



Fast Secure Roaming

The Fast Secure Roaming feature provides the ability for client devices to roam from one access point to another without requiring reauthentication by the main RADIUS server. By streamlining the roaming process, the Fast Secure Roaming feature provides support for client applications, such as VoIP, that require seamless roaming to avoid delays and gaps in transmission.

Feature History for the Fast Secure Roaming Feature

Release	Modification
12.2(11)JA	This feature was introduced on the Cisco IOS Release 12.2(11)JA on Cisco Aironet access points.
12.3(11)T	This feature was integrated into the Cisco IOS Release 12.3(11)T on the Cisco 2600XM, Cisco 2691, Cisco 2851, Cisco 2821, Cisco 2811, Cisco 3700 series, and Cisco 3800 series routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Configuring Fast Secure Roaming, page 2](#)
- [Restrictions for Configuring Fast Secure Roaming, page 2](#)
- [Information About Fast Secure Roaming, page 2](#)
- [How to Configure Fast Secure Roaming, page 5](#)
- [Configuration Examples for Fast Secure Roaming, page 12](#)
- [Additional References, page 17](#)
- [Command Reference, page 18](#)

Prerequisites for Configuring Fast Secure Roaming

To set up fast secure roaming, you must have these items on your wireless LAN:

- At least one access point or wireless-aware router that you can configure as the WDS device
- Cisco Aironet client devices running Cisco client firmware version 5.20.17 or later
- Cisco IOS Release 12.2(11)JA running on the access point and Release 12.3(11)T running on the wireless-aware router

Restrictions for Configuring Fast Secure Roaming

The following are restrictions for configuring the Fast Secure Roaming feature on access points:

- Configure an access point that does not serve a large number of client devices as the wireless domain services (WDS) device.
- Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to fall back to repeater mode in the event of an Ethernet failure.
- The WDS can provide fast secure roaming only among access points within the same broadcast domain.

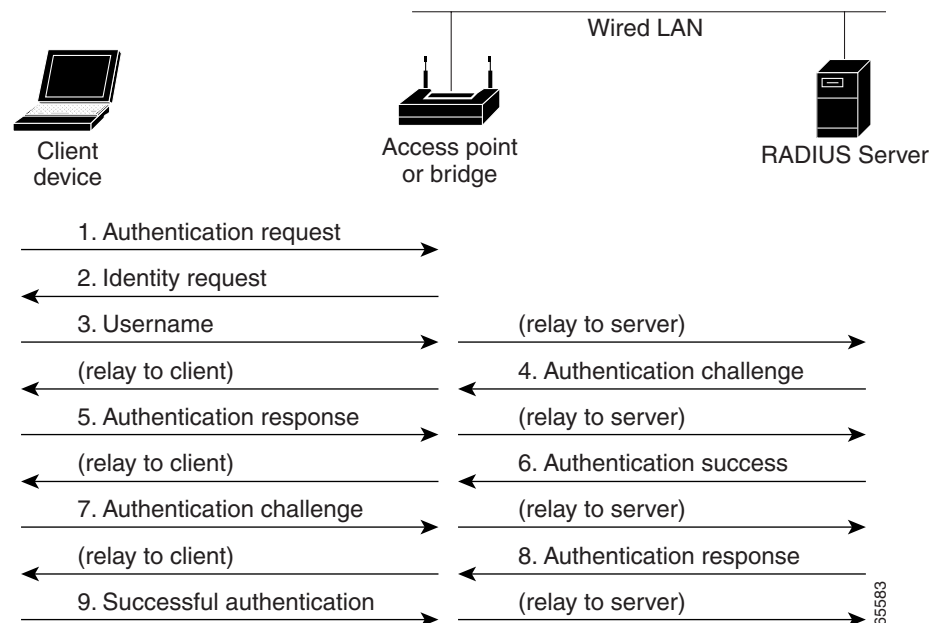
One restriction for a wireless-aware router is that only one instance of WDS can be configured on a router.

Information About Fast Secure Roaming

In many wireless LANs, access points and wireless-aware routers serve mobile client devices that roam from one access point to another. Some applications that run on client devices require fast reassociation when they roam. Voice applications, for example, require seamless roaming to prevent delays and gaps in conversation.

