Cisco Catalyst 6500 Series Wireless LAN Services Module Configuration Note

This document provides configuration procedures for the Cisco Catalyst 6500 series Wireless LAN Services Module (WLSM) and contains these sections:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

The Cisco wireless solution provides the framework to integrate and extend wireless networks efficiently and economically. The solution extends wireless into important elements of the network infrastructure, providing the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs. This document provides information about configuring the Cisco Catalyst 6500 series WLSM in a typical wireless network.

The WLSM is one component in the larger wireless LAN solution. The following are additional required components:

- Catalyst 6500 Series Switch running Cisco IOS Release 12.2(18)XSF2

  http://cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
- Catalyst 6500 Series WLSM release 2.1.1

  http://cisco.com/en/US/products/ps5865/tsd_products_support_model_home.html
- Cisco Aironet 1100, 1130AG, 1200, 1230AG, and 1240AG Series Access Points running Cisco IOS Release 12.3(8)JA

  http://cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html
- Cisco Aironet 1300 Series Outdoor Access Point/Bridge running Cisco IOS Release 12.3(8)JA

  http://cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html
- CiscoWorks Wireless LAN Solution Engine (WLSE) release 2.13

  http://cisco.com/en/US/products/ps6379/tsd_products_support_series_home.html

For more information on configuring the solution and for sample configurations, go to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/accsspts/techref/wlsm/wlsmcfg.htm

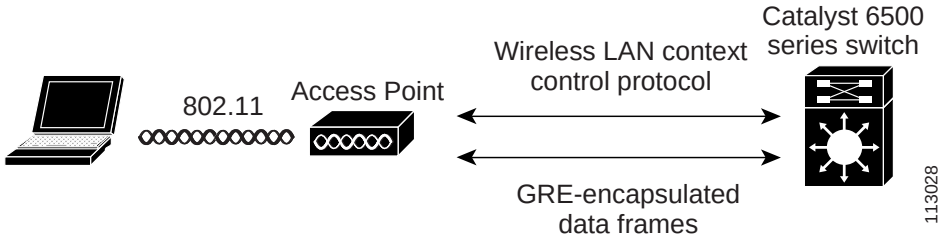
Understanding Wireless LAN Services

The WLSM provides the following features for 802.11 wireless clients on Catalyst 6500 series switches:

- Fast, uninterrupted, secure Layer 2 and Layer 3 wireless roaming
- Radio-management aggregation
- WLSM scalability (support for up to 600 access points)
- Graceful tunnel resiliency and redundancy
- RADIUS assigned mobility group
- Improved multicast support
- Support for 240 mobility groups
- Support for WDS information MIB

Figure 1 shows the system view for the WLSM. Traffic between the access point and the Catalyst 6500 series switch is IP directed. The two devices may be separated by bridges or routers.

Figure 1 WLSM System View



Wireless LAN context control protocol (WLCCP) messages carry authentication message exchanges between the access point and the wireless domain services (WDS) running on the Catalyst 6500 series switch. The Catalyst 6500 series switch acts as an authenticator by learning the location of every associated wireless client node.

The switch learns the MAC-to-IP bindings of the wireless clients either by snooping on the DHCP exchanges or by snooping ARP or IP packets from the wireless nodes. These two learning mechanisms enable the switch to provide uninterrupted Layer 3 mobility to roaming wireless nodes.

You configure a multipoint generic routing encapsulation (mGRE) tunnel between the Catalyst 6500 series switch and each access point so that mobile users can roam between access points and maintain Layer 3 connectivity. The multipoint GRE tunnels simulate logical Layer 3 networks between access points, providing an easier and faster solution for Layer 3 roaming.

Understanding WDS

WDS is a feature for access points in Cisco IOS software and the basis of the Catalyst 6500 series WLSM. WDS is a core function that enables other features such as these:

- Fast Secure Roaming
- Wireless LAN Solution Engine (WLSE) interaction
- Radio Management

You must establish relationships between the access points that participate in WDS and the Wireless LAN Services Module, before any other WDS-based features work. One of the purposes of WDS is to reduce the time required for client authentication by eliminating the need for the authentication server to validate user credentials.

In order to use WDS, you must designate one access point or the Wireless LAN Services Module as the WDS. A WDS access point must establish a relationship to an authentication server by authenticating to it with a WDS username and password. The authentication server can be either an external RADIUS server or the Local RADIUS Server feature in the WDS access point. The Wireless LAN Services Module must have a relationship with the authentication server, even though it does not need to authenticate to the server.

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

Client authentication is defined by one or more client server groups on the WDS.

When a client attempts to associate to an infrastructure access point, the infrastructure access point passes the credentials of the user to the WDS for validation. If it is the first time that the WDS sees the credentials, it turns to the authentication server to validate the credentials. The WDS then caches the credentials so that it does not have to return to the authentication server when that user attempts authentication again. Reauthentication can occur under any of the following conditions:

- When the access points rekey
- When the client roams between access points
- When the user starts up the client device

Any RADIUS-based Extensible Authentication Protocol (EAP) can be tunneled through WDS, such as these protocols:

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

The WDS and the infrastructure access points communicate over WLCCP. These multicast messages can not be routed, so a WDS and its associated infrastructure access points 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, the packets cannot be translated with a protocol like Network Address Translation (NAT).

