

Wireless Domain Services Configuration

Document ID: 44720

Introduction

Prerequisites

Requirements

Components Used

Conventions

Wireless Domain Services

Role of the WDS Device

Role of Access Points Using the WDS Device

Configuration

Designate an AP as WDS

Designate a WLSM as WDS

Designate an AP as Infrastructure Device

Define Client Authentication Method

Verify

Troubleshoot

Troubleshooting Commands

Related Information

Introduction

This document introduces the concept of Wireless Domain Services (WDS). The document also describes how to configure one access point (AP) or the Wireless LAN Services Module (WLSM) as the WDS and at least one other as an infrastructure AP. The procedure in this document guides you to a WDS that is functional and allows clients to associate to either the WDS AP or to an infrastructure AP. This document intends to establish a basis from which you can configure Fast Secure Roaming or introduce a Wireless LAN Solutions Engine (WLSE) into the network, so you can use the features.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Have thorough knowledge of wireless LAN networks and wireless security issues.
- Have knowledge of current Extensible Authentication Protocol (EAP) security methods.

Components Used

The information in this document is based on these software and hardware versions:

- APs with Cisco IOS® Software
- Cisco IOS Software Release 12.3(2)JA2 or later
- Catalyst 6500 Series Wireless LAN Services Module

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration and an IP address on interface BV11, so the unit is accessible from the Cisco IOS Software GUI or the command line interface (CLI). If you

work in a live network, ensure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Wireless Domain Services

WDS is a new feature for APs in Cisco IOS Software and the basis of the Catalyst 6500 Series WLSM. WDS is a core function that enables other features like these:

- Fast Secure Roaming
- WLSE interaction
- Radio Management

You must establish relationships between the APs that participate in WDS and the WLSM, before any other WDS-based features work. One of the purposes of WDS is to eliminate the need for the authentication server to validate user credentials and reduce the time required for client authentications.

In order to use WDS, you must designate one AP or the WLSM as the WDS. A WDS AP must use a WDS user name and password to establish a relationship with an authentication server. The authentication server can be either an external RADIUS server or the Local RADIUS Server feature in the WDS AP. The WLSM must have a relationship with the authentication server, even though WLSM does not need to authenticate to the server.

Other APs, called infrastructure APs, communicate with the WDS. Before registration occurs, the infrastructure APs must authenticate themselves to the WDS. An infrastructure server group on the WDS defines this infrastructure authentication.

One or more client server groups on the WDS define client authentication.

When a client attempts to associate to an infrastructure AP, the infrastructure AP passes the credentials of the user to the WDS for validation. If the WDS sees the credentials for the first time, WDS turns to the authentication server to validate the credentials. The WDS then caches the credentials, in order to eliminate the need to return to the authentication server when the same user attempts authentication again. Examples of re-authentication include:

- Re-keying
- Roaming
- When the user starts up the client device

Any RADIUS-based EAP authentication protocol can be tunneled through WDS such as these:

- Lightweight EAP (LEAP)
- Protected EAP (PEAP)
- EAP-Transport Layer Security (EAP-TLS)
- EAP-Flexible Authentication through Secure Tunneling (EAP-FAST)

MAC address authentication can also tunnel to either an external authentication server or against a list local to a WDS AP. The WLSM does not support MAC address authentication.

The WDS and the infrastructure APs communicate over a multicast protocol called WLAN Context Control Protocol (WLCCP). These multicast messages cannot be routed, so a WDS and the associated infrastructure

APs must be in the same IP subnet and on the same LAN segment. Between the WDS and the WLSE, WLCCP uses TCP and User Datagram Protocol (UDP) on port 2887. When the WDS and WLSE are on different subnets, a protocol like Network Address Translation (NAT) cannot translate the packets.

An AP configured as the WDS device supports up to 60 participating APs. An Integrated Services Router (ISR) configured as the WDS device supports up to 100 participating APs. And a WLSM-equipped switch supports up to 600 participating APs and up to 240 mobility groups. A single AP supports up to 16 mobility groups.

Note: Cisco recommends that the infrastructure APs run the same version of IOS as the WDS device. If you use an older version of IOS, the APs might fail to authenticate to the WDS device. In addition, Cisco recommends that you use the latest version of the IOS. You can find the latest version of IOS in the Wireless downloads page.

Role of the WDS Device

The WDS device performs several tasks on your wireless LAN:

- Advertises its WDS capability and participates in electing the best WDS device for your wireless LAN. When you configure your wireless LAN for WDS, you set up one device as the main WDS candidate and one or more additional devices as backup WDS candidates. If the main WDS device goes off line, one of the backup WDS devices takes its place.
- Authenticates all APs in the subnet and establishes a secure communication channel with each of them.
- Collects radio data from APs in the subnet, aggregates the data, and forwards it to the WLSE device on your network.
- Acts as a pass-through for all 802.1x-authenticated client devices associated to participating APs.
- Registers all client devices in the subnet that use dynamic keying, establishes session keys for them, and caches their security credentials. When a client roams to another AP, the WDS device forwards the client's security credentials to the new AP.

Role of Access Points Using the WDS Device

The APs on your wireless LAN interact with the WDS device in these activities:

- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.
- Report radio data to the WDS device.

Configuration

WDS presents the configuration in an ordered, modular fashion. Each concept builds on the concept that precedes. The WDS omits other configuration items such as passwords, remote access, and radio settings for clarity and focus on the core subject matter.

This section presents the information necessary to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Designate an AP as WDS

The first step is to designate an AP as the WDS. The WDS AP is the only one that communicates with the authentication server.

Complete these steps in order to designate an AP as WDS:

1. In order to configure the Authentication server on the WDS AP, choose **Security > Server Manager** to go to the Server Manager tab:
 - a. Under Corporate Servers, type the IP address of the authentication server in the Server field.
 - b. Specify the Shared Secret and the ports.
 - c. Under Default Server Priorities, set the Priority 1 field to that server IP address under the appropriate authentication type.