Device Authentication Using a RADIUS Server

In a wireless network, authentication of a client device is performed by an access point to which the client device is attempting to associate. The access point acts as a network access server (NAS) and communicates with the main RADIUS server. [Figure 1](#) depicts client authentication using a RADIUS server.

Figure 1 Client Authentication Using a RADIUS Server

Device Authentication Using CCKM and a WDS Access Point

Fast secure roaming is enabled on a wireless network by configuring a logical entity called the *wireless domain services* (WDS), either on an access point or on a wireless-aware router. The client devices must support the Light Extensible Authentication Protocol (LEAP) and Cisco Centralized Key Management (CCKM) to participate in the fast secure roaming. When you configure your wireless LAN for fast secure roaming, LEAP-enabled client devices roam from one access point to another without involving the main RADIUS server. Typical roaming time is 50 to 100 milliseconds.

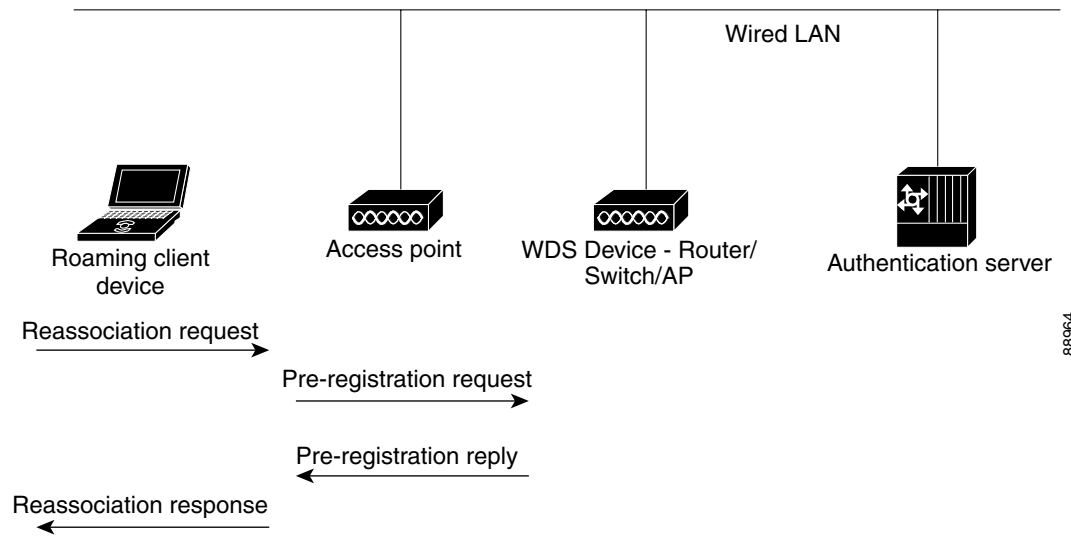


Note

The Fast Secure Roaming feature operates only at Layer 2. All access points must use a single VLAN/subnet for control traffic.

Figure 2 shows client authentication using CCKM.

Figure 2 Client Secure Roaming Using CCKM and a WDS Access Point



The WDS device maintains a cache of credentials for CCKM-capable client devices on a wireless LAN. When a CCKM-capable client roams from one access point to another, the client sends a reassociation request to the new access point, and the new access point relays the request to the WDS device. The WDS device forwards the client's credentials to the new access point, and the new access device sends the reassociation response to the client, reducing the reassociation time. The client also uses the reassociation response to generate the unicast key.

Wireless Domain Services in a Wireless LAN

The WDS device performs several tasks on the wireless LAN:

- Authenticates all access points in the subnet and establishes a secure communication channel with each of them.
- Registers all client devices in the subnet, establishes session keys for them, and caches their security credentials. When a client roams to another access point, the WDS device forwards the client's security credentials to the new access point.
- Advertises its WDS capability and participates in selecting the best WDS device for the wireless LAN. When you configure your wireless LAN for fast secure roaming, you set up one access point or router as the main WDS candidate and one or more additional devices as backup WDS candidates.
- Provides fast secure roaming among access points in the same broadcast domain.

The access points on the wireless LAN interact with the WDS device in these activities:

- Discovering and tracking the current WDS device and relaying WDS advertisements to the wireless LAN.
- Authenticating with the WDS device and establishing a secure communication channel to the WDS device.
- Registering associated client devices with the WDS device.

Table 1 shows the number of access points or clients that can be configured on a WDS device.

