently in the buffer.
subscriptions	Displays IDS SDEE subscription information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced.

Examples

The following is sample output from the **show ip sdee alerts** command. In this example, the alerts are numbered from 1 to 100 (because 100 events are currently in the event buffer). Following the alert number are 3 digits, which indicate whether the alert has been reported for the 3 possible subscriptions. In this example, these alerts have been reported for subscription number 1. The event ID is composed of the alert time and an increasing count, separated by a colon.

```
Router# show ip sdee alerts

Event storage:1000 events using 656000 bytes of memory
                                SDEE Alerts

SigID       SrcIP     DstIP       SrcPort  DstPort  Sev     Event ID        SigName
1:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211478597901  ICMP Echo Req
2:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211478887902  ICMP Echo Req
3:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211479247903  ICMP Echo Req
4:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211479457904  ICMP Echo Req
5:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211479487905  ICMP Echo Req
6:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211480077906  ICMP Echo Req
7:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211480407907  ICMP Echo Req
.....
.....
96:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750898596  ICMP Echo Req
97:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750898597  ICMP Echo Req
98:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750898598  ICMP Echo Req
99:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750908599  ICMP Echo Req
100:000 2004 10.0.0.2 10.0.0.1    8        0        2       10211750918600  ICMP Echo Req
```

The following is sample output is from the **show ip sdee subscriptions** command. In this example, SDEE is enabled, the maximum event buffer size has been set to 100, and the maximum number of subscriptions that can be open at the same time is 1.

```
Router# show ip sdee subscriptions

SDEE is enabled
Alert buffer size:100 alerts 65600 bytes
Maximum subscriptions:1

SDEE open subscriptions: 1
Subscription ID IDS1720:0:
Client address 10.0.0.2 port 1500
        Subscription opened at 13:21:30 MDT July 18 2003
        Total GET requests:0
        Max number of events:50
        Timeout:30
        Event Start Time:0
        Report alerts:true
        Alert severity level is INFORMATIONAL
        Report errors:false
        Report status:false
```

Table 56 describes the significant fields shown in the display.

Table 56 show ip sdee subscriptions Field Descriptions

Field	Description
Alert buffer size:100 alerts 65600 bytes	Maximum number of events that can be stored in the buffer. The maximum number of events to be stored refers to all types of events (alert, status, and error). (This value can be changed via the **ip sdee events** command.)
Maximum subscriptions:1	Maximum number of subscriptions that can be open at the same time. (This value can be changed via the **ip sdee subscriptions** command.)

The following is sample output from the **show ip sdee status** command. In this example, the buffer is set to store a maximum of 1000 events.

```
Router# show ip sdee status

Event storage:1000 events using 656000 bytes of memory

                   SDEE Status Messages
Time                              Message              Description
1:000 22:10:58 UTC Apr 18 2003  applicationStarted   STRING.UDP,0 ms
2:000 22:10:58 UTC Apr 18 2003  applicationStarted   STRING.TCP,0 ms
3:000 22:10:58 UTC Apr 18 2003  applicationStarted   OTHER,0 ms
4:000 22:10:58 UTC Apr 18 2003  applicationStarted   SERVICE.FTP,276 ms
5:000 22:11:07 UTC Apr 18 2003  applicationStarted   SERVICE.SMTP,8884 ms
6:000 22:11:07 UTC Apr 18 2003  applicationStarted   SERVICE.RPC,72 ms
7:000 22:11:07 UTC Apr 18 2003  applicationStarted   SERVICE.DNS,132 ms
8:000 22:11:15 UTC Apr 18 2003  applicationStarted   SERVICE.HTTP,7632 ms
9:000 22:11:15 UTC Apr 18 2003  applicationStarted   ATOMIC.TCP,24 ms
10:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.UDP,12 ms
11:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.ICMP,12 ms
12:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.IPOPTIONS,8 ms
13:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.L3.IP,8 ms
```

Related Commands

Command	Description
ip ips notify	Specifies the method of event notification.
id sdee events	Sets the maximum number of SDEE events that can be stored in the event buffer.
ip sdee subscriptions	Sets the maximum number of SDEE subscriptions that can be open simultaneously.

show ip source-track

To display traffic flow statistics for tracked IP host addresses, use the **show ip source-track** command in privileged EXEC mode.

show ip source-track [*ip-address*] [**summary** | **cache**]

Syntax Description

ip-address	(Optional) Displays the IP address of the tracked host for which traffic flow information is displayed.
summary	(Optional) Displays a summary of traffic flow information that is collected for a specified host address (via the *ip-address* argument) or for all configured hosts.
cache	(Optional) Displays detailed packet and flow information that is collected on line cards and port adapters for all tracked IP addresses or for specified IP address (not displayed in the a distributed platform such as the gigabit route processor (GRP) or route switch processor (RSP)).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Examples

The following example, which is sample output from the **show ip source-track summary** command, shows how to verify that IP source tracking is enabled for one or more hosts:

```
Router# show ip source-track summary

Address          Bytes    Pkts    Bytes/s   Pkts/s
10.0.0.1          119G   1194M    443535      4432
192.168.1.1       119G   1194M    443535      4432
192.168.42.42     119G   1194M    443535      4432
```

The following example, which is sample output from the **show ip source-track summary** command, shows how to verify that no traffic has yet to be received for the destination hosts that are being tracked:

```
Router# show ip source-track summary

Address        Bytes   Pkts   Bytes/s   Pkts/s
10.0.0.1           0      0         0        0
192.168.1.1        0      0         0        0
192.168.42.42      0      0         0        0
```

The following example, which is sample output from the **show ip source-track** command, shows that IP source tracking is processing packets to the hosts and exporting statistics from the line card or port adapter to the route processor:

```
Router# show ip source-track

Address         SrcIF    Bytes   Pkts   Bytes/s   Pkts/s
10.0.0.1        PO0/0    119G   1194M    513009     5127
192.168.1.1     PO0/0    119G   1194M    513009     5127
192.168.42.42   PO0/0    119G   1194M    513009     5127
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
ip source-track address-limit	Configures the maximum number of destination hosts that can be simultaneously tracked at any given moment.
ip source-track syslog-interval	Sets the time interval (in minutes) in which syslog messages are generated if IP source tracking is enabled on a device.

show ip source-track export flows

To display the last ten packet flows that were exported from the line card to the route processor, use the **show ip source-track export flows** command in privileged EXEC mode.

show ip source-track export flows

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

The **show ip source-track export flows** command can be issued only on distributed platforms such as the GRP and the RSP.

Examples

The following example displays the packet flow information that is exported from line cards and port adapters to the gigabit route processor (GRP) and the route switch processor (RSP):

```
Router# show ip source-track export flows

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
PO0/0         101.1.1.0       Null          100.1.1.1       06 0000 0000    88K
PO0/0         101.1.1.0       Null          100.1.1.3       06 0000 0000    88K
PO0/0         101.1.1.0       Null          100.1.1.2       06 0000 0000    88K
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
ip source-track export-interval	Sets the time interval (in seconds) in which IP source tracking statistics are exported from the line card to the RP.

show ip ssh

To display the version and configuration data for Secure Shell (SSH), use the **show ip ssh** command in privileged EXEC mode.

show ip ssh

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1 T.
12.1(5)T	This command was modified to display the SSH status—enabled or disabled.

Usage Guidelines

Use the **show ip ssh** command to view the status of configured options such as retries and timeouts. This command allows you to see if SSH is enabled or disabled.

Examples

The following is sample output from the **show ip ssh** command when SSH has been enabled:

```
Router# show ip ssh

SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

The following is sample output from the **show ip ssh** command when SSH has been disabled:

```
Router# show ip ssh

%SSH has not been enabled
```

Related Commands

Command	Description
show ssh	Displays the status of SSH server connections.

show ip traffic-export

To display information related to router IP traffic export (RITE), use the **show ip traffic-export** command in privileged EXEC mode.

show ip traffic-export [**interface** *interface-name* | **profile** *profile-name*]

Syntax Description

interface *interface-name*	(Optional) Only data associated with the monitored ingress interface is shown.
profile *profile-name*	(Optional) Only flow statistics, such as exported packets and number of bytes, are shown.

Defaults

If this command is enabled, all data (both interface- and profile-related data) is shown.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Examples

The following sample output from the **show ip traffic-export** command is for the profile "one." This example is for a single configured interface. If multiple interfaces are configured, the information shown below is displayed for each interface.

```
Router# show ip traffic-export

Router IP Traffic Export Parameters
Monitored Interface             FastEthernet0/0
        Export Interface                FastEthernet0/1
        Destination MAC address 0030.7131.abfc
        bi-directional traffic export is off
Input IP Traffic Export Information     Packets/Bytes Exported    0/0
        Packets Dropped           0
        Sampling Rate             one-in-every 1 packets
        No Access List configured
        Profile one is Active
```

Table 57 describes the significant fields shown in the display.

Table 57 show ip traffic-export Field Descriptions

Field	Description
Monitored Interface	Interface in which the profile was applied. (This interface is specified via the **ip traffic-export apply profile** command.)
Export Interface	Interface in which the profile exports all captured IP traffic. (This interface is specified via the **ip traffic-export profile** command.)
Destination MAC address	Ethernet address of the destination host, which is specified via the **mac-address** command.
bi-directional traffic export is	Incoming and outgoing IP traffic is exported on the monitored interface (via the **bidirectional** command). By default, only incoming traffic is exported.
Input IP Traffic Export Information Packets Dropped Sampling Rate No Access List Configured Profile one is Active	Incoming IP traffic information. The sampling rate and ACL can be defined via the **incoming** command. If the profile is incomplete, the profile will be listed as inactive.

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported across a monitored interface.
ip traffic-export apply profile	Applies an IP traffic export profile to a specific interface.
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
incoming	Configures filtering for incoming export traffic.
outgoing	Configures filtering for outgoing export traffic.

show ip trigger-authentication

To display the list of remote hosts for which automated double authentication has been attempted, use the **show ip trigger-authentication** command in privileged EXEC mode.

show ip trigger-authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Whenever a remote user needs to be user-authenticated in the second stage of automated double authentication, the local device sends a User Datagram Protocol (UDP) packet to the remote user's host. When the UDP packet is sent, the user's host IP address is added to a table. If additional UDP packets are sent to the same remote host, a new table entry is not created; instead, the existing entry is updated with a new time stamp. This remote host table contains a cumulative list of host entries; entries are deleted after a timeout period or after you manually clear the table using the **clear ip trigger-authentication** command. You can change the timeout period with the **ip trigger-authentication** (global) command.

Use this command to view the list of remote hosts for which automated double authentication has been attempted.

Examples

The following example shows output from the **show ip trigger-authentication** command:

```
Router# show ip trigger-authentication

Trigger-authentication Host Table:
Remote Host          Time Stamp
209.165.200.230       2940514234
```

This output shows that automated double authentication was attempted for a remote user; the remote user's host has the IP address 209.165.200.230. The attempt to automatically double authenticate occurred when the local host (myfirewall) sent the remote host (209.165.200.230) a packet to UDP port 7500. (The default port was not changed in this example.)

Related Commands

Command	Description
clear ip trigger-authentication	Clears the list of remote hosts for which automated double authentication has been attempted.

show ip urlfilter cache

To display the maximum number of entries that can be cached into the cache table and the number of entries and the destination IP addresses that are cached into the cache table, use the **show ip urlfilter cache** command in EXEC mode.

show ip urlfilter cache

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Examples

The following example is sample output from the **show ip urlfilter cache** command:

```
Router# show ip urlfilter cache

Maximum number of entries allowed: 5000
Number of entries cached: 5
IP addresses cached ....
 10.64.128.54
 172.28.139.21
 10.76.82.25
 192.168.0.1
 10.0.1.2
```

Table 58 describes the significant fields shown in the display.

Table 58 show ip urlfilter cache Field Descriptions

Field	Description
Maximum number of entries allowed	Maximum number of destination IP addresses that can be cached into the cache table. This parameter can be configured using the **ip url filter cache** command. (The default is 5000.)
Number of entries cached	Number of entries that have already been cached into the cache table.
IP addresses cached	IP addresses that have already been cached into the cache table.

Related Commands

Command	Description
clear ip urlfilter cache	Clears the cache table.
ip urlfilter cache	Configures cache parameters.

show ip urlfilter config

To display the size of the cache, the maximum number of outstanding requests, the allow mode state, and the list of configured vendor servers, use the **show ip urlfilter config** command in EXEC mode.

show ip urlfilter config

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Examples

The following example is sample output from the **show ip urlfilter config** command:

```
Router# show ip urlfilter config

URL filter is ENABLED

Primary Websense server configurations
==========================
Websense server IP address: 10.0.0.3
Websense server port: 15868
Websense retransmit time out: 5 (seconds)
Websense number of retransmit:2

Secondary Websense server configurations:
=============================
None.

Other configurations
===============
Allow mode: OFF
System Alert: ON
Log message on the router: OFF
Log message on URL filter server:ON
Maximum number of cache entries :5000
Cache timeout :12 (hours)
Maximum number of packet buffers:200
Maximum outstanding requests:1000
```

Related Commands

Command	Description
ip urlfilter allowmode	Turns on the default mode (allow mode) of the filtering algorithm.
ip urlfilter cache	Configures cache parameters.

Command	Description
ip urlfilter max-request	Sets the maximum number of outstanding requests that can exists at any given time.
ip urlfilter server vendor	Configures a vendor server for URL filtering.

show ip urlfilter statistics

To display URL filtering statistics, use the **show ip urlfilter statistics** command in EXEC mode.

show ip urlfilter statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

This command shows information, such as the number of requests that are sent to the vendor server (Websense or N2H2), the number of responses received from the vendor server, the numberof pending requests in the system, the number of failed requests, and the number of blocked URLs.

Examples

The following example is sample output from the **show ip urlfilter statistics** command:

```
Router# show ip urlfilter statistics

URL filtering statistics
================
Current requests count:25
Current packet buffer count(in use):40
Current cache entry count:3100

Maxever request count:526
Maxever packet buffer count:120
Maxever cache entry count:5000

Total requests sent to URL Filter Server: 44765
Total responses received from URL Filter Server: 44550
Total requests allowed: 44320
Total requests blocked: 224
```

Table 59 describes the significant fields shown in the display.

Table 59 show ip urlfilter statistics Field Descriptions

Field	Description
Current requests count[1]	Number of requests that have been sent to the vendor server.
Current packet buffer count (in use)[2]	Number of HTTP responses that are currently in the packet buffer of the firewall.

Table 59 show ip urlfilter statistics Field Descriptions (continued)

Field	Description
Current cache entry count[3]	Number of destination IP addresses that have been cached into the cache table.
Maxever request count[1]	Maximum number of requests that have been sent to the vendor server since power on.
Maxever packet buffer count[2]	Maximum number of HTTP responses that have been stored in the packet buffer of the firewall since power on.
Maxever cache entry count[3]	Maximum number of destination IP addresses that have been cached into the cache table since power on.

1. This value can be specified via the **ip urlfilter max-request** command.
2. This value can be specified via the **ip urlfilter max-resp-pak** command.
3. This value can be specified via the **ip urlfilter cache** command.

Related Commands

Command	Description
ip urlfilter cache	Configures cache parameters.
ip urlfilter max-request	Sets the maximum number of outstanding requests that can exist at any given time.
ip urlfilter max-resp-pak	Configures the maximum number of HTTP responses that the firewall can keep in its packet buffer.

show ip virtual-reassembly

To display the configuration and statistical information of the virtual fragment reassembly (VFR) on a given interface, use the **show ip virtual-reassembly** command in privileged EXEC mode.

show ip virtual-reassembly [**interface** *type*]

Syntax Description

interface *type*	(Optional) VFR information is shown only for the specified interface. If an interface is not specified, VFR information for all configured interfaces is shown.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example is sample output from the **show ip virtual-reassembly** command:

```
Router# show ip virtual-reassembly interface ethernet1/1

Ethernet1/1:
Virtual Fragment Reassembly (VFR) is ENABLED...
Concurrent reassemblies (max-reassemblies):64
Fragments per reassembly (max-fragments):16
Reassembly timeout (timeout):3 seconds
Drop fragments:OFF

Current reassembly count:12
Current fragment count:48
Total reassembly count:6950
Total reassembly failures:9
```

Table 60 describes the significant fields shown in the display.

Table 60 show ip virtual-reassembly Field Descriptions

Field	Description
Concurrent reassemblies (max-reassemblies):64	Maximum number of IP datagrams that can be reassembled at any given time. Value can be specified via the **max-reassemblies** *number* option from the **ip virtual-reassembly** command.
Fragments per reassembly (max-fragments):16	Maximum number of fragments that are allowed per IP datagram (fragment set). Value can be specified via the **max-fragments** *number* option from the **ip virtual-reassembly** command.
Reassembly timeout (timeout):3 seconds	Timeout value for an IP datagram that is being reassembled. Value can be specified via the **timeout** *seconds* option from the **ip virtual-reassembly** command.
Drop fragments:OFF	Specifies whether the VFR should drop all fragments that arrive on the configured interface. Function can be turned on or off via the **drop-fragments** keyword from the **ip virtual-reassembly** command.
Current reassembly count	Number of IP datagrams that are currently being reassembled
Current fragment count	Number of fragments that have been buffered by VFR for reassembly
Total reassembly count	Total number of datagrams that have been reassembled since the last system reboot.
Total reassembly failures	Total number of reassembly failures since the last system reboot.

Related Commands

Command	Description
ip virtual-reassembly	Enables VFR on an interface.

show kerberos creds

To display the contents of your credentials cache, use the **show kerberos creds** command in privileged EXEC mode.

show kerberos creds

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The **show kerberos creds** command is equivalent to the UNIX klist command.

When users authenticate themselves with Kerberos, they are issued an authentication ticket called a *credential*. The credential is stored in a credential cache.

Examples

The following example displays entries in the credentials cache:

```
Router > show kerberos creds

 Default Principal: user@example.com
 Valid Starting          Expires                 Service Principal
 18-Dec-1995 16:21:07    19-Dec-1995 00:22:24    krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

The following example returns output that acknowledges that credentials do *not* exist in the credentials cache:

```
Router > show kerberos creds

 No Kerberos credentials
```

Related Commands

Command	Description
clear kerberos creds	Deletes the contents of the credentials cache.

show login

To display login parameters, use the **show login** command in privileged EXEC mode.

show login [**failures**]

Syntax Description

failures	(Optional) Displays information related only to failed login attempts.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

The **show login** command allows users to verify the applied login configuration and present login status on your router.

Examples

The following sample output from the **show login** command verifies that no login parameters have been specified:

```
Router# show login

No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps

Router NOT enabled to watch for login Attacks
```

The following sample output from the **show login** command verifies that the **login block-for** command is issued. In this example, the command is configured to block login hosts for 100 seconds if 16 or more login requests fail within 100 seconds; five login requests have already failed.

```
Router# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.

Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.

Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5.
```

The following sample output from the **show login** command verifies that the router is in quiet mode. In this example, the **login block-for** command was configured to block login hosts for 100 seconds if three or more login requests fail within 100 seconds.

```
Router# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.

Router enabled to watch for login Attacks.
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.

Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.
```

Denying logins from all sources.

Table 61 describes the significant fields shown in the proceeding displays.

Table 61 show login Field Descriptions

Field	Description
A default login delay of 1 seconds is applied.	A delay of 1 second is enforced when the **login block-for** command is issued. To specify a different delay value, use the **login delay** command.
No Quiet-Mode access list has been configured.	No access control lists (ACLs) are exempt from the quiet period. To specify an ACL, use the l**ogin quiet-mode access-class** command.
All successful or failed login is logged and generate SNMP traps.	Logging messages and Simple Network Management Protocol (SNMP) traps are configured to be generated upon successful or failed login attempts. To change this setting, use the **login on-success** or l**ogin on-failure** command.
Router enabled to watch for login Attacks.	The Cisco IOS device has been configured with at least the **login block-for** command, which enables default login functionality. **Note** If no login parameters are specified, the following description appears: “Router NOT enabled to watch for login Attacks.”
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for 100 seconds.	Parameters of the **login block-for** *seconds* **attempts** *tries* **within** *seconds* command.

Table 61 show login Field Descriptions (continued)

Field	Description
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.	The router has switched to quiet mode. **Note** If the router is not in quiet mode, the following description appears: "Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds."
Denying logins from all sources.	The router is in quiet mode and no ACLs are defined, so the router is denying all login requests. **Note** If the router is not in quiet mode, the following description, which allows the user to keep track of the current failed login attempts, appears: "Present login failure count 5."

show login failure Sample Outputs

The following sample output from **show login failures** command shows all failed login attempts on the router:

```
Router# show login failures

Information about login failure's with the device

Username      Source IPAddr  lPort Count  TimeStamp
try1          10.1.1.1        23    1     21:52:49 UTC Sun Mar 9 2003
try2          10.1.1.2        23    1     21:52:52 UTC Sun Mar 9 2003
```

The following sample output from **show login failures** command verifies that no information is presently logged:

```
Router# show login failures

*** No logged failed login attempts with the device.***
```

Related Commands

Command	Description
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
login delay	Configures a uniform delay between successive login attempts.
login on-failure	Generates system logging messages for every login attempts.
login on-success	Generates system logging messages for successful login attempts.
login quiet-mode access-class	Specifies an ACL that is to be applied to the router when it switches to quiet mode.

show parser view

To display command-line interface (CLI) view information, use the **show parser view** command in privileged EXEC mode.

show parser view [**all**]

Syntax Description

all	(Optional) Displays information about all CLI views that are configured on the router.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

The **show parser view** command will display information only about the view that the user is currently in. This command is available for both root view users and lawful intercept view users—except for the **all** keyword, which is available only to root view users. However, the **all** keyword can be configured by a user in root view to be available for users in lawful intercept view.