Cisco 1200 Access Point

SERVER MANAGER | GLOBAL PROPERTIES

Hostname: WDS_AP 16:09:43 Fri Apr 23 2004

Security: Server Manager

Backup RADIUS Server

Backup RADIUS Server: (Hostname or IP Address)
Shared Secret:
[Apply] [Delete] [Cancel]

Corporate Servers

Current Server List
[RADIUS]

<NEW>
10.0.0.3
[Delete]

Server: 10.0.0.3 (Hostname or IP Address)
Shared Secret:
Authentication Port (optional): 1645 (0-65536)
Accounting Port (optional): 1646 (0-65536)
[Apply] [Cancel]

Default Server Priorities

EAP Authentication
Priority 1: 10.0.0.3
Priority 2: <NONE>
Priority 3: <NONE>

MAC Authentication
Priority 1: <NONE>
Priority 2: <NONE>
Priority 3: <NONE>

Accounting
Priority 1: <NONE>
Priority 2: <NONE>
Priority 3: <NONE>

Admin Authentication (RADIUS)
Priority 1: <NONE>
Priority 2: <NONE>
Priority 3: <NONE>

Admin Authentication (TACACS+)
Priority 1: <NONE>
Priority 2: <NONE>
Priority 3: <NONE>

Proxy Mobile IP Authentication
Priority 1: <NONE>
Priority 2: <NONE>
Priority 3: <NONE>

[Apply] [Cancel]

Alternatively, issue these commands from the CLI:

```
WDS_AP#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

WDS_AP(config)#aaa group server radius rad_eap

WDS_AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646

WDS_AP(config-sg-radius)#exit

WDS_AP(config)#aaa new-model

WDS_AP(config)#aaa authentication login eap_methods group rad_eap

WDS_AP(config)#radius-server host 10.0.0.3 auth-port 1645
    acct-port 1646 key labap1200ip102

    !--- This command appears over two lines here due to space limitations.

WDS_AP(config)#end

WDS_AP#write memory
```

2. The next step is to configure the WDS AP in the authentication server as an authentication, authorization, and accounting (AAA) client. For this, you need to add the WDS AP as an AAA client. Complete these steps:

Note: This document uses the Cisco Secure ACS server as the authentication server.

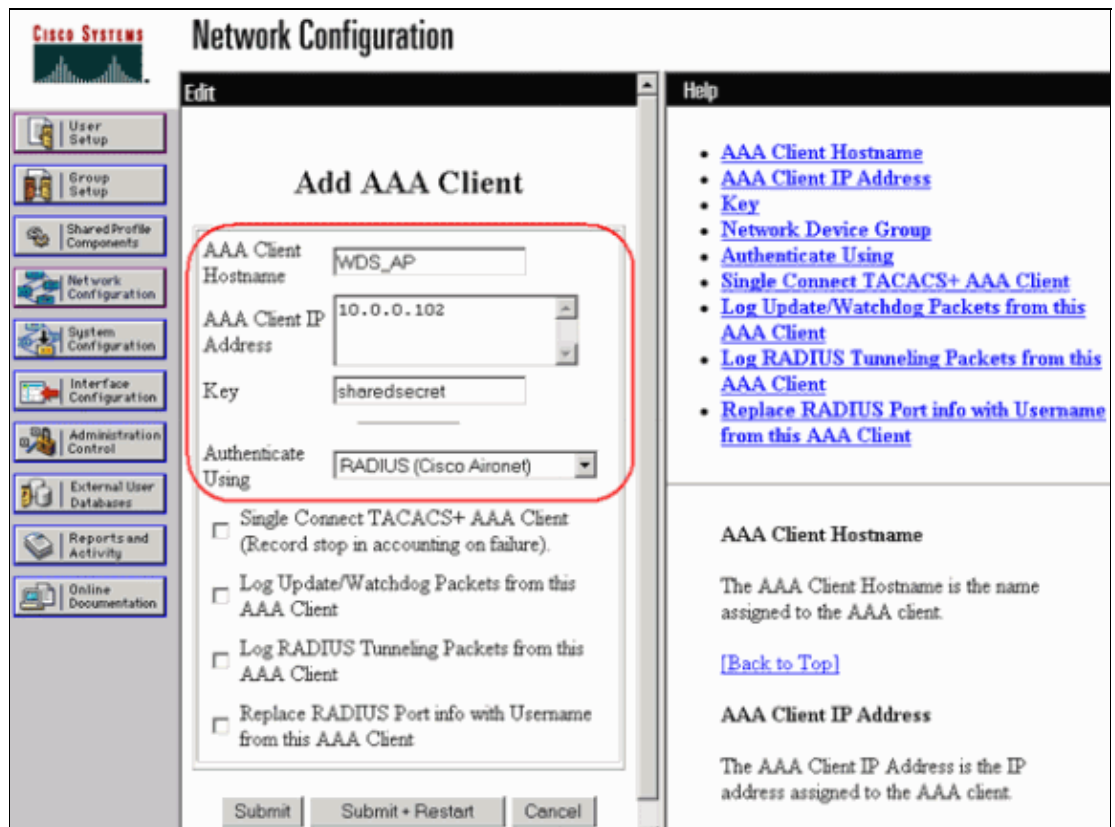
- a. In Cisco Secure Access Control Server (ACS), this occurs on the Network Configuration page where you define these attributes for the WDS AP:

- ◇ Name
- ◇ IP address
- ◇ Shared secret
- ◇ Authentication method

- RADIUS Cisco Aironet
- RADIUS Internet Engineering Task Force [IETF]

Click on **Submit**.

For other non-ACS authentication servers, refer to the documentation from the manufacturer.