Table 1 Maximum Number of Access Points That Can be Configured on a WDS Device

WDS Device	Maximum Number of Access Points
Cisco 2610XM, Cisco 2611XM routers	5
Cisco 2620XM, Cisco 2621XM routers	5
Cisco 2650XM, Cisco 2651XM routers	5
Cisco 2691 routers	10
Cisco 2811 router	10
Cisco 2821 router	10
Cisco 2851 router	20
Cisco 3725 router	25
Cisco 3745 router	50
Cisco 3825 router	50
Cisco 3845 router	100

How to Configure Fast Secure Roaming

This section contains the following procedures:

- [Configuring WDS Devices, page 5](#) (required)
- [Configuring Access Points to Use the WDS Device, page 7](#) (required)
- [Enabling Cipher Suites and WEP for the VLAN on Access Points, page 7](#) (required)
- [Enabling CCKM on Access Points for an SSID, page 8](#) (required)
- [Configuring the Authentication Server to Support LEAP, page 11](#) (required)
- [Verifying the WDS Configuration, page 11](#) (optional)

Configuring WDS Devices

**Note**

For the WDS candidate, configure an access point that does not serve a large number of client devices. If client devices associate to the WDS access point when it starts up, the clients might wait up to several minutes to be authenticated.

**Note**

Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to fall back to repeater mode in case of Ethernet failure.

Perform this task on the access point or wireless-aware router that you want to configure as your primary WDS candidate.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wlccp wds priority *priority* interface *interface***
4. **aaa group server {radius | tacacs+} *group-name***
5. **aaa authentication login *named-authentication-list* group *Server-group name***
6. **wlccp authentication-server infrastructure *list***
7. **wlccp authentication-server client [any | eap | leap | mac] *list***
8. **end**
9. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	Router> enable	Enables privileged EXEC mode.
Step 2	Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# wlccp wds priority <i>priority</i> interface <i>interface</i>	Enables the access point or wireless-aware router as a WDS device candidate. <ul style="list-style-type: none"> • Priority—Sets the priority (from 1 to 255) of this WDS candidate. The WDS candidate with the highest priority number becomes the active WDS device. • Interface—Sets the interface on which the access point or router sends out WDS advertisements. For a list of supported interfaces, see “wlccp wds priority interface” in the “Command Reference” section on page 18.
Step 4	Router(config)# aaa group server {radius tacacs+} <i>group-name</i>	Defines the AAA server group with a group name
Step 5	Router(config)# aaa authentication login <i>named-authentication-list</i> group <i>Server-group name</i>	Creates an authentication method list for the server group.
Step 6	Router(config)# wlccp authentication-server infrastructure <i>list</i>	Configures the list of servers to be used for 802.1x authentication for your wireless infrastructure devices, such as access points, wireless-aware routers, and repeaters.
Step 7	Router(config)# wlccp authentication-server client [any eap leap mac] <i>list</i>	Configures the list of servers to be used for 802.1X authentication for client devices. You can specify a separate list for clients using a certain type of authentication, such as Extensible Authentication Protocol (EAP), LEAP, or MAC-based, or specify a list for client devices using any type of authentication.
Step 8	Router(config)# end	Returns to privileged EXEC mode.
Step 9	Router# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Use the **no** form of the **wlccp wds** command to remove the access point or router from the list of WDS device candidates. Use the **no** form of the **wlccp authentication-server** commands to disable the server lists.

Configuring Access Points to Use the WDS Device

To configure an access point to authenticate through the WDS device and to participate in CCKM, enter the following command in global configuration mode:

```
AP(config)# wlccp ap username username password [0 | 7] password
```

Enter the username and password that the access point uses to authenticate to the network. The 0 or 7 option determines whether the device password is encrypted (7) or unencrypted (0).

Use the **no** form of the command to disable participation in CCKM.

Enabling Cipher Suites and WEP for the VLAN on Access Points

Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN. You must use a cipher suite to enable Wi-Fi Protected Access (WPA) or CCKM. Because cipher suites provide the protection of Wired Equivalent Privacy (WEP) while also allowing use of authenticated key management, it is recommended that you enable WEP by using the **encryption mode cipher** command in the command-line interface (CLI) or by using the cipher drop-down menu. Cipher suites that contain Temporal Key Integrity Protocol (TKIP) provide the best security for your wireless LAN, and cipher suites that contain only WEP are the least secure.

