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.

secondary-color

To specify the color of the secondary title bars on the login and portal pages of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **secondary-color** command in Web VPN configuration mode. To remove the color, use the **no** form of this command.

secondary-color *color*

no secondary-color *color*

Syntax Description

color	*The value can be a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a "#"), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation):* • \#/x{6} • \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255) • \w+ *The default is purple.*

Defaults

Purple

Command Modes

Web VPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

If a new color is configured, it will override the color that was already configured.

Examples

The following examples show three ways that a secondary color may be configured:

```
secondary-color darkseagreen

secondary-color #8FBC8F

secondary-color 143,188,143
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

secondary-text-color

To specify the color of the text on the secondary bars of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **secondary-text-color** command in Web VPN configuration mode. To revert to the default color, use the **no** form of this command.

secondary-text-color *[***black | white***]*

no secondary-text-color *[***black | white***]*

Syntax Description

black	(Optional) Color of the text is black. This is the default value.
white	(Optional) Color of the text is white.

Defaults

Color of the text is black.

Command Modes

Web VPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The color of the text on the secondary bars must be aligned with the color of the text on the title bar.

Examples

The following example shows that the secondary text color has been set to white:

```
secondary-text-color white
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

secret

To associate a command-line interface (CLI) view or a superview with a password, use the **secret** command in view configuration mode.

secret {*unencrypted-password* | **0** *unencrypted-password* | **5** *encrypted-password}*

Syntax Description

unencrypted-password	Nonencrypted password. A password can contain any combination of alphanumeric characters. The password is case sensitive. This clear-text password will be encrypted using the Message Digest 5 (MD5) method.
0	Specifes that an unencrypted password will follow.
5	Specifes that an encrypted password will follow.
encrypted-password	Encrypted password that you enter and that is copied from another router configuration.

Defaults

User cannot access a CLI view or superview.

Command Modes

View configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

A user cannot access any commands within the CLI view or superview until the **secret** command has been issued.

Note The password cannot be removed, but you can overwrite it.

Examples

The following examples show how to configure two CLI views, “first” and “second,” and associate each view with a password:

CLI View “first”

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view first
Router(config-view)#
*Dec  9 05:20:03.039: %PARSER-6-VIEW_CREATED: view 'first' successfully created.
Router(config-view)# secret firstpassword
Router(config-view)# secret secondpassword
% Overwriting existing secret for the current view
Router(config-view)# secret 0 thirdpassword
% Overwriting existing secret for the current view
Router(config-view)# secret 5 $1$jj1e$vmYyRbmj5UoU96tT1x7eP1
% Overwriting existing secret for the current view
```

```
Router(config-view)# secret 5 invalidpassword
ERROR: The secret you entered is not a valid encrypted secret.
To enter an UNENCRYPTED secret, do not specify type 5 encryption.
When you properly enter an UNENCRYPTED secret, it will be encrypted.

Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command configure include all ip
Router(config-view)# exit
```

CLI View "second"

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view second
Router(config-view)#
*Dec 30 06:11:52.915: %PARSER-6-VIEW_CREATED: view 'second' successfully created.
Router(config-view)# secret mypasswd
Router(config-view)# commands exec include ping
Router(config-view)# end

Router# show running-config

parser view second
 secret 5 $1$PWs8$lz3lSx6OqAnFrUx2hkI0w0
 commands exec include ping
!
```

The following is an example of **show running-config** output for a situation in which the **secret** command has been configured using a level 5 encrypted password:

```
Router: show running-config

parser view first
 secret 5 $1$jj1e$vmYyRbmj5UoU96tT1x7eP1
 commands configure include all ip
 commands exec include configure terminal
 commands exec include configure
 commands exec include show version
 commands exec include show
!
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.

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 valid value range for the *threshold-rate* argument is 2 to 1024. 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.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.3(7)T	The range of the *threshold-rate* value was changed from 1 through 1024 to 2 through 1024.

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.

Note Previous to the Cisco IOS software release 12.3(7)T the *threshold-rate* value range was 1 through 1024. Unsuccessful login attempts will not be logged if a value of 1 is configured. As of Cisco ISO release 12.3(7)T, use a value between 2 and 1024.

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**] [**default**] | *ip-address* [**default**] }

no set peer {*host-name* [**dynamic**] [**default**] | *ip-address* [**default**] }

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.
default	(Optional) If there are multiple IPSec peers, designates that the first peer is the default peer.
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.
12.3(14)T	The **default** 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.

The default Keyword

If there are multiple peers and you specify the **default** keyword, the first peer is designated as the default peer.

If dead peer detection (DPD) detects a failure, the default peer is retried before there is an attempt to connect to the next peer in the peer list.

If the default peer is unresponsive, the next peer in the peer list becomes the new current peer. Future connections through the crypto map will try that peer.

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 Domain Name System (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 ...
```