CISCO SYSTEMS Network Configuration

Edit

Add AAA Client

AAA Client Hostname: WDS_AP

AAA Client IP Address: 10.0.0.102

Key: sharedsecret

Authenticate Using: RADIUS (Cisco Aironet)

☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
☐ Log Update/Watchdog Packets from this AAA Client
☐ Log RADIUS Tunneling Packets from this AAA Client
☐ Replace RADIUS Port info with Username from this AAA Client

Submit Submit + Restart Cancel

Help

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

AAA Client Hostname

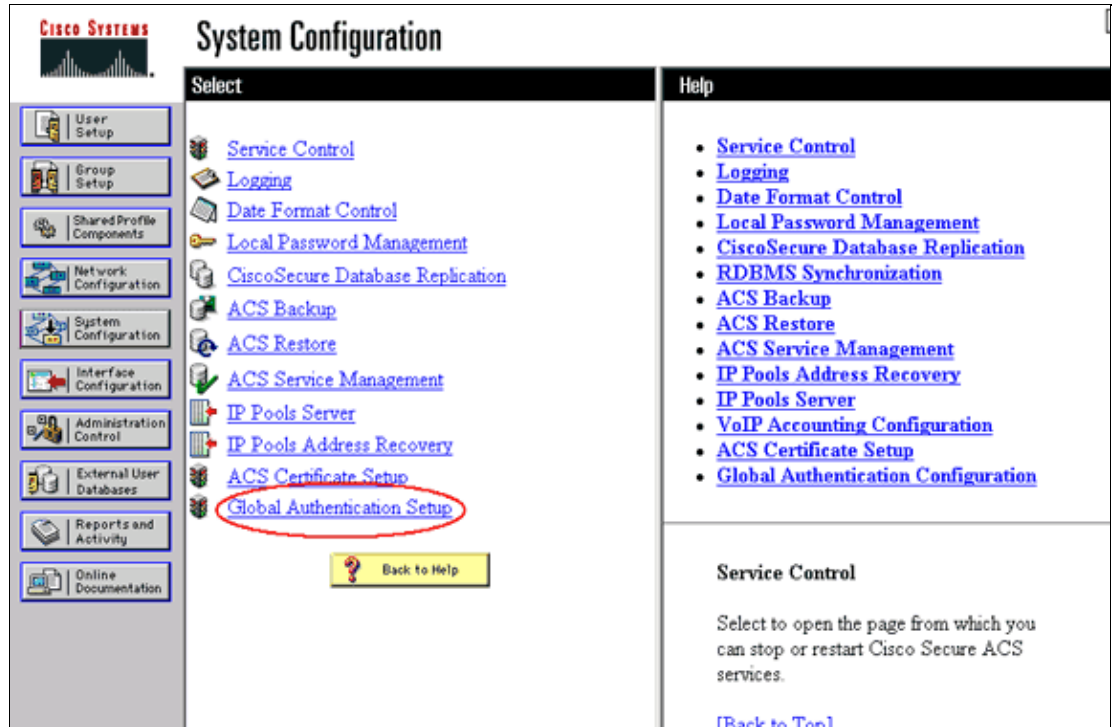
The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

- b. Also, in Cisco Secure ACS, ensure that you configure ACS to perform LEAP authentication on the System Configuration – Global Authentication Setup page. First, click **System Configuration**, then click **Global Authentication Setup**.



CISCO SYSTEMS System Configuration

Select

- [Service Control](#)
- [Logging](#)
- [Date Format Control](#)
- [Local Password Management](#)
- [CiscoSecure Database Replication](#)
- [ACS Backup](#)
- [ACS Restore](#)
- [ACS Service Management](#)
- [IP Pools Server](#)
- [IP Pools Address Recovery](#)
- [ACS Certificate Setup](#)
- [Global Authentication Setup](#)

[Back to Help](#)

Help

- [Service Control](#)
- [Logging](#)
- [Date Format Control](#)
- [Local Password Management](#)
- [CiscoSecure Database Replication](#)
- [RDBMS Synchronization](#)
- [ACS Backup](#)
- [ACS Restore](#)
- [ACS Service Management](#)
- [IP Pools Address Recovery](#)
- [IP Pools Server](#)
- [VoIP Accounting Configuration](#)
- [ACS Certificate Setup](#)
- [Global Authentication Configuration](#)

Service Control

Select to open the page from which you can stop or restart Cisco Secure ACS services.

[\[Back to Top\]](#)

- c. Scroll down the page to the LEAP setting. When you check the box, ACS authenticates LEAP.

System Configuration

Edit

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Reports and Activity

Online Documentation

Global Authentication Setup

EAP Configuration

PEAP

☒ Allow EAP-MSCHAPv2
 ☒ Allow EAP-GTC

Cisco client initial message:

PEAP session timeout (minutes):

☒ Enable Fast Reconnect

EAP-FAST

☒ Allow EAP-FAST

Active master key TTL:

months

Retired master key TTL:

months

PAC TTL:

weeks

Client initial message:

Authority ID Info:

☐ Allow automatic PAC provisioning
 ☒ EAP-FAST master server

Actual EAP-FAST server status: Master

EAP-TLS

☒ Allow EAP-TLS

Select one or more of the following options:

☒ Certificate SAN comparison
 ☒ Certificate CN comparison
 ☒ Certificate Binary comparison

EAP-TLS session timeout (minutes):

LEAP

☒ Allow LEAP (For Aironet only)

EAP-MD5

☒ Allow EAP-MD5

AP EAP request timeout (seconds):

MS-CHAP Configuration

☒ Allow MS-CHAP Version 1 Authentication
 ☒ Allow MS-CHAP Version 2 Authentication

Back to Help

Submit

Submit + Restart

Cancel

Help

- PEAP
- EAP-FAST
- EAP-TLS
- LEAP
- EAP-MD5
- AP EAP request timeout
- MS-CHAP Configuration

This page specifies settings for various authentication protocols.