If you configure an access point to use WPA or CCKM authenticated key management, you must select a cipher suite compatible with the authenticated key management type. [Table 2](#) lists the cipher suites that are compatible with WPA and CCKM.

Table 2 Cipher Suites That Are Compatible with WPA and CCKM

Authenticated Key Management Types	Compatible Cipher Suites
CCKM	<ul style="list-style-type: none"> • Encryption mode cipher wep128 • Encryption mode cipher wep40 • Encryption mode cipher ckip • Encryption mode cipher cmic • Encryption mode cipher ckip-cmic • Encryption mode cipher tkip • Encryption mode cipher tkip wep128 • Encryption mode cipher tkip wep40
WPA	<ul style="list-style-type: none"> • Encryption mode cipher tkip • Encryption mode cipher tkip wep128 • Encryption mode cipher tkip wep40

Perform the following task to enable a cipher suite on an access point.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11radio [0 | 1]**
4. **encryption [vlan *vlan-id*] mode cipher {ckip | cmic | ckip-cmic | tkip} {wep128 | wep40}**
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	AP> enable	Enables privileged EXEC mode.
Step 2	AP# configure terminal	Enters global configuration mode.
Step 3	AP(config)# interface dot11radio [0 1]	Enters interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 4	AP(config-if)# encryption [vlan <i>vlan-id</i>] mode cipher {ckip cmic ckip-cmic tkip} {wep128 wep40}	<p>Enables a cipher suite that contains the WEP protection that you need.</p> <ul style="list-style-type: none"> • (Optional) Select the VLAN for which you want to enable WEP and WEP features. • Set the cipher options and WEP level. You can combine TKIP with 128-bit or 40-bit WEP. <p>Note If you enable a cipher suite with two elements (such as TKIP and 128-bit WEP), the second cipher becomes the group cipher.</p> <p>Note You can also use the encryption mode wep command to set up static WEP. However, you should use encryption mode wep only if none of the clients that associate to the device is capable of key management.</p>
Step 5	AP(config-if)# end	Returns to privileged EXEC mode.
Step 6	AP# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Use the **no** form of the encryption command to disable a cipher suite.

Enabling CCKM on Access Points for an SSID

Perform this task to enable access points on the subnet to allow CCKM authenticated key management for at least one SSID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **interface dot11radio** [0|1]
4. **ssid** *ssid-string*
5. **authentication open** [*mac-address list-name* [**alternate**]][**eap** *list-name*]
6. **authentication shared** [*mac-address list-name*][**eap** *list-name*]
7. **authentication network-eap** *list-name* [*mac-address list-name*]
8. **authentication key-management** {**cckm** | **wpa**} [**optional**]
9. **end**
10. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	AP> enable	Enables privileged EXEC mode.
Step 2	AP# configure terminal	Enters global configuration mode.
Step 3	AP(config-if)# interface dot11radio {0 1}	Enters interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 4	AP(config-if)# ssid <i>ssid-string</i>	Creates a service set identifier (SSID) and enters SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. Note Do not include spaces in SSIDs.
Step 5	AP(config-if)# authentication open [<i>mac-address list-name</i> [alternate]] [eap <i>list-name</i>]	(Optional) Sets the authentication type to <i>open</i> for this SSID. Open authentication allows any device to authenticate and then attempt to communicate with the access point or router. <ul style="list-style-type: none"> • (Optional) Sets the SSID authentication type to open with MAC address authentication. The access point or router forces all client devices to perform MAC address authentication before these devices are allowed to join the network. For <i>list-name</i>, specify the authentication method list. Click this link for more information on method lists: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2 Use the alternate keyword to allow client devices that are using either MAC or EAP authentication to join the network. Clients that successfully complete either type of authentication are allowed to join the network. • (Optional) Sets the SSID authentication type to open with EAP authentication. The access point or router forces all client devices to perform EAP authentication before they are allowed to join the network. For <i>list-name</i>, specify the authentication method list. Note An access point or router that is configured for EAP authentication forces all client devices that associate to perform EAP authentication. Client devices that do not use EAP cannot use the access point or router.