The **show parser view** command cannot be excluded from any view.

Examples

The following example shows how to display information from the root view and the CLI view “first”:

```
Router# enable view
Router#
01:08:16:%PARSER-6-VIEW_SWITCH:successfully set to view 'root'.
Router#
! Enable the show parser view command from the root view
Router# show parser view
Current view is 'root'
! Enable the show parser view command from the root view to display all views
Router# show parser view all
Views Present in System:
View Name:   first
View Name:   second
! Switch to the CLI view “first.”
Router# enable view first
Router#
01:08:09:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
! Enable the show parser view command from the CLI view “first.”
Router# show parser view
Current view is 'first'
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.

show ppp queues

To monitor the number of requests processed by each authentication, authorization, and accounting (AAA) background process, use the **show ppp queues** command in privileged EXEC mode.

show ppp queues

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Usage Guidelines

Use the **show ppp queues** command to display the number of requests handled by each AAA background process, the average amount of time it takes to complete each request, and the requests still pending in the work queue. This information can help you balance the data load between the network access server and the AAA server.

This command displays information about the background processes configured by the **aaa processes** global configuration command. Each line in the display contains information about one of the background processes. If there are AAA requests in the queue when you enter this command, the requests will be printed as well as the background process data.

Examples

The following example shows output from the **show ppp queues** command:

```
Router# show ppp queues

Proc #0   pid=73  authens=59   avg. rtt=118s. authors=160  avg. rtt=94s.
Proc #1   pid=74  authens=52   avg. rtt=119s. authors=127  avg. rtt=115s.
Proc #2   pid=75  authens=69   avg. rtt=130s. authors=80   avg. rtt=122s.
Proc #3   pid=76  authens=44   avg. rtt=114s. authors=55   avg. rtt=106s.
Proc #4   pid=77  authens=70   avg. rtt=141s. authors=76   avg. rtt=118s.
Proc #5   pid=78  authens=64   avg. rtt=131s. authors=97   avg. rtt=113s.
Proc #6   pid=79  authens=56   avg. rtt=121s. authors=57   avg. rtt=117s.
Proc #7   pid=80  authens=43   avg. rtt=126s. authors=54   avg. rtt=105s.
Proc #8   pid=81  authens=139  avg. rtt=141s. authors=120  avg. rtt=122s.
Proc #9   pid=82  authens=63   avg. rtt=128s. authors=199  avg. rtt=80s.
queue len=0 max len=499
```

Table 62 describes the fields shown in the example.

Table 62 show ppp queues Field Descriptions

Field	Description
Proc #	Identifies the background process allocated by the **aaa processes** command to handle AAA requests for PPP. All of the data in this row relates to this process.
pid=	Identification number of the background process.
authens=	Number of authentication requests the process has performed.
avg. rtt=	Average delay (in seconds) until the authentication request was completed.
authors=	Number of authorization requests the process has performed.
avg. rtt=	Average delay (in seconds) until the authorization request was completed.
queue len=	Current queue length.
max len=	Maximum length the queue ever reached.

Related Commands

Command	Description
aaa processes	Allocates a specific number of background processes to be used to process AAA authentication and authorization requests for PPP.

show privilege

To display your current level of privilege, use the **show privilege** command in EXEC mode.

show privilege

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following example shows sample output from the **show privilege** command. The current privilege level is 15.

```
Router# show privilege

Current privilege level is 15
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the **enable password** command.

show radius local-server statistics

To display the statistics for the local authentication server, use the **show radius local-server statistics** command in privileged EXEC mode.

show radius local-server statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following output displays statistics for the local authentication server:

```
Router# show radius local-server statistics

Successes              : 11262       Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 8
Unknown NAS            : 0           Invalid packet from NAS: 0

NAS : 10.0.0.1
Successes              : 11262       Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 8
Corrupted packet       : 0           Unknown RADIUS message : 0
No username attribute  : 0           Missing auth attribute : 0
Shared key mismatch    : 0           Invalid state attribute: 0
Unknown EAP message    : 0           Unknown EAP auth type  : 0

Maximum number of configurable users: 50, current user count: 11
Username                   Successes  Failures  Blocks
vayu-ap-1                       2235         0       0
vayu-ap-2                       2235         0       0
vayu-ap-3                       2246         0       0
vayu-ap-4                       2247         0       0
vayu-ap-5                       2247         0       0
vayu-11                            3         0       0
vayu-12                            5         0       0
vayu-13                            5         0       0
vayu-14                           30         0       0
vayu-15                            3         0       0
scm-test                           1         8       0
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

show radius statistics

To display the RADIUS statistics for accounting and authentication packets, use the **show radius statistics** command in EXEC mode.

show radius statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

The following example is sample output for the **show radius statistics** command:

```
Router# show radius statistics
                                 Auth.       Acct.        Both
          Maximum inQ length:      NA          NA           1
        Maximum waitQ length:      NA          NA           1
        Maximum doneQ length:      NA          NA           1
        Total responses seen:       3           0           3
     Packets with responses:        3           0           3
   Packets without responses:       0           0           0
  Average response delay(ms):    5006           0        5006
  Maximum response delay(ms):   15008           0       15008
   Number of Radius timeouts:       3           0           3
        Duplicate ID detects:       0           0           0
```

Table 63 describes significant fields shown in the display.

Table 63 show radius statistics Field Descriptions

Field	Description
Auth.	Statistics for authentication packets.
Acct.	Statistics for accounting packets.
Both	Combined statistics for authentication and accounting packets.
Maximum inQ length	Maximum number of entries allowed in the queue, that holds the RADIUS messages not yet sent.
Maximum waitQ length	Maximum number of entries allowed in the queue, that holds the RADIUS messages that have been sent and are waiting for a response.
Maximum doneQ length	Maximum number of entries allowed in the queue, that holds the messages that have received a response and will be forwarded to the code that is waiting for the messages.
Total responses seen	Number of RADIUS responses seen from the server. In addition to the expected packets, this includes repeated packets and packets that do not have a matching message in the waitQ.
Packets with responses	Number of packets that received a response from the RADIUS server.
Packets without responses	Number of packets that never received a response from any RADIUS server.
Average response delay	Average time from when the packet was first transmitted to when it received a response. If the response timed out and the packet was sent again, this value includes the timeout. If the packet never received a response, this is not included in the average.
Maximum response delay	Maximum delay observed while gathering average response delay information.
Number of RADIUS timeouts	Number of times a server did not respond, and the RADIUS server re-sent the packet.
Duplicate ID detects	RADIUS has a maximum of 255 unique IDs. In some instances there can be more than 255 outstanding packets. When a packet is received, the doneQ is searched from the oldest entry to the youngest. If the IDs are the same, further techniques are used to see if this response matches this entry. If it is determined that this does not match, the duplicate ID detect counter is increased.

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server retransmit	Specifies how many times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval for which a router waits for a server host to reply.

show secure bootset

To display the status of Cisco IOS image and configuration resilience, use the **show secure bootset** command in privileged EXEC mode.

show secure bootset

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **show secure bootset** command instead of the **dir** command, the Cisco IOS directory listing command, to verify the existence of an image archive. This command will also display output that shows whether the image or configuration archive is ready for upgrade.

Examples

The following is self-explanatory sample output from the **show secure bootset** command:

```
Router# show secure bootset

%IOS image and configuration resilience is not active


Router# show secure bootset

IOS resilience router id JMX0704L5GH

IOS image resilience version 12.3 activated at 08:16:51 UTC Sun Jun 16 2002
Secure archive slot0:c3745-js2-mz type is image (elf) []
  file size is 25469248 bytes, run size is 25634900 bytes
  Runnable image, entry point 0x80008000, run from ram

IOS configuration resilience version 12.3 activated at 08:17:02 UTC Sun Jun 16 2002
Secure archive slot0:.runcfg-20020616-081702.ar type is config
configuration archive size 1059 bytes
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
secure boot-config	Saves a secure copy of the router running configuration in persistent storage.
secure boot-image	Enables Cisco IOS image resilience.

show ssh

To display the status of Secure Shell (SSH) server connections, use the **show ssh** command in privileged EXEC mode.

show ssh

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

Use the **show ssh** command to display the status of the SSH connections on your router. This command does not display any SSH configuration data; use the **show ip ssh** command for SSH configuration information such as timeouts and retries.

Examples

The following is sample output from the **show ssh** command with SSH enabled:

```
Router# show ssh

Connection      Version     Encryption     StateUsername
    0   1.5 3DESSession Startedguest
```

The following is sample output from the **show ssh** command with SSH disabled:

```
Router# show ssh
%No SSH server connections running.
```

Related Commands

Command	Description
show ip ssh	Displays the version and configuration data for SSH.

show tacacs

To display statistics for a TACACS+ server, use the **show tacacs** command in EXEC mode.

show tacacs

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following example is sample output for the **show tacacs** command:

```
Router# show tacacs

Tacacs+ Server             : 172.19.192.80/49
              Socket opens:          3
             Socket closes:          3
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
   Failed Connect Attempts:          0
        Total Packets Sent:          7
        Total Packets Recv:          7
          Expected Replies:          0
  No current connection
```

Table 64 describes the significant fields shown in the display.

Table 64 show tacacs Field Descriptions

Field	Description
Tacacs+ Server	IP address of the TACACS+ server.
Socket opens	Number of successful TCP socket connections to the TACACS+ server.
Socket closes	Number of successfully closed TCP socket attempts.
Socket aborts	Number of premature TCP socket closures to the TACACS+ server; that is, the peer did not wait for a reply from the server after a the peer sent its request.
Socket errors	Any other socket read or write errors, such as incorrect packet format and length.
Failed Connect Attempts	Number of failed TCP socket connections to the TACACS+ server.
Total Packets Sent	Number of packets sent to the TACACS+ server.

Table 64 show tacacs Field Descriptions (continued)

Field	Description
Total Packets Recv	Number of packets received from the TACACS+ server.
Expected replies	Number of outstanding replies from the TACACS+ server.

Related Commands

Command	Description
tacacs-server host	Specifies a TACACS+ host.

show tcp intercept connections

To display TCP incomplete and established connections, use the **show tcp intercept connections** command in EXEC mode.

show tcp intercept connections

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

Use the **show tcp intercept connections** command to display TCP incomplete and established connections.