[Back to Top](#)

PEAP

Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have

3. In order to configure the WDS settings on the WDS AP, choose **Wireless Services > WDS** on the WDS AP, and click on the **General Set-Up** tab. Perform these steps:
 - a. Under WDS—Wireless Domain Services – Global Properties, check **Use this AP as Wireless Domain Services**.
 - b. Set the value for the Wireless Domain Services Priority field to a value of approximately **254**, because this is the first one. You can configure one or more APs or switches as candidates to provide WDS. The device with the highest priority provides WDS.



Alternatively, issue these commands from the CLI:

```
WDS_AP#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

WDS_AP(config)#wlccp wds priority 254 interface BVI1

WDS_AP(config)#end

WDS_AP#write memory
```

4. Choose **Wireless Services > WDS**, and go to the **Server Groups** tab:
 - a. Define a Server Group Name that authenticates the other APs, an Infrastructure group.
 - b. Set Priority 1 to the previously configured authentication server.
 - c. Click the **Use Group For: Infrastructure Authentication** radio button.
 - d. Apply the settings to the relevant Service Set Identifiers (SSIDs).

Cisco Systems Cisco 1200 Access Point

WDS STATUS SERVER GROUPS GENERAL SET-UP

Hostname WDS_AP 16:26:44 Fri Apr 23 2004

Wireless Services: WDS - Server Groups

Server Group List

<NEW>
Infrastructure

Delete

Server Group Name: Infrastructure

Group Server Priorities: [Define Servers](#)

Priority 1: 10.0.0.3

Priority 2: <NONE>

Priority 3: <NONE>

Use Group For:

☒ Infrastructure Authentication

☐ Client Authentication

Authentication Settings

☐ EAP Authentication

☐ LEAP Authentication

☐ MAC Authentication

☐ Default (Any) Authentication

SSID Settings

☒ Apply to all SSIDs

☐ Restrict SSIDs (Apply only to listed SSIDs)

SSID: DISABLED Add Remove

Apply Cancel

Alternatively, issue these commands from the CLI:

```
WDS_AP#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

WDS_AP(config)#wlccp authentication-server infrastructure
method_Infrastructure

WDS_AP(config)#aaa group server radius Infrastructure

WDS_AP(config-sg-radius)#server 10.0.0.3 auth-port 1645
acct-port 1646

WDS_AP(config-sg-radius)#exit

WDS_AP(config)#aaa authentication login method_Infrastructure
group Infrastructure

WDS_AP(config)#end
```

```
WDS_AP#write memory
```

*!--- Some of the commands in this table appear over two lines here due to
!--- space limitations. Ensure that you enter these commands in a single line.*

5. Configure the WDS user name and password as a user in your authentication server.

In Cisco Secure ACS, this occurs on the User Setup page, where you define the WDS user name and password. For other non-ACS authentication servers, refer to the documentation from the manufacturer.

Note: Do not put the WDS user in a group that is assigned many rights and privileges WDS only requires limited authentication.

The screenshot displays the Cisco Systems User Setup interface. The main content area is titled 'Edit' and shows the configuration for a user named 'WDSUser (New User)'. The 'User Setup' section is highlighted with a red box, indicating the 'Password Authentication' dropdown is set to 'CiscoSecure Database', the 'CiscoSecure PAP' checkbox is checked, and the 'Password' and 'Confirm Password' fields are present. The 'Supplementary User Info' section includes fields for 'Real Name' and 'Description'. The left sidebar contains navigation links such as 'User Setup', 'Group Setup', 'Shared Profile Components', 'Network Configuration', 'System Configuration', 'Interface Configuration', 'Administration Control', 'External User Databases', 'Reports and Activity', and 'Online Documentation'. The right sidebar contains a 'Help' section with links to various configuration options, including 'Account Disabled', 'Deleting a Username', 'Supplementary User Info', 'Password Authentication', 'Group to which the user is assigned', 'Callback', 'Client IP Address Assignment', 'Advanced Settings', 'Network Access Restrictions', 'Max Sessions', 'Usage Quotas', 'Account Disable', 'Downloadable ACLs', 'Advanced TACACS+ Settings', 'TACACS+ Enable Control', 'TACACS+ Enable Password', 'TACACS+ Outbound Password', 'TACACS+ Shell Command Authorization', 'Command Authorization for Network Device Management Applications', 'TACACS+ Unknown Services', 'IETF RADIUS Attributes', and 'RADIUS Vendor-Specific Attributes'.

6. Choose **Wireless Services** > **AP**, and click **Enable** for the Participate in SWAN infrastructure option. Then type the WDS Username and Password.

You must define a WDS user name and password on the authentication server for all devices that you designate members of the WDS.

Cisco Systems

Cisco 1200 Access Point

Hostname: WDS_AP 16:00:29 Fri Apr 23 2004

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
NETWORK INTERFACES
SECURITY
SERVICES
WIRELESS SERVICES
AP
WDS
SYSTEM SOFTWARE
EVENT LOG

Wireless Services: AP

Participate in SWAN Infrastructure: ☒ Enable ☐ Disable

WDS Discovery: ☒ Auto Discovery
☐ Specified Discovery: (IP Address)

Username:
Password:
Confirm Password:

L3 Mobility Service via IP/GRE Tunnel: ☐ Enable ☒ Disable

Apply Cancel

Alternatively, issue these commands from the CLI:

```
WDS_AP#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

WDS_AP(config)#wlccp ap username wdsap password wdsap

WDS_AP(config)#end

WDS_AP#write memory
```

7. Choose **Wireless Services > WDS**. On the WDS AP WDS Status tab, check whether the WDS AP appears in the WDS Information area, in the ACTIVE State. The AP must also appear in the AP Information area, with State as REGISTERED.
 - a. If the AP does not appear REGISTERED or ACTIVE, check the authentication server for any errors or failed authentication attempts.
 - b. When the AP registers appropriately, add an infrastructure AP to use the services of the WDS.