	Command	Purpose
Step 6	<pre>AP(config-if)# authentication shared [mac-address list-name] [eap list-name]</pre>	<p>(Optional) Sets the authentication type for the SSID to shared key.</p> <p>Note Because of security flaws in shared key authentication, we recommend that you avoid using it.</p> <p>Note You can assign shared key authentication to only one SSID.</p> <ul style="list-style-type: none"> (Optional) Sets the SSID authentication type to shared key with MAC address authentication. For <i>list-name</i>, specify the authentication method list. (Optional) Sets the SSID authentication type to shared key with EAP authentication. For <i>list-name</i>, specify the authentication method list.
Step 7	<pre>AP(config-if)# authentication network-eap list-name [mac-address list-name]</pre>	<p>(Optional) Sets the authentication type for the SSID to network EAP. By using the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server, the access point or router helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. However, the access point or router does not force all client devices to perform EAP authentication.</p> <ul style="list-style-type: none"> (Optional) Sets the SSID authentication type to network EAP with MAC address authentication. All client devices that associate to the access point or router are required to perform MAC address authentication. For <i>list-name</i>, specify the authentication method list.
Step 8	<pre>AP(config-if)# authentication key-management {cckm wpa} [optional]</pre>	<p>(Optional) Sets the authentication type for the SSID to CCKM or WPA. If you use the optional keyword, client devices that use authentication methods other than CCKM and WPA will be able to use this SSID. If you do not use the optional keyword, only the client devices that use CCKM or WPA will be allowed to use the SSID.</p> <p>To enable CCKM for an SSID, you must also enable network EAP authentication. To enable WPA for an SSID, you must also enable Open authentication or network EAP or both.</p> <p>Note Before you can enable CCKM or WPA, you must set the encryption mode for the SSID VLAN to one of the cipher suite options.</p> <p>Note If you enable WPA for an SSID without a preshared key, the key management type is WPA. If you enable WPA with a preshared key, the key management type is WPA-PSK.</p>
Step 9	<pre>AP(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 10	<pre>AP# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Use the **no** form of the SSID commands to disable the SSID or to disable SSID features.

Configuring the Authentication Server to Support LEAP

The WDS device should be configured as a valid network access server (NAS) on the authentication server. The access points must authenticate to the authentication server. On the authentication server, you must configure usernames and passwords for the access points and clients.

If your authentication server runs Cisco Secure ACS, go to the following location for documentation about Cisco Secure ACS:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/index.htm

Verifying the WDS Configuration

Use the following commands to view information about the current WDS device and other wireless devices participating in CCKM.

	Command	Purpose
Step 1	AP> enable or Router> enable	Enables privileged EXEC mode.
Step 2	AP# show wlccp ap	For access points only. On devices participating in CCKM, displays the WDS device's MAC address, the WDS device's IP address, the access point's state (authenticating, authenticated, or registered), the IP address of the infrastructure authenticator, and the IP address of the client device or mobile node (MN) authenticator.
Step 3	Router# show wlccp wds {ap mn} [detail] [mac-addr mac-address]	<p>On the WDS device only, displays cached information about access points, wireless-aware routers, and client devices.</p> <ul style="list-style-type: none"> • ap—Displays access points and routers participating in CCKM. The command displays each access point's MAC address, IP address, state (authenticating, authenticated, or registered), and lifetime (seconds remaining before the access point must reauthenticate). • mn—Displays cached information about client devices, also called <i>mobile nodes</i>. The command displays each client's MAC address, IP address, the access point or router to which the client is associated, and state (authenticating, authenticated, or registered). • detail—Displays the client's lifetime (seconds remaining before the client must reauthenticate), SSID, and VLAN ID. • mac-addr—Displays information about a specific access point or router. <p>If you just enter show wlccp wds, without entering any options, the command displays the access point's IP address, MAC address, priority, and interface state (administratively standalone, active, backup, or candidate). For the backup interface state, the command also displays the current WDS access point's IP address, MAC address, and priority.</p>

Configuration Examples for Fast Secure Roaming

This section provides the following configuration examples:

- [Setting Up a WDS Candidate: Example](#)
- [Setting Up Cipher Suite: Example](#)
- [Setting Up CCKM Authentication: Example](#)
- [Configuration on a Cisco Access Point: Example](#)
- [Configuration on Cisco a 3745 Router: Example](#)

Setting Up a WDS Candidate: Example

This example shows how to set up a high-priority WDS access point candidate that uses different server lists for authenticating infrastructure devices, client devices using LEAP, and client devices using MAC-based authentication:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# wlccp wds priority 100 interface bvi1
Router(config)# wlccp authentication-server infrastructure wlan-list1
Router(config)# wlccp authentication-server client leap leap-list1
Router(config)# wlccp authentication-server client mac mac-list1
Router(config)# end
```

Setting Up Cipher Suite: Example

This example (for access points only) sets up a cipher suite for VLAN 22 that enables CKIP, CMIC, and 128-bit WEP.