Examples

The following is sample output from the **show tcp intercept connections** command:

```
Router# show tcp intercept connections

Incomplete:
Client                Server              State    Create   Timeout  Mode
172.19.160.17:58190   10.1.1.30:23        SYNRCVD  00:00:09 00:00:05 I
172.19.160.17:57934   10.1.1.30:23        SYNRCVD  00:00:09 00:00:05 I

Established:
Client                Server              State    Create   Timeout  Mode
171.69.232.23:1045    10.1.1.30:23        ESTAB    00:00:08 23:59:54 I
```

Table 65 describes significant fields shown in the display.

Table 65 show tcp intercept connections Field Descriptions

Field	Description
Incomplete:	Rows of information under “Incomplete” indicate connections that are not yet established.
Client	IP address and port of the client.
Server	IP address and port of the server being protected by TCP intercept.
State	SYNRCVD—establishing with client. SYNSENT—establishing with server. ESTAB—established with both, passing data.
Create	Hours:minutes:seconds since the connection was created.
Timeout	Hours:minutes:seconds until the retransmission timeout.

Table 65 show tcp intercept connections Field Descriptions (continued)

Field	Description
Mode	I—intercept mode. W—watch mode.
Established:	Rows of information under "Established" indicate connections that are established. The fields are the same as those under "Incomplete" except for the Timeout field described below.
Timeout	Hours:minutes:seconds until the connection will timeout, unless the software sees a FIN exchange, in which case this indicates the hours:minutes:seconds until the FIN or RESET timeout.

Related Commands

Command	Description
ip tcp intercept connection-timeout	Changes how long a TCP connection will be managed by the TCP intercept after no activity.
ip tcp intercept finrst-timeout	Changes how long after receipt of a reset or FIN-exchange the software ceases to manage the connection.
ip tcp intercept list	Enables TCP intercept.
show tcp intercept statistics	Displays TCP intercept statistics.

show tcp intercept statistics

To display TCP intercept statistics, use the **show tcp intercept statistics** command in EXEC mode.

show tcp intercept statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

Use the **show tcp intercept statistics** command to display TCP intercept statistics.

Examples

The following is sample output from the **show tcp intercept statistics** command:

```
Router# show tcp intercept statistics

intercepting new connections using access-list 101
2 incomplete, 1 established connections (total 3)
1 minute connection request rate 2 requests/sec
```

Related Commands

Command	Description
ip tcp intercept connection-timeout	Changes how long a TCP connection will be managed by the TCP intercept after no activity.
ip tcp intercept finrst-timeout	Changes how long after receipt of a reset or FIN-exchange the software ceases to manage the connection.
ip tcp intercept list	Enables TCP intercept.
show tcp intercept connections	Displays TCP incomplete and established connections.

show wlccp wds

To display information either about the wireless domain services (WDS) device or about client devices, use the **show wlccp wds** command in privileged EXEC mode.

show wlccp wds [**ap** | **mn**] [**detail**] [**mac-addr** *mac-address*]

Syntax Description

ap	(Optional) Displays access points participating in Cisco Centralized Key Management.
mn	(Optional) Displays cached information about client devices, also called mobile nodes.
detail	(Optional) Displays the lifetime of the client, the service set identifier (SSID), and the virtual VLAN ID.
mac-addr	(Optional) Displays information about a specific client device.
mac-address	Client's MAC address.

Defaults

If you do not enter any options with the **show wlccp wds** command, this command displays the IP address of the WDS device, the MAC address, the priority, and the interface state. If the interface state is backup, the command also displays the IP address of the current WDS device, the MAC address, and the priority.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

To show information about the WDS device, do not enter any keywords with this command.

Examples

The following command entry displays information about the WDS device:

```
Router# show wlccp wds ap
```

The following command entry displays cached information, including details, about the client device with the specified MAC address:

```
Router# show wlccp wds mn detail mac-addr 00-05-C2-00-01-F5
```

The following is sample output from the **show wlccp wds** command:

```
Router# show wlccp wds
```

```
MAC:0001.28e0.a400, IP-ADDR:10.0.0.1       , Priority:255
Interface Vlan1, State:Administratively StandAlone - ACTIVE
AP Count:1    , MN Count:0    , MAX AP Count:50
```

Table 66 describes the significant fields shown in the display.

Table 66 show wlccp wds Command Field Descriptions

Field	Description
MAC	MAC address of the interface on which the WDS is configured.
IP-ADDR	IP address of the interface on which the WDS is configured.
Priority	Priority of the WDS.
Interface	Interface on which the WDS is configured.
State	State of the WDS. The state can be INITIALIZATION, BACKUP, or ACTIVE.
AP Count	Number of access points registered to the WDS.
MN Count	Number of mobile nodes registered to the WDS.
MAX AP Count	Maximum number of access points that can be registered.

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

shutdown (certificate server)

To allow a certificate server to be disabled without removing the configuration, use the **shutdown** command in certificate server configuration mode. To reenable the certificate server, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

no shutdown

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

You should issue the **no shutdown** command only after you have completely configured your certificate server.

The **shutdown** command disables the certificate server. If you prefer to disable simple certificate enrollment protocol (SCEP) but still want the certificate server for manual certificate enrollment, use the **no ip http server** command.

Examples

To ensure that the specified URL is working correctly, configure the **database url** command before you issue the **no shutdown** command on the certificate server for the first time. If the URL is broken, you will see output as follows:

```
Router(config)# crypto pki server mycs
Router(cs-server)# database url ftp://myftpserver
Router(cs-server)# no shutdown
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: yes
Translating "myftpserver"

% Failed to generate CA certificate - 0xFFFFFFFF
% The Certificate Server has been disabled.
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.
database url	Specifies the location where all database entries for the certificate server will be written out.
ip http server	Enables an HTTP server on your network.

snmp-server enable traps ipsec

To enable the router to send IP Security (IPSec) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps ipsec** command in global configuration mode. To disable IPSec SNMP notifications, use the **no** form of this command.

snmp-server enable traps ipsec [**cryptomap** [**add** | **delete** | **attach** | **detach**] | **tunnel** [**start** | **stop**] | **too-many-sas**]

no snmp-server enable traps ipsec [**cryptomap** [**add** | **delete** | **attach** | **detach**] | **tunnel** [**start** | **stop**] | **too-many-sas**]

Syntax Description

cryptomap add	(Optional) Notifications for cipsCryptomapAdded { cipsMIBNotifications 3 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a new cryptomap is added to the specified cryptomap set.
cryptomap delete	(Optional) Notifications for cipsCryptomapDeleted { cipsMIBNotifications 4 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap is removed from the specified cryptomap set.
cryptomap attach	(Optional) Notifications for cipsCryptomapSetAttached { cipsMIBNotifications 5 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap set is attached to an active interface of the managed entity.
cryptomap detach	(Optional) Notifications for cipsCryptomapSetDetached { cipsMIBNotifications 6 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap set is detached from an interface to which it was previously bound.
tunnel start	(Optional) Notifications for cipSecTunnelStart { cipSecMIBNotifications 7 } events are generated, as defined in the CISCO-IPSEC-FLOW-MONITOR-MIB. These notifications are generated when an IPsec Phase-2 Tunnel becomes active.
tunnel stop	(Optional) Notifications for cipSecTunnelStop { cipSecMIBNotifications 8 } events are generated, as defined in the CISCO-IPSEC-FLOW-MONITOR-MIB. These notifications are generated when an IPsec Phase-2 Tunnel becomes inactive.
too-many-sas	(Optional) Notifications for cipsTooManySAs { cipsMIBNotifications 7 } events are generated, as defined in the CISCO-IPSEC-MIB.my. These notifications are generated when an attempt to make a new security association (SA) is made but there is insufficient memory on the device.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T, 12.1(11b)E	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

A cryptomap is a table that maps an IPSec Phase-2 tunnel to the corresponding IPSec Policy element.

For a complete description of the notification types and additional MIB functions, refer to the CISCO-IP-SEC.my and CISCO-IPSEC-FLOW-MONITOR-MIB.my files, available on Cisco.com through:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

The **snmp-server enable traps ipsec** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send IPSec MIB inform notifications to the host nms.cisco.com using the community string named “public”:

```
snmp-server enable traps ipsec
snmp-server host nms.cisco.com informs public ipsec
```

Related Commands

Command	Description
snmp-server enable traps isakmps	Controls the sending of (ISAKMP) SNMP notifications
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps isakmp

To enable the router to send IP Security (IPSec) Internet Security Association and Key Exchange Protocol (ISAKMP) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps isakmp** command in global configuration mode. To disable ISAKMP IPSec SNMP notifications, use the **no** form of this command.

snmp-server enable traps isakmp [**policy** {**add** | **delete**} | **tunnel** {**start** | **stop**}]

no snmp-server enable traps isakmp [**policy** {**add** | **delete**} | **tunnel** {**start** | **stop**}]

Syntax Description

policy add	(Optional) Notifcations for cipsIsakmpPolicyAdded { cipsMIBNotifications 1 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a new ISAKMP policy element is defined on the managed entity. The context of the event includes the updated number of ISAKMP policy elements currently available.
policy delete	(Optional) Notifcations for cipsIsakmpPolicyDeleted { cipsMIBNotifications 2 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when an existing ISAKMP policy element is deleted on the managed entity. The context of the event includes the updated number of ISAKMP policy elements currently available.
tunnel start	(Optional) Notifications for cikeTunnelStart { cipSecMIBNotifications 1 } events are generated, as defined by in the CISCO-IPSEC-FLOW-MONITOR-MIB.my. These notifications are generated when an IPsec Phase-1 IKE Tunnel becomes active.
tunnel stop	(Optional) Notifications for cikeTunnelStop { cipSecMIBNotifications 2 } events are generated, as defined by in the CISCO-IPSEC-FLOW-MONITOR-MIB.my. These notifications are generated when an IPsec Phase-1 IKE Tunnel becomes inactive.

Defaults

SNMP notifications are disabled by default.

If no keywords are specified, all available ISAKMP traps are enabled (or disabled if the **no** form is used).

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T, 12.1(11b)E	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both ISAKMP trap and inform requests.

For a complete description of these notifications and additional MIB functions, refer to the CISCO-IPSEC-MIB.myand CISCO-IPSEC-FLOW-MONITOR-MIB.my files, available on Cisco.com through:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

The **snmp-server enable traps isakmp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send IPSec MIB inform notifications to the host nms.cisco.com using the community string named "public":

```
snmp-server enable traps isakmp
snmp-server host nms.cisco.com informs public ipsec
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

source interface

To specify the address of an interface to be used as the source address for all outgoing TCP connections associated with a trustpoint, use the **source interface** command in ca-trustpoint configuration mode. To disable the interface that was specified, use the **no** form of this command.

source interface *interface-name*

no source interface *interface-name*

Syntax Description

interface-name	Interface address to be used as the source address for all outgoing TCP connections associated with a trustpoint.