The following example shows that the first peer, at IP address 1.1.1.1, is the default peer.

```
crypto map tohub 1 ipsec-isakmp
 set peer 1.1.1.1 default
 set peer 2.2.2.2
```

The following example shows that the peer with the host name fred is the default peer.

```
crypto map tohub 2 ipsec-isakmp
 set peer fred dynamic default
 set peer barney dynamic
```

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.
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 idle-time

To specify the maximum amount of time for which the current peer can be idle before the default peer is used, use the **set security-association idle-time** command in crypto map configuration mode. To disable this feature, use the **no** form of this command.

set security-association idle-time *seconds* [**default**]

no set security-association idle-time *seconds* [**default**]

Syntax Description

seconds	Number of seconds for which the current peer can be idle before the default peer is used. Valid values are 60 to 86400.
default	(Optional) Specifies that the next connection is directed to the default peer.

Defaults

If the **default** keyword is not specified and there is a connection timeout, the current peer remains unchanged.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is optional. Use this command if you want the default peer to be used if the current peer times out. If there is a timeout to the current peer, the connection to that peer is closed. The next time a connection is initiated, it is directed to the default peer specified in the **set peer** command.

Examples

In the following example, if the current peer is idle for 120 seconds, the default peer 10.1.1.1 (which was specified in the **set peer** command) is used for the next attempted connection:

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
 set security-association idle-time 120 default
```

Related Commands

Command	Description
set peer (IPsec)	Specifies an IPsec peer in a crypto map entry.

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 security-association replay disable

To disable anti-replay checking for a particular crypto map, dynamic crypto map, or crypto profile, use the **set security-association replay disable** command in crypto map configuration or crypto profile configuration mode. To enable anti-replay checking, use the **no** form of this command.

set security-association replay disable

no set security-association replay disable

Syntax Description

This command has no arguments or keywords.

Defaults

Anti-replay checking is enabled.

Command Modes

Crypto map configuration
Crypto profile configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows that anti-replay checking has been disabled for the crypto map named "mymap."

```
crypto map mymap 30
set security-association replay disable
```

Related Commands

Command	Description
set security-association replay window-size	Controls the SAs that are created using the policy specified by a particular crypto map, dynamic crypto map, or crypto profile.

set security-association replay window-size

To control the security associations (SAs) that are created using the policy specified by a particular crypto map, dynamic crypto map, or crypto profile, use the **set security-association replay window-size** command in crypto map configuration or crypto profile configuration mode. To reset the crypto map to follow the global configuration that was specified by the **crypto ipsec security-association replay window-size** command, use the **no** form of this command.

set security-association replay window-size [*N***]**

no set security-association replay window-size

Syntax Description

N	(Optional) Size of the window. The value can be 64, 128, 256, 512, or 1024. This value sets the window size for a particular crypto map, dynamic crypto map, or crypto profile.

Defaults

Window size is not set.

Command Modes

Crypto map configuration
Crypto profile configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows that the SA window size has been set to 256 for the crypto map named "mymap":

```
crypto map mymap 10
set security-association replay window-size 256
```

Related Commands

Command	Description
set security-association replay disable	Disables anti-replay checking for a particular crypto map, dynamic crypto map, or crypto profile.

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 authentication

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 attributes [**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 radius** keyword was added.
12.3(14)T	T.38 fax relay call statistics were made available to Call Detail Records (CDRs) through Vendor-Specific Attributes (VSAs) and added to the call log.

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
```