```
AP# configure terminal
AP(config)# configure interface dot11radio 0
AP(config-if)# encryption vlan 22 mode cipher ckip-cmic wep128
AP(config-if)# end
```

Setting Up CCKM Authentication: Example

This example sets the authentication type for the SSID *batman* to network EAP with CCKM authentication. Client devices that use the *batman* SSID will authenticate by using the *adam* server list. After they are authenticated, CCKM-enabled clients can perform fast reassociation using CCKM.

```
ap1200# configure terminal
ap1200(config)# configure interface dot11radio 0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management cckm optional
ap1200(config-ssid)# end
```

Configuration on a Cisco Access Point: Example

```
AP2# show run
Building configuration...

Current configuration : 1589 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AP2
!
aaa new-model
!
!
aaa group server radius LEAP_GROUP
 server 20.0.0.100 auth-port 1812 acct-port 1813
!
aaa authentication login AUTH_LEAP group LEAP_GROUP
aaa session-id common
enable secret 5 $1$Y8Mb$AEKQ17Fv8KBxbWWLoVGfg.
enable password 7 151EOA0E
!
username Cisco password 7 05280F1C2243
ip subnet-zero
!
!
bridge irb
!
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption mode ciphers wep128
 !
 ssid 802.11a1
 authentication network-eap AUTH_LEAP
 authentication key-management cckm optional
 !
 ssid tsunami
 authentication open
 guest-mode
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 rts threshold 2312
 power client 5
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unk
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
 !
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
```

```

bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface BVI1
ip address 20.0.0.102 255.0.0.0
no ip route-cache
!
ip http server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
bridge 1 route ip
!
wlccp authentication-server infrastructure AUTH_LEAP
wlccp ap username ap2 password 7 050A165D
!
line con 0
exec-timeout 0 0
privilege level 15
line vty 5 15
!
end

```

Configuration on Cisco a 3745 Router: Example

```

c3745# show run
Building configuration...

Current configuration : 3801 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname c3745
!
!
aaa new-model
!
!
aaa group server radius LEAP_GROUP
server 20.0.0.100 auth-port 1812 acct-port 1813
!
aaa authentication login LEAP group LEAP_GROUP
aaa session-id common
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
mpls ldp logging neighbor-changes
no ftp-server write-enable
no scripting tcl init
no scripting tcl encdir
!
!
!
!
!

```

```
!  
!  
!  
!  
!  
no voice hpi capture buffer  
no voice hpi capture destination  
!  
!  
!  
!  
!  
interface FastEthernet0/0  
  ip address 1.3.213.105 255.255.0.0  
  duplex auto  
  speed auto  
  bridge-group 1  
  bridge-group 1 spanning-disabled  
!  
interface FastEthernet0/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
  bridge-group 1  
  bridge-group 1 spanning-disabled  
!  
interface FastEthernet2/0  
  no ip address  
!  
interface FastEthernet2/1  
  no ip address  
!  
interface FastEthernet2/2  
  no ip address  
!  
interface FastEthernet2/3  
  no ip address  
!  
interface FastEthernet2/4  
  no ip address  
  shutdown  
!  
interface FastEthernet2/5  
  no ip address  
  shutdown  
!  
interface FastEthernet2/6  
  no ip address  
  shutdown  
!  
interface FastEthernet2/7  
  no ip address  
  shutdown  
!  
interface FastEthernet2/8  
  no ip address  
  shutdown  
!  
interface FastEthernet2/9  
  no ip address  
  shutdown  
!
```