Defaults

If this command is not specified, the address of the outgoing interface is used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command must be used following the **crypto ca trustpoint** command. If this command is used and the address of the outgoing interface is specified, the router uses the specified address (or address of the specified interface) as the source address for any datagrams that are sent to the certification authority (CA) server or Lightweight Directory Access Protocol (LDAP) server during authentication, enrollment, and if appropriate, when obtaining certificate revocation lists (CRLs).

Examples

In the following example, the router is located in a branch office. The router uses IP Security (IPSec) to communicate with the main office. Ethernet 1 is the "outside" interface that connects to the Internet Service Provider (ISP). Ethernet 0 is the interface connected to the LAN of the branch office. To access the CA server located in the main office the router needs to send its IP datagrams out interface Ethernet 1 (address 10.2.2.205) using the IPSec tunnel. Address 10.2.2.205 is assigned by the ISP. Address 10.2.2.205 is not a part of the branch office or main office.

The CA cannot access any address outside the company because of a firewall. The CA sees a message coming from 10.2.2.205 and cannot respond (that is, it does not know that the router is located in a branch office at address 10.1.1.1, which it is able to reach).

Adding the **source interface** command tells the router to use address 10.1.1.1 as the source address of the IP datagram that it sends to the CA. The CA is able to respond to 10.1.1.1.

This scenario is configured using the **source interface** command and the interface addresses as described above.

```
crypto ca trustpoint ms-ca
 enrollment url http://yourname:80/certsrv/mscep/mscep.dll
 source interface ethernet0
```

```
!
interface ethernet 0
 description inside interface
 ip address 10.1.1.1 255.255.255.0
!
interface ethernet 1
 description outside interface
 ip address 10.2.2.205 255.255.255.0
 crypto map main-office
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

split-dns

To specify a domain name that must be tunneled or resolved to the private network, use the **split-dns** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove a domain name, use the **no** form of this command.

split-dns *domain-name*

no split-dns *domain-name*

Syntax Description

domain-name	Name of the Domain Name System (DNS) domain that must be tunneled or resolved to the private network.

Defaults

All domain names are resolved via the public DNS server.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

If you configure the **split-dns** command, the split-dns attribute will be added to the policy group. The attribute will include the list of domain names that you configured. All other names will be resolved via the public DNS server.

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that needs to be defined or changed, before enabling the **split-dns** command.

Note If you have to configure more than one domain name, you have to add a **split-dns** command line for each.

Examples

The following example shows that the domain names “green.com” and “acme.org” will be added to the policy group:

```
Router (config)# crypto isakmp client configuration group cisco
Router (config-isakmp-group)# key cisco
Router (config-isakmp-group)# dns 10.2.2.2 10.2.2.3
Router (config-isakmp-group)# wins 10.6.6.6
Router (config-isakmp-group)# domain cisco.com
Router (config-isakmp-group)# pool green
Router (config-isakmp-group)# acl 199
Router (config-isakmp-group)# split-dns green.com
Router (config-isakmp-group)# split-dns acme.org
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies group policy information that needs to be defined or changed.

ssh

To start an encrypted session with a remote networking device, use the **ssh** command in privileged EXEC or user EXEC mode.

ssh [**-v** {**1** | **2**}] [**-c** {**3des | aes128-cbc | aes192-cbc | aes256-cbc**}] [**-l** *userid* | **-l** *userid***:***{number} {ip-address}* | **-l** *userid***:rotary***{number} {ip-address}*] [**-m** {**hmac-md5 | hmac-md5-96 | hmac-sha1 | hmac-sha1-96**}] [**-o numberofpasswordprompts** *n*] [**-p** *port-num*] {*ip-addr* | *hostname*} [*command*]

Syntax Description

-v	(Optional) Specifies the version of Secure Shell (SSH) to use to connect to the server. • **1**—Connects using SSH Version 1. • ***2***—Connects using SSH Version 2.
-c {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc**}	(Optional) Specifies the crypto algorithms Data Encryption Standard (DES), Triple DES (3DES), or Advanced Encryption Standard (AES) to use for encrypting data. AES algorithms supported are aes128-cbc, aes192-cbc, and aes256-cbc. • To use SSH Version 1, you must have an encryption image running on the router. Cisco software images that include encryption have the designators “k8” (DES) or “k9” (3DES). • SSH Version 2 supports only the following crypto algorithms: aes128-cbc, aes192-cbc, aes256-cbc, and 3des-cbc. SSH Version 2 is supported only in 3DES images. • If you do not specify the **-c** keyword, during negotiation the remote networking device sends all the supported crypto algorithms. • If you configure the **-c** keyword and the server does not support the argument that you have shown (des, 3des, aes128-cbc, aes192-cbc, or aes256-cbc), the remote networking device closes the connection.
-l *userid*	(Optional) Specifies the user ID to use when logging in on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID.
-l *userid***:{***number} {ip-address}*	(Optional) Specifies the user ID when configuring reverse SSH by including port information in the *userid* field. • **:—Signifies that a port number and terminal IP address will follow the user ID.** • *number*—Terminal or auxiliary line number. • *ip-address*—IP address of the terminal server. **Note** The *userid argument and* **:{***number} {ip-address*} delimiter and arguments must be used if you are configuring reverse SSH by including port information in the *userid* field (a method that is easier than the longer method of listing each terminal or auxiliary line on a separate command configuration line).

-l *userid***:rotary{***number}* *{ip-address}*	(Optional) Specifies that the terminal lines are to be grouped under the rotary group for reverse SSH. • **:**—Signifies that a rotary group number and terminal IP address will follow. • *number*—Terminal or auxiliary line number. • *ip-address*—IP address of the terminal server. **Note** The *userid argument and* **:rotary{***number} {ip-address*} delimiter and arguments must be used if you are configuring reverse SSH by including rotary information in the *userid* field (a process that is easier than the longer process of listing each terminal or auxiliary line on a separate command configuration line).
-m {**hmac-md5 | hmac-md5-96 | hmac-sha1 | hmac-sha1-96}**	(Optional) Specifies a Hashed Message Authentication Code (HMAC) algorithm. • SSH Version 1 does not support HMACs. • If you do not specify the **-m** keyword, the remote device sends all the supported HMAC algorithms during negotiation. If you specify the **-m** keyword and the server does not support the argument that you have shown (hmac-md5, hmac-md5-96, hmac-sha1, and hmac-sha1-96), the remote device closes the connection.
-o numberofpasswordprompts *n*	(Optional) Specifies the number of password prompts that the software generates before ending the session. The SSH server may also apply a limit to the number of attempts. If the limit set by the server is less than the value specified by the **-o numberofpasswordprompts** keyword, the limit set by the server takes precedence. The default is 3 attempts, which is also the Cisco IOS SSH server default. The range of values is from 1 to 5.
-p *port-num*	(Optional) Indicates the desired port number for the remote host. The default port number is 22.
ip-addr | *hostname*	Specifies the IPv4 or IPv6 address or host name of the remote networking device.
command	(Optional) Specifies the Cisco IOS command that you want to run on the remote networking device. If the remote host is not running Cisco IOS software, this may be any command recognized by the remote host. If the command includes spaces, you must enclose the command in quotation marks.

Defaults

Disabled

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(8)T	Support for IPv6 addresses was added.
12.0(21)ST	IPv6 address support was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	IPv6 address support was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	IPv6 address support was integrated into Cisco IOS Release 12.2(14)S.
12.3(7)T	This command was expanded to include Secure Shell Version 2 support. The **-c** keyword was expanded to include support for the following cryptic algorithms: aes128-cbc, aes192-cbc, and aes256-cbc. The **-m** keyword was added, with the following algorithms: hmac-md5, hmac-md5-96, hmac-sha1, and hmac-sha1-96. The **-v** keyword and arguments **1** and **2** were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The **-l** *userid***:***{number} {ip-address} and* **-l** *userid***:rotary***{number} {ip-address} keyword and argument options were added.*

Usage Guidelines

The **ssh** command enables a Cisco router to make a secure, encrypted connection to another Cisco router or device running an SSH Version 1 or Version 2 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

Note

- SSH 1 is supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
- SSH Version 2 supports only the following crypto algorithms: aes128-cbc, aes192-cbc, and aes256-cbc. SSH Version 2 is supported only in 3DES images.
- SSH Version 1 does not support HMAC algorithms.

Examples

The following example illustrates the initiation of a secure session between the local router and the remote host HQhost to run the **show users** command. The result of the **show users** command is a list of valid users who are logged in to HQhost. The remote host will prompt for the adminHQ password to authenticate the user adminHQ. If the authentication step is successful, the remote host will return the result of the **show users** command to the local router and will then close the session.

```
ssh -l adminHQ HQhost "show users"
```

The following example illustrates the initiation of a secure session between the local router and the edge router HQedge to run the **show ip route** command. In this example, the edge router prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the edge router will return the result of the **show ip route** command to the local router.

```
ssh -l adminHQ HQedge "show ip route"
```

The following example shows the SSH client using 3DES to initiate a secure remote command connection with the HQedge router. The SSH server running on HQedge authenticates the session for the admin7 user on the HQedge router using standard authentication methods. The HQedge router must have SSH enabled for authentication to work.

```
ssh -l admin7 -c 3des -o numberofpasswordprompts 5 HQedge
```

The following example shows a secure session between the local router and a remote IPv6 router with the address 3ffe:1111:2222:1044::72 to run the **show running-config** command. In this example, the remote IPv6 router prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the remote IPv6 router will return the result of the **show running-config** command to the local router and will then close the session.

```
ssh -l adminHQ 3ffe:1111:2222:1044::72 "show running-config"
```

Note A hostname that maps to the IPv6 address 3ffe:1111:2222:1044::72 could have been used in the last example.

The following example shows a SSH Version 2 session using the crypto algorithm aes256-cbc and an HMAC of hmac-sha1-96. The user ID is user2, and the IP address is 10.76.82.24.

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-96 -1 user2 10.76.82.24
```

The following example shows that reverse SSH has been configured on the SSH client:

```
ssh -l lab:1 router.example.com
```

The following command shows that Reverse SSH will connect to the first free line in the rotary group:

```
ssh -l lab:rotary1 router.example.com
```

Related Commands

Command	Description
ip ssh	Configures SSH server control parameters on the router.
show ip ssh	Displays the version and configuration data for SSH.
show ssh	Displays the status of SSH server connections.

ssid

To enter up to 20 service set identifiers (SSIDs) to a user group, use the **ssid** command in local RADIUS server group configuration mode. To instruct the access point (AP) not to check if the client has come in on a list of specified SSIDs, use the **no** form of this command.

ssid *ssid-number*

no ssid *ssid-number*

Syntax Description

ssid-number	SSID number of user group members.

Defaults

No default behavior or values

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

You can enter up to 20 SSIDs to limit users to those SSIDs.

Examples

The following example shows that the SSID “green” has been added to the local user group:

```
ssid green
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.