Alternatively, issue these commands from the CLI:

```
WDS_AP#show wlccp wds ap

      MAC-ADDR      IP-ADDR      STATE      LIFETIME
0005.9a38.429f      10.0.0.102      REGISTERED      261

WDS_AP#show wlccp ap

WDS = 0005.9a38.429f, 10.0.0.102
state = wlccp_ap_st_registered
IN Authenticator = 10.0.0.102
MN Authenticator = 10.0.0.102

WDS_AP#
```

Note: You cannot test client associations because client authentication does not have provisions yet.

Designate a WLSM as WDS

This section explains how to configure a WLSM as a WDS. The WDS is the only device that communicates with the authentication server.

Note: Issue these commands at the enable command prompt of the WLSM, not of the Supervisor Engine 720. In order to get to the command prompt of the WLSM, issue these commands at an enable command prompt in the Supervisor Engine 720:

```
c6506#session slot x proc 1
```

!--- In this command, x is the slot number where the WLSM resides.

The default escape character is Ctrl-^, then x.

You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.51 ... Open

User Access Verification

Username: <username>

Password: <password>

wlan>**enable**

Password: <enable password>

wlan#

Note: In order to troubleshoot and maintain your WLSM more easily, configure Telnet remote access to the WLSM. Refer to Configuring Telnet Remote Access.

In order to designate a WLSM as WDS:

1. From the CLI of the WLSM, issue these commands, and establish a relationship with the authentication server:

```
wlan#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
wlan(config)#aaa new-model
```

```
wlan(config)#aaa authentication login leap-devices group radius
```

```
wlan(config)#aaa authentication login default enable
```

```
wlan(config)#radius-server host ip_address_of_authentication_server  
auth-port 1645 acct-port 1646
```

!--- This command needs to be on one line.

```
wlan(config)#radius-server key shared_secret_with_server
```

```
wlan(config)#end
```

```
wlan#write memory
```

Note: There is no priority control in the WLSM. If the network contains multiple WLSM modules, WLSM uses redundancy configuration in order to determine the primary module.

2. Configure the WLSM in the authentication server as an AAA client.

In Cisco Secure ACS, this occurs on the Network Configuration page where you define these attributes for the WLSM:

- ◆ Name
- ◆ IP address
- ◆ Shared secret
- ◆ Authentication method

◇ RADIUS Cisco Aironet

◇ RADIUS IETF

For other non-ACS authentication servers, refer to the documentation from the manufacturer.

Network Configuration

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Key:

Authenticate Using:

☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

☐ Log Update/Watchdog Packets from this AAA Client

☐ Log RADIUS Tunneling Packets from this AAA Client

☐ Replace RADIUS Port info with Username from this AAA Client

Help

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

- a. Also, in Cisco Secure ACS, configure ACS to perform LEAP authentication on the System Configuration – Global Authentication Setup page. First, click **System Configuration**, then click **Global Authentication Setup**.

System Configuration

Select

- [Service Control](#)
- [Logging](#)
- [Date Format Control](#)
- [Local Password Management](#)
- [CiscoSecure Database Replication](#)
- [ACS Backup](#)
- [ACS Restore](#)
- [ACS Service Management](#)
- [IP Pools Server](#)
- [IP Pools Address Recovery](#)
- [ACS Certificate Setup](#)
- [Global Authentication Setup](#)

Help

- [Service Control](#)
- [Logging](#)
- [Date Format Control](#)
- [Local Password Management](#)
- [CiscoSecure Database Replication](#)
- [RDBMS Synchronization](#)
- [ACS Backup](#)
- [ACS Restore](#)
- [ACS Service Management](#)
- [IP Pools Address Recovery](#)
- [IP Pools Server](#)
- [VoIP Accounting Configuration](#)
- [ACS Certificate Setup](#)
- [Global Authentication Configuration](#)

Service Control

Select to open the page from which you can stop or restart Cisco Secure ACS services.

[\[Back to Top\]](#)

- b. Scroll down the page to the LEAP setting. When you check the box, ACS authenticates LEAP.

CISCO SYSTEMS

System Configuration

Edit

Global Authentication Setup

EAP Configuration

PEAP

- ☒ Allow EAP-MSCHAPv2
- ☒ Allow EAP-GTC
- Cisco client initial message: from 10.0.0.3
- PEAP session timeout (minutes): 120
- Enable Fast Reconnect: ☒

EAP-FAST

- ☒ Allow EAP-FAST
- Active master key TTL: 1 months
- Retired master key TTL: 3 months
- PAC TTL: 1 weeks
- Client initial message:
- Authority ID Info: eironetlab.net
- Allow automatic PAC provisioning: ☐
- EAP-FAST master server: ☒
- Actual EAP-FAST server status: Master

EAP-TLS

- ☒ Allow EAP-TLS
- Select one or more of the following options:
 - ☒ Certificate SAN comparison
 - ☒ Certificate CN comparison
 - ☒ Certificate Binary comparison
- EAP-TLS session timeout (minutes): 120

LEAP

- ☒ Allow LEAP (For Aironet only)

EAP-MD5

- ☒ Allow EAP-MD5
- AP EAP request timeout (seconds): 20

MS-CHAP Configuration

- ☒ Allow MS-CHAP Version 1 Authentication
- ☒ Allow MS-CHAP Version 2 Authentication

Back to Help

Submit Submit + Restart Cancel

Help

- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP EAP request timeout](#)
- [MS-CHAP Configuration](#)

This page specifies settings for various authentication protocols.