The following example is sample output for the **show aaa attributes** command. In this example, all the T.38 fax relay statistics are displayed.

```
Router# show aaa attributes
!
    Type=485   Name=originating-line-info          Format=Ulong
    Type=486   Name=charge-number                  Format=String
    Type=487   Name=transmission-medium-req        Format=Ulong
    Type=488   Name=redirecting-number             Format=String
    Type=489   Name=backward-call-indicators       Format=String
    Type=490   Name=remote-media-udp-port          Format=Ulong
    Type=491   Name=remote-media-id                Format=String
    Type=492   Name=supp-svc-xfer-by               Format=String
    Type=493   Name=faxrelay-start-time            Format=String
    Type=494   Name=faxrelay-max-jit-buf-depth     Format=String
    Type=495   Name=faxrelay-jit-buf-ovflow        Format=String
    Type=496   Name=faxrelay-mr-hs-mod             Format=String
    Type=497   Name=faxrelay-init-hs-mod           Format=String
    Type=498   Name=faxrelay-num-pages             Format=String
    Type=499   Name=faxrelay-direction             Format=String
    Type=500   Name=faxrelay-ecm-in-use            Format=String
    Type=501   Name=faxrelay-encap-prot            Format=String
    Type=502   Name=faxrelay-nsf-country-code      Format=String
    Type=503   Name=faxrelay-nsf-manuf-code        Format=String
    Type=504   Name=faxrelay-fax-success           Format=String
    Type=505   Name=faxrelay-tx-packets            Format=String
    Type=506   Name=faxrelay-rx-packets            Format=String
```

Table 31 provides an alphabetical listing of the fields displayed in the output of the **show aaa attributes** command displaying T.38 statistics and a description of each field.

Table 31 show aaa attributes Field Descriptions

Field	Description
Format=Ulong	Format type is ULong.
Format=String	Format type is string.
Name=backward-call-indicators	Backward call indicator.
Name=charge-number	Charge number.
Name=faxrelay-direction	Direction of fax relay.
Name=faxrelay-ecm-in-use	Error correction mode in use for the fax relay.
Name=faxrelay-encap-prot	Encapsulation protocol for fax relay.
Name=faxrelay-fax-success	Fax relay success.
Name=faxrelay-init-hs-mod	Fax relay initial high-speed modulation.
Name=faxrelay-jit-buf-ovflow	Fax relay jitter buffer overflow.
Name=faxrelay-max-jit-buf-depth	Fax relay maximum jitter buffer depth.
Name=faxrelay-mr-hs-mod	Fax relay most recent high speed modulation.
Name=faxrelay-num-pages	Fax relay number of fax pages.
Name=faxrelay-nsf-country-code	Fax relay Nonstandard Facilities (NSF) country code.
Name=faxrelay-nsf-manuf-code	Fax relay NSF manufacturers code.
Name=faxrelay-rx-packets	Fax relay received packets
Name=faxrelay-start-time	Fax relay start time.

Table 31 show aaa attributes Field Descriptions (continued)

Field	Description
Name=faxrelay-tx-packets	Fax relay transmitted packets.
Name=originating-line-info	Originating line information.
Name=redirecting-number	Redirecting number.
Name=remote-media-id	Remote media ID.
Name=remote-media-udp-port	Remote media UDP port.
Name=supp-svc-xfer-by	Supplementary service transfer.
Name=transmission-medium-req	Transmission medium requirement.
Type=	Type of fax relay string.

Related Commands

Command	Description
debug voip aaa	Enables debugging messages for gateway authentication, authorization, and accounting (AAA) to be sent to the system console.

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 32 describes the significant fields shown in the display.

Table 32 show aaa cache filterserver 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 local user locked

To display a list of all locked-out users, use the **show aaa local user locked** command in privileged EXEC mode.

show aaa local user locked

Syntax Description

This command has no arguments or keywords.

Defaults

Names of locked-out users are not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command can be used only by users having root privilege.

Examples

The following output of the **show aaa local user locked** command illustrates that user1 is locked out:

```
Router# show aaa local user locked

               Local-user          Lock time
               user1                  04:28:49 UTC Sat Jun 19 2004
```

The fields in the output example are self-explanatory.

Related Commands

Command	Description
aaa local authentication attempts max-fail	Specifies the maximum number of unsuccessful authentication attempts before a user is locked out.
clear aaa local user fail-attempts	Clears the unsuccessful login attempts of a user.
clear aaa local user lockout	Unlocks the locked-out user.