Command	Description
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

subject-name

To specify the subject name in the certificate request, use the **subject-name** command in ca-trustpoint configuration mode. To clear any subject name from the configuration, use the **no** form of this command.

subject-name [*x.500-name*]

no subject-name [*x.500-name*]

Syntax Description

x.500-name	(Optional) Specifies the subject name used in the certificate request.

Defaults

If the *x-500-name* argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Before you can issue the **subject-name** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

The **subject-name** command is an attribute that can be set for autoenrollment; thus, issuing this command prevents you from being prompted for a subject name during enrollment.

Examples

The following example shows how to specify the subject name for the “frog” certificate:

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 auto-enroll regenerate
 password revokme
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

tacacs-server directed-request

To send only a username to a specified server when a direct request is issued, use the **tacacs-server directed-request** command in global configuration mode. To send the entire string to the TACACS+ server, use the **no** form of this command.

tacacs-server directed-request [**restricted**] [**no-truncate**]

no tacacs-server directed-request

Syntax Description

restricted	(Optional) Restrict queries to directed request servers only.
no-truncate	(Optional) Do not truncate the @hostname from the username.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with the directed-request feature enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Disabling **tacacs-server directed-request** causes the whole string, both before and after the "@" symbol, to be sent to the default TACACS+ server. When the directed-request feature is disabled, the router queries the list of servers, starting with the first one in the list, sending the whole string, and accepting the first response that it gets from the server. The **tacacs-server directed-request** command is useful for sites that have developed their own TACACS+ server software that parses the whole string and makes decisions based on it.

With **tacacs-server directed-request** enabled, only configured TACACS+ servers can be specified by the user after the "@" symbol. If the host name specified by the user does not match the IP address of a TACACS+ server configured by the administrator, the user input is rejected.

Use **no tacacs-server directed-request** to disable the ability of the user to choose between configured TACACS+ servers and to cause the entire string to be passed to the default server.

Examples

The following example enables **tacacs-server directed-request** so that the entire user input is passed to the default TACACS+ server:

```
no tacacs-server directed-request
```

tacacs-server host

To specify a TACACS+ host, use the **tacacs-server host** command in global configuration mode. To delete the specified name or address, use the **no** form of this command.

tacacs-server host *host-name* [**port** *integer*] [**timeout** *integer*] [**key** *string*] [**single-connection**] [**nat**]

no tacacs-server host *host-name*

Syntax Description

host-name	Name or IP address of the host.
port	(Optional) Specifies a server port number. This option overrides the default, which is port 49.
integer	(Optional) Port number of the server. Valid port numbers range from 1 to 65535.
timeout	(Optional) Specifies a timeout value. This overrides the global timeout value set with the **tacacs-server timeout** command for this server only.
integer	(Optional) Integer value, in seconds, of the timeout interval.
key	(Optional) Specifies an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command **tacacs-server key** for this server only.
string	(Optional) Character string specifying authentication and encryption key.
single-connection	(Optional) Maintains a single open connection between the router and the TACACS+ server.
nat	(Optional) Port Network Address Translation (NAT) address of the client is sent to the TACACS+ server.

Defaults

No TACACS+ host is specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(11), 12.2(6)	The **nat** keyword was added.
12.2(8)T	The **nat** keyword was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

You can use multiple **tacacs-server host** commands to specify additional hosts. The Cisco IOS software searches for hosts in the order in which you specify them. Use the **port**, **timeout**, **key, single-connection, and nat** keywords only when running a AAA/TACACS+ server.

Because some of the parameters of the **tacacs-server host** command override global settings made by the **tacacs-server timeout** and **tacacs-server key** commands, you can use this command to enhance security on your network by uniquely configuring individual routers.

The **single-connection** keyword specifies a single connection (only valid with CiscoSecure Release 1.0.1 or later). Rather than have the router open and close a TCP connection to the server each time it must communicate, the single-connection option maintains a single open connection between the router and the server. The single connection is more efficient because it allows the server to handle a higher number of TACACS operations.

Examples

The following example specifies a TACACS+ host named Sea_Change:

```
tacacs-server host Sea_Change
```

The following example specifies that, for authentication, authorization, and accounting (AAA) confirmation, the router consults the TACACS+ server host named Sea_Cure on port number 51. The timeout value for requests on this connection is three seconds; the encryption key is a_secret.

```
tacacs-server host Sea_Cure port 51 timeout 3 key a_secret
```

Related Commands

Command	Description
aaa authentication	Specifies or enables AAA authentication.
aaa authorization	Sets parameters that restrict user access to a network.
aaa accounting	Enables AAA accounting of requested services for billing or security.
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host using SLIP.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon, use the **tacacs-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

tacacs-server key *key*

no tacacs-server key [*key*]

Syntax Description

key	Key used to set authentication and encryption. This key must match the key used on the TACACS+ daemon.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) with the **aaa new-model** command, you must set the authentication and encryption key using the **tacacs-server key** command.

The key entered must match the key used on the TACACS+ daemon. All leading spaces are ignored; spaces within and at the end of the key are not. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Examples

The following example sets the authentication and encryption key to “dare to go”:

```
tacacs-server key dare to go
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
tacacs-server host	Specifies a TACACS+ host.

template (identity profile)

To specify a virtual template from which commands may be cloned, use the **template** command in identity profile configuration mode. To disable the virtual template, use the **no** form of this command.

template *virtual-template*

no template *virtual-template*

Syntax Description

virtual-template	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.

Defaults

A virtual template from which commands may be cloned is not specified.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The **identity profile command and default** keyword must be entered in global configuration mode before the **template** command can be used.

Examples

The following example shows that a default identity profile and a template have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# template virtualtemplate1
```

Related Commands

Command	Description
description	Enters an identity profile description.
device	Statically authorizes or rejects individual devices.
identity profile	Creates an identity profile.

template (identity policy)

To specify a virtual template from which commands may be cloned, use the **template** command in identity policy configuration mode. To disable the virtual template, use the **no** form of this command.

template {virtual-template *template-number}*

no template {virtual-template *template-number}*

Syntax Description

virtual-template	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.
template-number	Template interface number. The value ranges from 1 through 200.

Defaults

A virtual template from which commands may be cloned is not specified.

Command Modes

Identity policy configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **identity policy** command must be entered in global configuration mode before the **template** command can be used.

Examples

The following example shows that an identity policy and a template have been specified:

```
Router (config)# identity policy mypolicy
Router (config-identity-policy)# template virtual-template 1
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

template config

To specify a remote URL for a Cisco IOS command-line interface (CLI) configuration template, use the **template config** command in tti-registrar configuration mode. To remove the template from the configuration and use the default template, use the **no** form of this command.

template config *url*

no template config *url*

Syntax Description

url	One of the keywords in Table 67.

Defaults

A default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **template config** command to specify a URL in which to retrieve the template that will be sent from the Easy Secure Device Deployment (EzSDD) registrar to the EzSDD petitioner during the Trusted Transitive Introduction (TTI) exchange.

The default template, which is used if a template is not specified, contains the following commands:

```
!
$t
!
$c
!
end
```

The variable "$t" will be expanded to include a Cisco IOS public key infrastructure (PKI) trustpoint that is configured for autoenrollment with the certificate server of the registrar. The variable "$c" will be expanded into the correct certificate chain for the certificate server of the registrar.

If an external template is specified, it must include the "$t" and "$c" variables to enable the petitioner device to obtain a certificate. The **end** command must be specified. If you want to specify details about the trustpoint, you can specify a template as follows:

```
!
crypto ca trustpoint $1
 enrollment url http://<registrar fqdn>
 rsakeypair $k $s
 auto-enroll 70
!
$c
end
```

Where $l comes from “trustpoint” configured under the petitioner, $k comes from “rsakeypair” under the trustpoint:

```
! $l will be replaced by 'mytp.'
crypto wui tti petitioner
  trustpoint mytp
! $k will be replaced by 'mykey.'
crypto ca trustpoint mytp
rsakeypair mykey
!
```

Note The template configuration location may include a variable “$n,” which is expanded to the name of the introducer.

Table 67 lists the available options for the *url* argument.

Table 67 Options for the url Argument

Keyword	Description
cns:	Retrieves from the Cisco Networking Services (CNS) configuration engine.
flash:	Retrieves from flash memory.
ftp:	Retrieves from the FTP network server.
http:	Retrieves from a HTTP server (also called a web server).
https:	Retrieves from a Secure HTTP (HTTPS) server.
null:	Retrieves from the file system.
nvram:	Retrieves from the NVRAM of the router.
rcp:	Retrieves from a remote copy (rcp) protocol network server.
scp:	Retrieves from a network server that supports Secure Shell (SSH).
system:	Retrieves from system memory, which includes the running configuration.
tftp:	Retrieves from a TFTP network server.
webflash:	Retrieves from the file system.
xmodem:	Retrieves from a network machine that uses the Xmodem protocol.

Examples

The following example shows how to specify the HTTP URL “http://pki1-36a.cisco.com:80” for the Cisco IOS CLI configuration template, which is sent from the EzSDD registrar to the EzSDD petitioner during the TTI exchange:

```
crypto wui tti registrar
 pki-server cs1
 template config http://pki1-36a.cisco.com:80
```

Related Commands

Command	Description
authentication list (tti-registrar)	Authenticates the introducer in an EzSDD operation.
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner in an EzSDD operation.
crypto wui tti registrar	Configures a device to become an EzSDD registrar and enters tti-registrar configuration mode.
debug crypto wui	Displays information about an EzSDD operation.
template username	Establishes a template username and password to access the configuration template on the file system.

template username

To establish a template username in which to access the file system, use the **template username** command in tti-registrar configuration mode.

template username *name*

Syntax Description

name	Template username.

Defaults

A template username is not established.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **template username** command to create a username-based authentication system that allows you to access the configuration template, which is sent from the easy secure device deployment (EzSDD) registrar to the EzSDD petitioner during the Trusted Transitive Introduction (TTI) exchange.

Examples

The following example shows how to create the username “mycs” to access the configuration template for the TTI exchange:

```
crypto wui tti registrar
 pki-server cs1
 template username mycs
```

Related Commands

Command	Description
crypto wui tti registrar	Configures a device to become an EzSDD registrar and enters tti-registrar configuration mode.
template config	Specifies a remote URL for a Cisco IOS CLI configuration template.

test aaa group

To associate a dialed number identification service (DNIS) or calling line identification (CLID) user profile with the record that is sent to the RADIUS server, use the **test aaa group** command in privileged EXEC mode.

test aaa group {*group-name* | **radius**} *username password* **new-code** [**profile** *profile-name*]

Syntax Description

group-name	Subset of RADIUS servers that are used as defined by the server group *group-name*.
radius	Uses RADIUS servers for authentication.
username	Specifies a name for the user.
password	Character string that specifies the password.
new-code	The code path through the new code, which supports a CLID or DNIS user profile association with a RADIUS server.
profile *profile-name*	(Optional) Identifies the user profile specified in the **aaa user profile** command. To associate a user profile with the RADIUS server, the user profile name must be identified.

Defaults

If this command is not enabled, DNIS or CLID attribute values will not be sent to the RADIUS server.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use the **test aaa group** command to associate a DNIS or CLID named user profile with the record that is sent to the RADIUS server, which can then access DNIS or CLID information when the server receives a RADIUS record.

Note The **test aaa group** command does not work with TACACS+.

Examples

The following example shows how to configure a dnis = dnisvalue user profile named “prfl1” and associate it with a **test aaa group** command:

```
aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
  aaa attribute clid clidvalue
  no aaa attribute clid
```

```
  exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile prfl1
```

Related Commands

Command	Description
aaa attribute	Adds DNIS or CLID attribute values to a user profile.
aaa user profile	Creates an AAA user profile.

timeout login response

To specify how long the system will wait for login input (such as username and password) before timing out, use the **timeout login response** command in line configuration mode. To set the timeout value to 30 seconds (which is the default timeout value), use the **no** form of this command.

timeout login response *seconds*

no timeout login response *seconds*

Syntax Description

seconds	Integer that determines the number of seconds the system will wait for login input before timing out. Available settings are from 1 to 300 seconds. The default value is 30 seconds.

Defaults

The default login timeout value is 30 seconds.

Command Modes

Line configuration

Command History

Release	Modification
11.3	This command was introduced.

Examples

The following example changes the login timeout value to 60 seconds:

```
line 10
 timeout login response 60
```

trustpoint (tti-petitioner)

To specify the trustpoint that is to be associated with the Trusted Transitive Introduction (TTI) exchange between the easy secure device deployment (EzSDD) petitioner and the EzSDD registrar, use the **trustpoint** command in tti-petitioner configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

trustpoint *trustpoint-label*

no trustpoint *trustpoint-label*

Syntax Description

trustpoint-label	Name of trustpoint.

Defaults

If a trustpoint is not specified, a default trustpoint called “tti” is generated.

Command Modes

tti-petitioner configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **trustpoint** command in tti-petitioner configuration mode to associate a trustpoint with the EzSDD petitioner.

Examples

The following example shows how specify the trustpoint “mytrust”:

```
crypto wui tti petitioner
 trustpoint mytrust
```

After the EzSDD exchange is complete, the petitioner will automatically enroll with the registrar and obtain a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration which generates the default trustpoint “tti”:

```
crypto pki trustpoint tti
 enrollment url http://pki1-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
crypto wui tti petitioner	Configures a device to become an EzSDD petitioner and enters tti-petitioner configuration mode.

usage

To specify the intended use for the certificate, use the **usage** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

usage *method1* [*method2* [*method3*]]

no usage *method1* [*method2* [*method3*]]

Syntax Description

method1 [*method2* [*method3*]]	Intended use for the certificate; the available options are **ike**, **ssl-client**, and **ssl-server**. You must choose at least one method, and you may choose all three methods.

Defaults

ike

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Before you can issue the **usage** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

This command may be used as a hint to set or clear key usage or other attributes in the certificate request.

Examples

The following example shows how to specify the certificate named “frog” for Internet Key Exchange (IKE):

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 usage ike
 auto-enroll regenerate
 password revokeme
 rsa-key frog 2048
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

user

To enter the names of users that are allowed to authenticate using the local authentication server, use the **user** command in local RADIUS server configuration mode. To remove the username and password from the local RADIUS server, use the **no** form of this command.

user *username* {**password** | **nthash**} *password* [**group** *group-name*]

no user *username* {**password** | **nthash**} *password* [**group** *group-name*]

Syntax Description

username	Name of the user that is allowed to authenticate using the local authentication server.
password	Indicates that the user password will be entered.
nthash	Indicates that the NT value of the password will be entered.
password	User password.
group *group-name*	(Optional) Name of group to which the user will be added.

Defaults

If no group name is entered, the user is not assigned to a VLAN and is never required to reauthenticate.

Command Modes

Local RADIUS server configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

If you do not know the user password, look up the NT value of the password in the authentication server database, and enter the NT hash as a hexadecimal string.

Examples

The following example shows that user “user1” has been allowed to authenticate using the local authentication server (using the password “userisok”). The user will be added to the group “team1”:

```
user user1 password userisok group team1
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
vlan	Specifies a VLAN to be used by members of a user group.

username

To establish a username-based authentication system, use the **username** command in global configuration mode.

username *name* {**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}

username *name* **password** *secret*

username *name* [**access-class** *number*]

username *name* [**autocommand** *command*]

username *name* [**callback-dialstring** *telephone-number*]

username *name* [**callback-rotary** *rotary-group-number*]

username *name* [**callback-line** [**tty**] *line-number* [*ending-line-number*]]

username *name* **dnis**

username *name* [**nocallback-verify**]

username *name* [**noescape**] [**nohangup**]

username *name* [**privilege** *level*]

username *name* **user-maxlinks** *number*

username [**lawful-intercept**] *name* [**privilege** *privilege-level* | **view** *view-name*] **password** *password*

Syntax Description

name	Host name, server name, user ID, or command name. The name argument can be only one word. Blank spaces and quotation marks are not allowed.
nopassword	No password is required for this user to log in. This is usually most useful in combination with the **autocommand** keyword.
password	Specifies a possibly encrypted password for this username.
password	Password a user enters.
encryption-type	Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Currently defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm.
encrypted-password	Encrypted password a user enters.
password	Password to access the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.

secret	For CHAP authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. The secret can consist of any string of up to 11 ASCII characters. There is no limit to the number of username and password combinations that can be specified, allowing any number of remote devices to be authenticated.
access-class	(Optional) Specifies an outgoing access list that overrides the access list specified in the **access-class** line configuration command. It is used for the duration of the user's session.
number	(Optional) Access list number.
autocommand	(Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and contain embedded spaces, commands using the **autocommand** keyword must be the last option on the line.
command	(Optional) The command string. Because the command can be any length and contain embedded spaces, commands using the **autocommand** keyword must be the last option on the line.
callback-dialstring	(Optional) For asynchronous callback only: permits you to specify a telephone number to pass to the DCE device.
telephone-number	(Optional) For asynchronous callback only: telephone number to pass to the DCE device.
callback-rotary	(Optional) For asynchronous callback only: permits you to specify a rotary group number. The next available line in the rotary group is selected.
rotary-group-number	(Optional) For asynchronous callback only: integer between 1 and 100 that identifies the group of lines on which you want to enable a specific username for callback.
callback-line	(Optional) For asynchronous callback only: specific line on which you enable a specific username for callback.
tty	(Optional) For asynchronous callback only: standard asynchronous line.
line-number	(Optional) For asynchronous callback only: relative number of the terminal line (or the first line in a contiguous group) on which you want to enable a specific username for callback. Numbering begins with zero.
ending-line-number	(Optional) Relative number of the last line in a contiguous group on which you want to enable a specific username for callback. If you omit the keyword (such as **tty**), then *line-number* and *ending-line-number* are absolute rather than relative line numbers.
dnis	Do not require password when obtained via DNIS.
nocallback-verify	(Optional) Authentication not required for EXEC callback on the specified line.
noescape	(Optional) Prevents a user from using an escape character on the host to which that user is connected.
nohangup	(Optional) Prevents Cisco IOS software from disconnecting the user after an automatic command (set up with the **autocommand** keyword) has completed. Instead, the user gets another EXEC prompt.
privilege	(Optional) Sets the privilege level for the user.
level	(Optional) Number between 0 and 15 that specifies the privilege level for the user.

user-maxlinks	Limit the user's number of inbound links.
number	User-maxlinks limit for inbound links.
lawful-intercept	(Optional) Configures lawful intercept users on a Cisco device.
name	Host name, server name, user ID, or command name. The name argument can be only one word. Blank spaces and quotation marks are not allowed.
privilege	(Optional) Sets the privilege level for the user.
privilege-level	(Optional) Number between 0 and 15 that specifies the privilege level for the user.
view	(Optional) For command-line interface (CLI) view only: associates a CLI view name with the local authentication, authorization, and accounting (AAA) database.
view-name	(Optional) For CLI view only: view name, which was specified via the **parser view** command, that is to be associated with the AAA local database.
password *password*	Password to access the CLI view.

Defaults

No username-based authentication system is established.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1	The following keywords and arguments were added: • **username** *name* [**callback-dialstring** *telephone-number*] • **username** *name* [**callback-rotary** *rotary-group-number*] • **username** *name* [**callback-line** [**tty**] *line-number* [*ending-line-number*]] • **username** *name* [**nocallback-verify**]
12.3(7)T	The following keywords and arguments were added: • **lawful-intercept** • **view** • *view-name*

Usage Guidelines

The **username** command provides username or password authentication, or both, for login purposes only.

Multiple **username** commands can be used to specify options for a single user.

Add a username entry for each remote system with which the local router communicates and from which it requires authentication. The remote device must have a username entry for the local router. This entry must have the same password as the local router's entry for that remote device.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an "info" username that does not require a password but connects the user to a general purpose information service.

The **username** command is required as part of the configuration for the Challenge Handshake Authentication Protocol (CHAP). Add a username entry for each remote system from which the local router requires authentication.

Note To enable the local router to respond to remote CHAP challenges, one **username** *name* entry must be the same as the **hostname** entry that has already been assigned to the other router.

CLI and Lawful Intercept Views

Both CLI views and lawful intercept views restrict access to specified commands and configuration information. A lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of simple network management protocol (SNMP) commands that stores information about calls and users.

Users who are specified via the **lawful-intercept** keyword are placed in the lawful-intercept view, by default, if no other privilege level or view name has been explicitly specified.

If there is no *secret* specified and the **debug serial-interface** command is enabled, an error is displayed when a link is established and the CHAP challenge is not implemented. CHAP debugging information is available using the **debug ppp negotiation, debug serial-interface,** and **debug serial-packet** commands. For more information about **debug** commands, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following example implements a service similar to the UNIX **who** command, which can be entered at the login prompt and lists the current users of the router:

```
username who nopassword nohangup autocommand show users
```

The following example implements an information service that does not require a password to be used. The command takes the following form:

```
username info nopassword noescape autocommand telnet nic.ddn.mil
```

The following example implements an ID that works even if all the TACACS+ servers break. The command takes the following form:

```
username superuser password superpassword
```

The following example enables CHAP on interface serial 0 of "server_l." It also defines a password for a remote server named "server_r."