[Back to Top](#)

PEAP

Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have

3. On the WLSM, define a method that authenticates the other APs (an infrastructure server group).

```
wlan#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
wlan(config)#wlccp authentication-server infrastructure leap-devices

wlan(config)#end
wlan#write memory
```

4. On the WLSM, define a method that authenticates the client devices (a client server group) and what EAP types those clients use.

```
wlan#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
wlan(config)#wlccp authentication-server client any leap-devices

wlan(config)#end
wlan#write memory
```

Note: This step eliminates the need for the Define Client Authentication Method process.

5. Define a unique VLAN between the Supervisor Engine 720 and the WLSM in order to allow the WLSM to communicate with outside entities like APs and authentication servers. This VLAN is unused anywhere else or for any other purpose on the network. Create the VLAN on the Supervisor Engine 720 first, then issue these commands:

- ◆ On the Supervisor Engine 720:

```
c6506#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
c6506(config)#wlan module slot_number allowed-vlan vlan_number

c6506(config)#vlan vlan_number

c6506(config)#interface vlan vlan_number

c6506(config-if)#ip address ip_address subnet_mask

c6506(config-if)#no shut
c6506(config)#end
c6506#write memory
```

- ◆ On the WLSM:

```
wlan#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
wlan(config)#wlan vlan vlan_number

wlan(config)#ipaddr ip_address subnet_mask

wlan(config)#gateway ip_address_of_vlan_interface_on_Sup720_created_above

wlan(config)#ip route 0.0.0.0 0.0.0.0

!--- This is typically the same address as the gateway statement.

wlan(config)#admin
wlan(config)#end
wlan#write memory
```

6. Verify the function of the WLSM with these commands:

- ◆ On the WLSM:

```
wlan#show wlccp wds mobility

LCP link status: up
HSRP state: Not Applicable
Total # of registered AP: 0
Total # of registered MN: 0

Tunnel Bindings:
```


Network ID	Tunnel IP	MTU	FLAGS
=====	=====	=====	=====
<vlan>	<ip address>	1476	T

Flags: T=Trusted, B=IP Broadcast enabled, N=Nonexistent
wlan#

- ◆ On the Supervisor Engine 720:

```
c6506#show mobility status
WLAN Module is located in Slot: 5 (HSRP State: Active)
LCP Communication status      : up
Number of Wireless Tunnels    : 0
Number of Access Points       : 0
Number of Access Points       : 0
```

Designate an AP as Infrastructure Device

Next, you must designate at least one infrastructure AP and relate the AP to the WDS. The clients associate to infrastructure APs. The infrastructure APs request the WDS AP or WLSM to perform authentication for them.

Complete these steps in order to add an infrastructure AP that uses the services of the WDS:

Note: This configuration applies only to the infrastructure APs and not the WDS AP.

1. Choose **Wireless Services > AP**. On the infrastructure AP, select **Enable** for the Wireless Services option. Then type the WDS Username and Password.

You must define a WDS user name and password on the authentication server for all devices that are to be members of the WDS.

Cisco 1200 Access Point

Hostname: infrastructure_AP 10:00:26 Mon Apr 26 2004

Wireless Services: AP

Participate in SWAN Infrastructure: ☒ Enable ☐ Disable

WDS Discovery: ☒ Auto Discovery ☐ Specified Discovery: (IP Address)

Username:
 Password:
 Confirm Password:

L3 Mobility Service via IP/GRE Tunnel: ☐ Enable ☒ Disable

Apply Cancel

Alternatively, issue these commands from the CLI:

```
WDS_AP#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Infrastructure_AP(config)#wlccp ap username infrastructureap password infrastructureap
```

```
Infrastructure_AP(config)#end
```

```
Infrastructure_AP#write memory
```

2. Choose **Wireless Services > WDS**. On the WDS AP WDS Status tab, the new infrastructure AP appears in the WDS Information area, with State as ACTIVE, and in the AP Information area, with State as REGISTERED.
 - a. If the AP does not appear ACTIVE and/or REGISTERED, check the authentication server for any errors or failed authentication attempts.
 - b. After the AP appears ACTIVE and/or REGISTERED, add a client authentication method to the WDS.

MAC Address	IP Address	Priority	State
0005.9a38.429f	10.0.0.102	254	Administratively StandAlone - ACTIVE

MAC Address	IP Address	State
000c.8547.b6c7	10.0.0.108	REGISTERED
0005.9a38.429f	10.0.0.102	REGISTERED

Alternatively, issue this command from the CLI:

```
WDS_AP#show wlccp wds ap
```

MAC-ADDR	IP-ADDR	STATE	LIFETIME
000c.8547.b6c7	10.0.0.108	REGISTERED	194
0005.9a38.429f	10.0.0.102	REGISTERED	76

Alternatively, issue this command from the WLSM:

```
wlan#show wlccp wds ap
      MAC-ADDR      IP-ADDR      STATE      LIFETIME
000c.8547.b6c7      10.0.0.108      REGISTERED      194
0005.9a38.429f      10.0.0.102      REGISTERED      76
wlan#
```

Then, issue this command on the infrastructure AP:

```
Infrastructure_AP#show wlccp ap

WDS = 0005.9a38.429f, 10.0.0.102
state = wlccp_ap_st_registered
IN Authenticator = 10.0.0.102
MN Authenticator = 10.0.0.102

Infrastructure_AP#
```

Note: You cannot test client associations because client authentication does not have provisions yet.

Define Client Authentication Method

Finally, define a method of client authentication.

Complete these steps in order to add a client authentication method:

1. Choose **Wireless Services > WDS**. Perform these steps on the WDS AP Server Groups tab:
 - a. Define a server group that authenticates clients (a Client group).
 - b. Set Priority 1 to the previously configured authentication server.
 - c. Set the applicable type of authentication (LEAP, EAP, MAC, and so forth).
 - d. Apply the settings to the relevant SSIDs.