```

interface FastEthernet2/10
  no ip address
  shutdown
!
.
.
.
interface FastEthernet2/33
  no ip address
  shutdown
!
interface FastEthernet2/34
  no ip address
  shutdown
!
interface FastEthernet2/35
  no ip address
  shutdown
!
interface GigabitEthernet2/0
  no ip address
  shutdown
!
interface GigabitEthernet2/1
  no ip address
  shutdown
!
interface Vlan1
  ip address 20.0.0.100 255.0.0.0
!
ip classless
ip route 223.255.254.0 255.255.255.0 1.3.0.1
!
ip http server
no ip http secure-server
!
!
!
!
radius-server local
  nas 20.0.0.2 key 0 cisco
  nas 20.0.0.101 key 0 cisco
  nas 20.0.0.102 key 0 cisco
  nas 20.0.0.1 key 0 cisco
  nas 20.0.0.100 key 0 cisco
  user ap1 nhash 7
02205C7D2E552D77181859385343475D2D517B73050A126770355135532300090E
  user client1 nhash 7
1444405A2D5C0F0E020D1110734322355752077B01727528254937087C07770602
  user ap2 nhash 7
072A711D6F5D4D2332455C28257879707C6011073722442752060F7907755B204E
!
radius-server host 20.0.0.100 auth-port 1812 acct-port 1813
radius-server key cisco
!
!
!
!
wlccp authentication-server infrastructure LEAP
wlccp authentication-server client leap LEAP
wlccp wds priority 10 interface Vlan1
!
line con 0

```

```

exec-timeout 0 0
privilege level 15
line aux 0
line vty 0 4
!
!
end

```

Additional References

The following sections provide references related to fast secure roaming.

Related Documents

Related Topic	Document Title
Comprehensive set of software configuration commands	<i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points</i>
Configuration commands for local authentication	<i>Configuring Remote Site IEEE 802.1x Local Authentication Service</i>

MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3(11)T command reference publications.

This section contains descriptions for the following commands:

- [debug wlccp packet](#)
- [debug wlccp wds](#)
- [show wlccp wds](#)
- [wlccp authentication-server client](#)
- [wlccp authentication-server infrastructure](#)
- [wlccp wds priority interface](#)

debug wlccp packet

To display the packets that are delivered to and from the wireless domain services (WDS) device, use the **debug wlccp packet** command in privileged EXEC mode. Use the **no** form of this command to disable the packet display.

debug wlccp packet

no debug wlccp packet

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(11)JA	This command was introduced on Cisco Aironet access points.
	12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700 series, and Cisco 3800 series routers.

Examples The following command displays the packets delivered to and from the WDS device:

```
Router# debug wlccp packet
```

Related Commands	Command	Description
	debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
	show wlccp wds	Shows information about access points and client devices on the WDS router.
	wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
	wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.
	wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

debug wlccp wds

To display wireless domain services (WDS) debug messages, state messages, and failure statistics, use the **debug wlccp wds** command in privileged EXEC mode. Use the **no** form of this command to disable the debugging output.

```
debug wlccp wds { authenticator | state | statistics }
```

```
no debug wlccp wds
```

Syntax Description

authenticator	MAC and Extensible Authentication Protocol (EAP) authentication.
state	WDS state and debug messages.
statistics	WDS failure statistics.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700 series, and Cisco 3800 series routers.

Examples

The following command displays WDS failure statistics:

```
Router# debug wlccp wds statistics
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
show wlccp wds	Shows information about access points and client devices on the WDS router.
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

show wlccp wds

To display information about the wireless domain services (WDS) device or information about client devices, use the **show wlccp wds** command in privileged EXEC mode.

```
show wlccp wds [ap | mn] [detail] [mac-addr mac-address]
```

Syntax	Description
ap	Displays access points that are authenticated and registered to WDS.
mn	Displays cached information about client devices, also called <i>mobile nodes</i> , that are authenticated and registered to WDS.
detail	Displays the client's lifetime, service set identifier (SSID), and VLAN ID.
mac-addr	Displays information about a specific client device.
<i>mac-address</i>	Client's MAC address.

Defaults

If you do not enter any options with the **show wlccp wds** command, this command displays the WDS device's IP address, MAC address, priority, and interface state. If the interface state is backup, the command also displays the current WDS device's IP address, MAC address, and priority.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700 series, and Cisco 3800 series routers.

Usage Guidelines

To show information about the WDS device, do not enter any options with this command.