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 33.

```
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 33 describes the significant fields in the display.

Table 33 show aaa server-private 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.

Table 33 show aaa server-private Field Descriptions

Field	Description
acct-port	UDP destination port for accounting requests. The default value is 1646.
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 34 describes the significant fields in the display.

Table 34 show aaa servers 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 34 show aaa servers 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 34 show aaa servers 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 34 show aaa servers 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 35.

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 35.

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 35 lists the significant fields shown in the display.

Table 35 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 appfw

To display application firewall policy configuration information, use the **show appfw configuration** command in privileged EXEC mode.

show appfw configuration [*name*]

Syntax Description

name	(Optional) Displays information only for the specified policy.

Defaults

If no keywords are specified, information for all policies is shown.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to display information regarding the application firewall policy configuration.

Examples

This sample output for the **show appfw configuration** command and the **show ip inspect configuration** command displays the configuration for the inspection rule "mypolicy," which has been applied to all incoming HTTP traffic on the FastEthernet0/0 interface. In this example, you can see that all available HTTP inspection parameters have been defined.

```
Router# show appfw configuration

Application Firewall Rule configuration
  Application Policy name mypolicy
    Application http
      strict-http action allow alarm
      content-length minimum 0 maximum 1 action allow alarm
      content-type-verification match-req-rsp action allow alarm
      max-header-length request length 1 response length 1 action allow alarm
      max-uri-length 1 action allow alarm
      port-misuse default action allow alarm
      request-method rfc default action allow alarm
      request-method extension default action allow alarm
      transfer-encoding default action allow alarm

Router# show ip inspect config

Session audit trail is disabled
Session alert is enabled
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 firewall
http alert is on audit-trail is off timeout 3600
```

Related Commands

Command	Description
show ip inspect	Displays firewall configuration and session information.

show auto secure config

To display AutoSecure configurations, use the **show auto secure config** command in privileged EXEC mode.

show auto 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.
12.3(15)	Autosecure disables the configuration of the autosec_iana_reserved_block, autosec_private_block, or autosec_complete_bogon access control lists (acls), and application-to-edge interfaces. Output for these acls is no longer shown in the show output.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

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
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 36 describes the significant fields shown in the display.

Table 36 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 37 describes the significant fields shown in the display.

Table 37 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 37 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 eng qos

To monitor and maintain low latency queueing (LLQ) for IP security (IPsec) encryption engines, use the **show crypto eng qos** command in privileged EXEC mode.

show crypto eng qos

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

Use the **show crypto eng qos** command to determine whether quality of service (QoS) is enabled on LLQ for IPsec encryption engines.

Examples

The following example shows whether LLQ for IPsec encryption engines is enabled:

```
Router# show crypto eng qos

crypto engine name: Multi-ISA Using VAM2
        crypto engine type: hardware
                      slot: 5
                  queuing: enabled
         visible bandwidth: 30000 kbps
                   llq size: 0
    default queue size/max: 0/64
      interface table size: 32

  FastEthernet0/0 (3), iftype 1, ctable size 16, input filter:ip
precedence 5
class voice (1/3), match ip precedence 5
          bandwidth 500 kbps, max token 100000
          IN  match pkt/byte 0/0, police drop 0
          OUT match pkt/byte 0/0, police drop 0

  class default, match pkt/byte 0/0, qdrop 0
  crypto engine bandwidth:total 30000 kbps, allocated 500 kbps
```

The field descriptions in the above display are self-explanatory.

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 the **show crypto engine** command and the **brief** keyword shows typical crypto engine summary 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 38 describes significant fields shown in the display.

Table 38 show crypto engine 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 decompressed0 packets compressed
     0 compressed bytes in0 encompassed bytes in
     0 packets bypass compression0 packet abort compression
     0 packets fail compression
    4:1 compression ratio2:1 overall compression ratio
     0 decompressed bytes out0 compressed bytes out
     0 packets decrypted0 packets encrypted
     0 bytes decrypted0 bytes encrypted
     0 bytes before decrypt0 bytes after encrypt
     0 paks/sec in0 paks/sec out
```

```
 0 Kbits/sec decrypted0 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 39 describes significant fields shown in the display.

Table 39 show crypto engine accelerator statistics 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 39 show crypto engine accelerator statistics 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 40 describes significant fields shown by the **show crypto ipsec client ezvpn** command:

Table 40 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 **show 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
```