The image shows the Cisco 1200 Access Point configuration interface. The top navigation bar includes 'HOME', 'EXPRESS SET-UP', 'EXPRESS SECURITY', 'NETWORK MAP', 'ASSOCIATION', 'NETWORK INTERFACES', 'SECURITY', 'SERVICES', 'WIRELESS SERVICES', 'AP', 'WDS', 'SYSTEM SOFTWARE', and 'EVENT LOG'. The 'WDS STATUS' tab is selected, showing 'Hostname WDS_AP' and the date '10:23:43 Mon Apr 26 2004'.

The main configuration area is titled 'Wireless Services: WDS - Server Groups'. It contains a 'Server Group List' with a table showing a single entry 'Client' with a 'Delete' button next to it. To the right of the list, the 'Server Group Name' is set to 'Client'. Below this, 'Group Server Priorities' are defined: 'Priority 1' is '10.0.0.3', 'Priority 2' is '< NONE >', and 'Priority 3' is '< NONE >'. A 'Define Servers' link is also present.

Under 'Use Group For:', 'Client Authentication' is selected. This section includes 'Authentication Settings' with checkboxes for 'EAP Authentication' (checked), 'LEAP Authentication' (checked), 'MAC Authentication' (unchecked), and 'Default (Any) Authentication' (unchecked). To the right, 'SSID Settings' are configured with 'Apply to all SSIDs' selected and 'Restrict SSIDs' (Apply only to listed SSIDs) unselected. The 'SSID' field is set to 'DISABLED', and there are 'Add' and 'Remove' buttons.

At the bottom right, there are 'Apply' and 'Cancel' buttons.

Alternatively, issue these commands from the CLI:

```
WDS_AP#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

WDS_AP(config)#wlccp authentication-server client eap method_Client
WDS_AP(config)#wlccp authentication-server client leap method_Client
WDS_AP(config)#aaa group server radius Client
WDS_AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646
WDS_AP(config-sg-radius)#exit
WDS_AP(config)#aaa authentication login method_Client group Client
WDS_AP(config)#end
WDS_AP#write memory
```

Note: The example WDS AP is dedicated and does not accept client associations.

Note: Do not configure on the infrastructure APs for server groups because infrastructure APs forward any requests to the WDS to be processed.

2. On the infrastructure AP or APs:

- a. Under the **Security > Encryption Manager** menu item, click **WEP Encryption** or **Cipher**, as required by the authentication protocol you use.

Cisco Systems Cisco 1200 Access Point

RADIO0-802.11B RADIO1-802.11A

Hostname Infrastructure_AP 10:36:59 Mon Apr 26 2004

Security: Encryption Manager - Radio0-802.11B

Encryption Modes

☐ None

☒ **WEP Encryption** Mandatory

Cisco Compliant TKIP Features: ☐ Enable MIC ☐ Enable Per Packet Keying

☐ Cipher WEP 128 bit

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit

- b. Under the **Security > SSID Manager** menu item, select authentication methods as required by the authentication protocol you use.

The screenshot displays the Cisco 1200 Access Point configuration interface. The top navigation bar includes the Cisco Systems logo, the title "Cisco 1200 Access Point", and a user icon. Below this, tabs for "RADIO0-802.11B" and "RADIO1-802.11A" are visible. The left sidebar contains a menu with options like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, Admin Access, Encryption Manager, SSID Manager (highlighted), Server Manager, Local RADIUS Server, Advanced Security, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG.

The main content area shows the "Security: SSID Manager - Radio0-802.11B" section. It includes a "Current SSID List" with a table containing one entry: "infraSSID". To the right of the list are input fields for "SSID:" (set to "infraSSID"), "VLAN:" (set to "< NONE >"), and "Network ID:" (set to "0-4096"). Below these are "Delete-Radio0" and "Delete-All" buttons.

The "Authentication Settings" section is highlighted with a red box. It contains a "Methods Accepted:" section with three options:

- ☒ Open Authentication: with EAP (dropdown)
- ☐ Shared Authentication: < NO ADDITION > (dropdown)
- ☒ Network EAP: < NO ADDITION > (dropdown)

3. You can now successfully test whether clients authenticate to infrastructure APs. The AP of the WDS in the WDS Status tab (under the **Wireless Services** > **WDS** menu item) indicates that the client appears in the Mobile Node Information area and has a REGISTERED State.

If the client does not appear, check the authentication server for any errors or failed authentication attempts by the clients.

Cisco 1200 Access Point

WDS STATUS | SERVER GROUPS | GENERAL SET-UP

Hostname WDS_AP 10:49:24 Mon Apr 26 2004

Wireless Services: WDS - Wireless Domain Services - Status

WDS Information

MAC Address	IP Address	Priority	State
0005.9a38.429f	10.0.0.102	254	Administratively StandAlone - ACTIVE

WDS Registration

APs: 2 Mobile Nodes: 1

AP Information

MAC Address	IP Address	State
000c.8547.b6c7	10.0.0.108	REGISTERED
0005.9a38.429f	10.0.0.102	REGISTERED

Mobile Node Information

MAC Address	IP Address	State	SSID	VLAN ID	BSSID
0030.6527.f74a	10.0.0.25	REGISTERED	infraSSID	-	0007.85b4.113b

Wireless Network Manager Information

IP Address	Authentication Status

Refresh

Alternatively, issue these commands from the CLI:

```
WDS_AP#show wlcgp wds

      MAC: 0005.9a38.429f, IP-ADDR: 10.0.0.102      , Priority: 254
      Interface BV11, State: Administratively StandAlone - ACTIVE
      AP Count: 2      , MN Count: 1

WDS_AP#show wlcgp wds mn

      MAC-ADDR      IP-ADDR      Cur-AP      STATE
0030.6527.f74a  10.0.0.25      000c.8547.b6c7      REGISTERED

WDS_AP#
```

Note: If you need to debug authentication, ensure that you debug on the WDS AP, because the WDS AP is the device that communicates with the authentication server.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information that you can use to troubleshoot your configuration. This list shows some of the common questions related to the WDS command in order to further clarify the usefulness of these commands:

- **Question: On the WDS AP, what are the recommended settings for these items?**

- ◆ **radius-server timeout**
- ◆ **radius-server deadtime**
- ◆ **Temporal Key Integrity Protocol (TKIP) message integrity check (MIC) Failure Holdoff Time**
- ◆ **Client Holdoff Time**
- ◆ **EAP or MAC Reauthentication Interval**
- ◆ **EAP Client Timeout (optional)**

Answer: It is suggested that you keep the configuration with default settings regarding these special settings, and only use them when there is a problem regarding timing.