Examples

The following command displays information about the WDS device:

```
# show wlccp wds ap
```

The following command displays cached information, including details, about the client device with the specified MAC address:

```
# show wlccp wds mn detail mac-addr 00-05-C2-00-01-F5
```

The following shows example output, followed by field descriptions.

```
# show wlccp wds
  MAC:0001.28e0.a400, IP-ADDR:10.0.0.1      , Priority:255
  Interface Vlan1, State:Administratively StandAlone - ACTIVE
  AP Count:1      , MN Count:0      , MAX AP Count:50
#
```

Table 3 *Output of show wlccp wds Command*

Field	Description
MAC	MAC address of interface on which WDS is configured
IP-Addr	IP address of interface on which WDS is configured
Priority	Priority of WDS
Interface	Interface on which WDS is configured
State	State of WDS: Initialization, backup, or active
AP Count	Number of access points registered to WDS
MN Count	Number of mobile nodes registered to WDS
MAX AP Count	Maximum number of access points that can be registered

Related Commands

Command	Description
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
debug wlccp packet	Displays packet traffic to and from the WDS router.
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

wlccp authentication-server client

To configure the list of servers to be used for 802.1X authentication, use the **wlccp authentication-server client** command in global configuration mode. You can specify a list of client devices that use any type of authentication, or you can specify a list of client devices that use a certain type of authentication (such as EAP, LEAP, or MAC-based authentication). Use the **no** form of this command to disable the server list.

wlccp authentication-server client {any | eap | leap | mac} *list*

no wlccp authentication-server client {any | eap | leap | mac} *list*

Syntax Description

any	Specifies client devices that use any authentication.
eap	Specifies client devices that use Extensible Authentication Protocol (EAP) authentication.
leap	Specifies client devices that use Light Extensible Authentication Protocol (LEAP) authentication.
mac	Specifies client devices that use MAC-based authentication.
<i>list</i>	List of client devices.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700 series, and Cisco 3800 series routers.

Examples

The following example shows how to configure the server list for LEAP authentication for client devices:

```
router# wlccp authentication-server client leap leap-list1
```

Related Commands

Command	Description
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
debug wlccp packet	Displays packet traffic to and from the WDS router.
show wlccp wds	Shows information about access points and client devices on the WDS router.

Command	Description
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

wlccp authentication-server infrastructure

To configure the list of servers to be used for 802.1X authentication for the wireless infrastructure devices, use the **wlccp authentication-server infrastructure** command in global configuration mode. Use the **no** form of this command to disable the server list.

wlccp authentication-server infrastructure *list*

no wlccp authentication-server infrastructure *list*

Syntax Description	<i>list</i>	List of servers to be used for 802.1X authentication for the wireless infrastructure devices, such as access points, repeaters, and wireless-aware routers.
---------------------------	-------------	---

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(11)JA	This command was introduced on Cisco Aironet access points.
	12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700 series, and Cisco 3800 series routers.

Examples This example shows how to configure the server list for 802.1x authentication for infrastructure devices participating in CCKM:

```
router# wlccp authentication-server infrastructure wlan-list1
```

Related Commands	Command	Description
	debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
	debug wlccp packet	Displays packet traffic to and from the WDS router.
	show wlccp wds	Shows information about access points and client devices on the WDS router.
	wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
	wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

wlccp wds priority interface

To configure the router or access point to provide wireless domain services (WDS), use the **wlccp wds priority interface** command in global configuration mode. Use the **no** form of the command to remove the WDS configuration from the router or access point.

wlccp wds priority *priority interface interface*

no wlccp wds priority *priority interface interface*

Syntax Description

priority <i>priority</i>	Priority of the WDS candidate. The WDS candidate with the highest priority becomes the active WDS. The valid range is from 1 to 255. The greater the priority value, the higher the priority.
interface <i>interface</i>	Interface on which the router sends out WDS advertisements. Supported interface types are: <ul style="list-style-type: none"> • For access points—Bridged Virtual Interface • For wireless-aware routers—Bridged Virtual Interface, Switched Virtual Interface, Fast Ethernet, and Gigabit Ethernet

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced with support for Cisco Aironet access points.
12.3(11T)	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700 series, and Cisco 3800 series routers.

Usage Guidelines

The WDS candidate with the highest priority becomes the active WDS device.

Examples

This example shows how to configure the priority for an access point as a candidate to provide WDS; the access point has a priority of 200:

```
AP# wlccp wds priority 200 interface bvi 1
```

Related Commands

Command	Description
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
debug wlccp packet	Displays packet traffic to and from the WDS router.

Command	Description
show wlccp wds	Shows information about access points and client devices on the WDS router.
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.