```
hostname server_l
username server_r password theirsystem
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

When you look at your configuration file, the passwords will be encrypted, and the display will look similar to the following:

```
hostname server_1
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

Related Commands

Command	Description
arap callback	Enables an ARA client to request a callback from an ARA client.
callback forced-wait	Forces the Cisco IOS software to wait before initiating a callback to a requesting client.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.
ppp callback (PPP client)	Enables a PPP client to dial into an asynchronous interface and request a callback.
show users	Displays information about the active lines on the router.

username secret

To encrypt a user password with Message Digest 5 (MD5) encryption, use the **username secret** command in global configuration mode.

username *name* **secret** {[**0**] *password* | **5** *encrypted-secret*}

Syntax Description

name	Username.
0	(Optional) Clear text password, which will be MD5 encrypted.
password	Clear text password.
5 *encrypted-secret*	MD5-encrypted text string, which will be stored as the encrypted user password.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use the **username secret** command to configure a username and MD5-encrypted user password. The optional **0** keyword enables MD5 encryption on a clear text password; the **5** keyword enters an MD5 encryption string and saves it as the user MD5-encrypted secret. MD5 encryption is a strong encryption method that is not retrievable; thus, you cannot use MD5 encryption with protocols that require clear text passwords, such as Challenge Handshake Authentication Protocol (CHAP).

The **username secret** command provides an additional layer of security over the username password. It also provides better security by encrypting the password using nonreversible MD5 encryption and storing the encrypted text. The added layer of MD5 encryption is useful in environments in which the password crosses the network or is stored on a TFTP server.

Use MD5 as the encryption type if you paste into this command an encrypted password that you copied from a router configuration file.

Examples

The following example shows how to configure username “abc” and enable MD5 encryption on the clear text password “xyz”:

```
username abc secret xyz
```

The following example shows how to configure username “cde” and enter an MD5 encrypted text string that is stored as the username password:

```
username cde secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the enable password command.
username	Establishes a username-based authentication system.

view

To add a normal command-line interface (CLI) view to a superview, use the **view** command in view configuration mode. To remove a CLI view from a superview, use the **no** form of this command.

view *view-name*

no view *view-name*

Syntax Description

view-name	CLI view that is to be added to the given superview.

Defaults

A superview will not contain any CLI views until this command is enabled.

Command Modes

View configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Before you can use this command to add normal views to a superview, ensure that the following steps have been taken:

- A password has been configured for the superview (via the **password 5** command).
- The normal views that are to be added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

Examples

The following sample output from the **show running-config** command shows that “view_one” and “view_two” have been added to superview “su_view1,” and “view_three” and “view_four” have been added to superview “su_view2”:

```
!
parser view su_view1 superview
 password5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 password5 <encoded password>
 view view_three
 view view_four
!
```

Related Commands!

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.
password 5	Associates a CLI view or a superview with a password.

vlan (local RADIUS server group)

To specify a VLAN to be used by members of the user group, use the **vlan** command in local RADIUS server group configuration mode. To reset the parameter to the default value, use the **no** form of this command.

vlan *vlan*

no vlan *vlan*

Syntax Description

vlan	VLAN ID.

Defaults

No default behavior or values

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

The access point or router moves group members into the VLAN that you specify, overriding any other VLAN assignments. You can assign only one VLAN to a user group.

Examples

The following example shows that VLAN "225" *is* to be used by members of the user group:

```
vlan 225
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.

Command	Description
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.

vpdn aaa attribute nas-port vpdn-nas

To enable the L2TP network server (LNS) to send PPP extended NAS-Port format values from the L2TP access concentrator (LAC) to the RADIUS server for accounting, use the **vpdn aaa attribute nas-port vpdn-nas** command in global configuration mode. To prevent the LNS from sending PPP extended NAS-Port format values, use the **no** form of this command.

vpdn aaa attribute nas-port vpdn-nas

no vpdn aaa attribute nas-port vpdn-nas

Syntax Description

This command has no arguments or keywords.

Defaults

The LNS will not send PPP extended NAS-Port format values to the RADIUS server.

Command Modes

Global configuration

Command History

Release	Modification
11.3(8.1)T	This command was introduced.
12.1(5)T	This command was modified to support the PPP extended NAS-Port format.

Usage Guidelines

The PPP extended NAS-Port format enables the NAS-Port and NAS-Port-Type attributes to provide port details to the RADIUS server when PPP over ATM, PPP over Ethernet (PPPoE) over ATM, or PPPoE over 802.1Q VLANs is used.

The **vpdn aaa attribute nas-port vpdn-nas** command should be configured on the LNS only. The **radius-server attribute nas-port format** command with the **d** keyword must also be configured on the LNS and the L2TP access concentrator (LAC), and the LAC and LNS must both be Cisco routers.

Examples

In the following example, the LNS is configured to recognize and forward PPP extended NAS-Port format values to the RADIUS server. PPP extended NAS-Port format must also be configured on the LAC for this configuration to be effective.

```
vpdn enable
no vpdn logging
!
vpdn-group L2TP-tunnel
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname lac1
 local name lns1
!
aaa new-model
aaa authentication ppp default local group radius
aaa authorization network default local group radius
```

```
aaa accounting network default start-stop group radius

radius-server host 171.79.79.76 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key lns123
!
vpdn aaa attribute nas-port vpdn-nas
```

Related Commands

Command	Description
radius-server attribute nas-port format	Selects the NAS-Port format used for RADIUS accounting features.

vrf (isakmp profile)

To define the virtual routing and forwarding (VRF) value to which the IP Security (IPSec) tunnel will be mapped, use the **vrf** command in Internet Security Association Key Management (ISAKMP) profile configuration mode. To disable the VRF that was defined, use the **no** form of this command.

vrf *ivrf*

no vrf *ivrf*

Syntax Description

ivrf	VRF to which the IPSec tunnel will be mapped.

Defaults

The VRF will be the same as the front door VRF (FVRF).

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use this command to map IPSec tunnels that terminate on a global interface to a specific Virtual Private Network (VPN).

If traffic from the router to a certification authority (CA) (for authentication, enrollment, or for obtaining a certificate revocation list [CRL]) or to a Lightweight Directory Access Protocol (LDAP) server (for obtaining a CRL) needs to be routed via a VRF, the **vrf** command must be added to the trustpoint. Otherwise, such traffic will use the default routing table.

If a profile does not specify one or more trustpoints, all trustpoints in the router will be used to attempt to validate the certificate of the peer (Internet Key Exchange [IKE] main mode or signature authentication). If one or more trustpoints are specified, only those trustpoints will be used.

Examples

The following example shows that two IPSec tunnels to VPN 1 and VPN 2 are terminated:

```
crypto isakmp profile vpn1
 vrf vpn1
 keyring vpn1
 match identity address 172.16.1.1 255.255.255.255
crypto isakmp profile vpn2
 vrf vpn2
 keyring vpn2
 match identity address 10.1.1.1 255.255.255.255
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
crypto ipsec transform-set vpn2 esp-3des esp-md5-hmac
!
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
```

```
 set isakmp-profile vpn1
 match address 101
crypto map crypmap 3 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set vpn2
 set isakmp-profile vpn2
 match address 102
!
!
interface Ethernet1/2
 ip address 172.26.1.1 255.255.255.0
 duplex half
 no keepalive
 no cdp enable
 crypto map crypmap
```

wins

To specify the primary and secondary Windows Internet Naming Service (WINS) servers, use the **wins** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration, use the **no** form of this command.

wins *primary-server secondary-server*

no wins *primary-server secondary-server*

Syntax Description

primary-server	Name of the primary WINS server.
secondary-server	Name of the secondary WINS server.

Defaults

No default behavior or values.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

You must enable the **crypto isakmp client configuration group command, which specifies group policy information that has to be defined or changed, before enabling the wins command.**

Examples

The following example shows how to define a primary and secondary WINS server for the group “cisco”:

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
  wins 10.1.1.2 10.1.1.3
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

wlccp authentication-server client

To configure the list of servers to be used for 802.1X authentication, use the **wlccp authentication-server client** command in global configuration mode. To disable the server list, use the **no** form of this command.

wlccp authentication-server client {**any** | **eap** | **leap** | **mac**} *list*

no wlccp authentication-server client {**any** | **eap** | **leap** | **mac**} *list*

Syntax Description

any	Specifies client devices that use any authentication.
eap	Specifies client devices that use Extensible Authentication Protocol (EAP) authentication.
leap	Specifies client devices that use Light Extensible Authentication Protocol (LEAP) authentication.
mac	Specifies client devices that use MAC-based authentication.
list	List of client devices.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

You can specify a list of client devices that use any type of authentication, or you can specify a list of client devices that use a certain type of authentication (such as EAP, LEAP, or MAC-based authentication).

Examples

The following example shows how to configure the server list for LEAP authentication for client devices:

```
Router (config)# wlccp authentication-server client leap leap-list1
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.

Command	Description
show wlccp wds	Shows information about access points and client devices on the WDS router.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

wlccp authentication-server infrastructure

To configure the list of servers to be used for 802.1X authentication for the wireless infrastructure devices, use the **wlccp authentication-server infrastructure** command in global configuration mode. To disable the server list, use the **no** form of this command.

wlccp authentication-server infrastructure *list*

no wlccp authentication-server infrastructure *list*

Syntax Description

list	List of servers to be used for 802.1X authentication for the wireless infrastructure devices, such as access points, repeaters, and wireless-aware routers.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet access points.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

This example shows how to configure the server list for 802.1X authentication for infrastructure devices participating in Cisco Centralized Key Management:

```
Router (config)# wlccp authentication-server infrastructure wlan-list1
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
show wlccp wds	Shows information about access points and client devices on the WDS router.
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

wlccp wds priority interface

To configure the router or access point to provide wireless domain services (WDS), use the **wlccp wds priority interface** command in global configuration mode. To remove the WDS configuration from the router or access point, use the **no** form of this command.

wlccp wds priority *priority* **interface** *interface*

no wlccp wds priority *priority* **interface** *interface*

Syntax Description

priority	Priority of this WDS candidate. The valid range is from 1 to 255. The greater the priority value, the higher the priority.
interface	Interface on which the router sends out WDS advertisements. Supported interface types are as follows: • For access points—bvi • For wireless-aware routers—bvi, svi, Fast Ethernet, and Gigabit Ethernet.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced with support for Cisco Aironet access points.
12.3(11T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

The WDS candidate with the highest priority becomes the active WDS device.

Examples

This example shows how to configure the priority for an access point as a candidate to provide WDS with priority 200:

```
Router (config)# wlccp wds priority 200 interface bvi 1
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
show wlccp wds	Shows information about access points and client devices on the WDS router.

Command	Description
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.