These are the recommended settings for the WDS AP:

- ◆ Disable **radius-server timeout**. This is the number of seconds an AP waits for a reply to a RADIUS request before it resends the request. The default is 5 seconds.
 - ◆ Disable **radius-server deadtime**. The RADIUS is skipped by additional requests for the duration of minutes unless all servers are marked dead.
 - ◆ TKIP MIC Failure Holdoff Time is enabled by default to 60 seconds. If you enable holdoff time, you can enter the interval in seconds. If the AP detects two MIC failures within 60 seconds, it blocks all TKIP clients on that interface for the holdoff time period specified here.
 - ◆ Client Holdoff Time should be disabled by default. If you enable holdoff, enter the number of seconds that the AP should wait after an authentication failure before a subsequent authentication request is processed.
 - ◆ EAP or MAC Reauthentication Interval is disabled by default. If you enable reauthentication, you can specify the interval or accept the interval given by the authentication server. If you choose to specify the interval, enter the interval in seconds that the AP waits before it forces an authenticated client to reauthenticate.
 - ◆ EAP Client Timeout (optional) is 120 seconds by default. Enter the amount of time the AP should wait for wireless clients to respond to EAP authentication requests.
- **Question: In regards to TKIP holdoff time, I read that this should be set to 100 ms and not 60 seconds. I assume it is set to one second from the browser because that is the lowest number you can select?**

Answer: There is no specific recommendation to set it to 100 ms unless there is a failure reported where the only solution is to increase this time. One second is the lowest setting.

- **Question: Do these two commands help client authentication in any way and are they needed on the WDS or infrastructure AP?**

- ◆ **radius-server attribute 6 on-for-login-auth**
- ◆ **radius-server attribute 6 support-multiple**

Answer: These commands do not help the authentication process and they are not needed on the WDS or the AP.

- **Question: On the infrastructure AP, I assume that none of the Server Manager and Global Properties settings are needed because the AP receives information from the WDS. Are any of these specific commands needed for the infrastructure AP?**

- ◆ **radius-server attribute 6 on-for-login-auth**
- ◆ **radius-server attribute 6 support-multiple**
- ◆ **radius-server timeout**
- ◆ **radius-server deadtime**

Answer: There is no need to have Server Manager and Global Properties for the infrastructure APs. The WDS takes care of that task and there is no need to have these settings:

- ◆ **radius-server attribute 6 on-for-login-auth**
- ◆ **radius-server attribute 6 support-multiple**
- ◆ **radius-server timeout**
- ◆ **radius-server deadtime**

The **radius-server attribute 32 include-in-access-req format %h** setting remains by default and is required.

An AP is a Layer 2 device. Therefore, the AP does not support Layer 3 mobility when the AP is configured to act as a WDS device. You can achieve Layer 3 mobility only when you configure the WLSM as the WDS device. Refer to the *Layer 3 Mobility Architecture* section of Cisco Catalyst 6500 Series Wireless LAN Services Module: White Paper for more information.

Therefore, when you configure an AP as a WDS device, do not use the **mobility network-id** command. This command applies to Layer 3 mobility and you need to have a WLSM as your WDS device in order to properly configure Layer 3 mobility. If you use the **mobility network-id** command incorrectly, you can see some of these symptoms:

- Wireless clients cannot associate with the AP.
- Wireless clients can associate to the AP, but do not receive an IP address from the DHCP server.
- A wireless phone is not authenticated when you have a voice over WLAN deployment.
- EAP authentication does not occur. With the **mobility network-id** configured, the AP tries to build a Generic Routing Encapsulation (GRE) tunnel to forward EAP packets. If no tunnel is established, the packets do not go anywhere.
- An AP configured as a WDS device does not function as expected, and the WDS configuration does not work.

Note: You cannot configure the Cisco Aironet 1300 AP/Bridge as a WDS master. The 1300 AP/Bridge does not support this functionality. The 1300 AP/Bridge can participate in a WDS network as an infrastructure device in which some other AP or WLSM is configured as a WDS master.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug dot11 aaa authenticator all** Shows the various negotiations that a client goes through as the client associates and authenticates through the 802.1x or EAP process. This debug was introduced in Cisco IOS Software Release 12.2(15)JA. This command obsoletes **debug dot11 aaa dot1x all** in that and later releases.
- **debug aaa authentication** Shows the authentication process from a generic AAA perspective.
- **debug wlccp ap** Shows the WLCCP negotiations involved as an AP joins a WDS.
- **debug wlccp packet** Shows the detailed information about WLCCP negotiations.
- **debug wlccp leap-client** Shows the details as an infrastructure device joins a WDS.

Related Information

- **Configuring WDS, Fast Secure Roaming, and Radio Management**
- **Catalyst 6500 Series Wireless LAN Services Module Configuration Note**
- **Configuring Cipher Suites and WEP**
- **Configuring Authentication Types**
- **Wireless LAN Support Pages**

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 19, 2009

Document ID: 44720