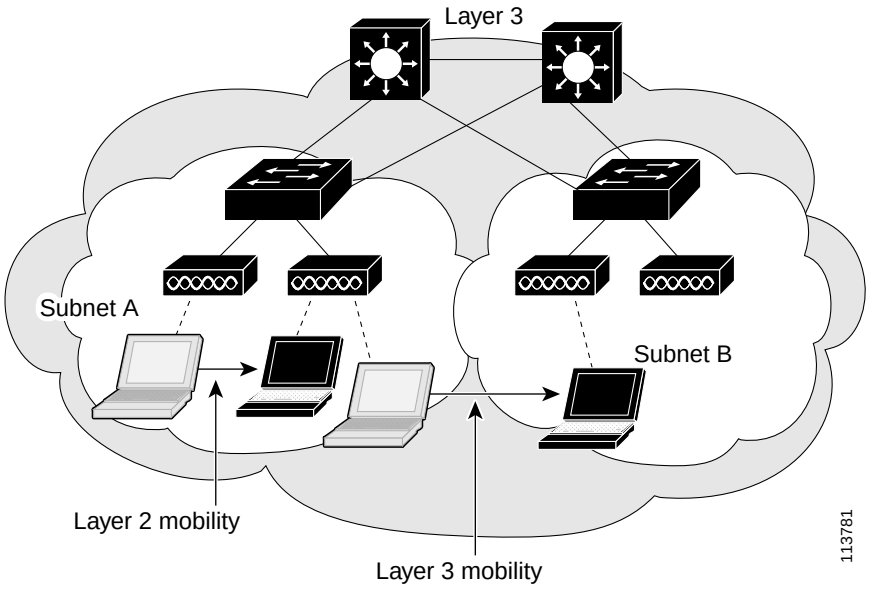
Current design recommendations specify one WDS access point per thirty infrastructure access points. The Wireless LAN Services Module can handle up to 600 infrastructure access points.

Layer 2 and Layer 3 Mobility

Layer mobility occurs when a wireless LAN client moves between wireless access points that are within the same IP subnet. Layer 3 mobility occurs when a wireless LAN client moves between wireless access points that are in different IP subnets. (See Figure 2.)

Fast secure roaming enables a client to change its connection between access points in the same subnet (Layer 2 mobility) or between subnets (Layer 3 mobility) to support time-sensitive applications such as VoIP, video on demand, VPN over wireless, and client/server-based applications.

Figure 2 Examples of Layer 2 and Layer 3 Mobility



Layer 2 Mobility

Layer 2 mobility occurs when a wireless LAN device physically moves enough so that its radio associates to a different access point. The original and the updated access points offer coverage for the same IP subnet, so that the wireless LAN client is still valid after the roam.

Layer 3 Mobility

Mobility in a wireless LAN environment can present a challenge as the physical reach of the network grows. Applications such as voice require roam times below 150 ms and require IP address continuity regardless of the Layer 3 boundaries that are crossed. Deploying a sprawling Layer 2 network can subject user traffic to delays and loss of service due to issues such as broadcast storms and Spanning Tree Protocol (STP) reconvergence times.

Layer 3 mobility provides a better performing and more scalable approach. Access points may be deployed in any location in a large Layer 3 network without requiring a single VLAN to be carried throughout the wired switch infrastructure. An overlay of multipoint GRE (mGRE) tunnels allows clients to roam to other access points residing on different Layer 3 subnets without loss of connectivity or a change in IP addressing.

The Cisco Layer 3 mobility solution consists of various hardware and software components. For more information about the Cisco wireless solution go to cisco.com:

http://cisco.com/en/US/products/hw/wireless/index.html

The primary devices are as follows:

- Cisco Aironet 1100, 1130AG, 1200, 1230AG, and 1240AG Series Access Points and Cisco Aironet 1300 Series Outdoor Access Point/Bridges
- Catalyst 6500 Series Switch (and its Supervisor 720 Module)
- Catalyst 6500 Series WLSM

Wireless Domain Services (WDS) coordinates these devices and the mobile nodes. The WDS runs on the WLSM. These components must be configured to work together as a unified system.

Configuring Layer 3 mobility requires linkage between different hardware and software components. Linkage is best accomplished by separating the functional components into modules, configuring each module individually, and verifying that each module works properly before proceeding to the next.

New Features in Release 2.1.1

The following sections describe the new features supported in Release 2.1.1:

Increased Access Point Scalability

Memory and software improvements have increased scalability from 300 to 600 access points.

Multiple WLSMs per Catalyst 6500 Chassis

In Release 2.1.1, the Supervisor 720 now supports two WLSMs in a chassis. In this configuration, only one WLSM can be active; the other is operating in a standby state. If the active WLSM fails, the standby WLSM becomes active in a matter of seconds, and combined with graceful tunnel resiliency, the WLSM switchover is seamless and transparent to the user. New clients and roaming clients are minimally affected because of the short time it takes to bring the standby WLSM to the active state.

Running Hot Standby Router Protocol (HSRP) on all WLSMs acheives intra-switch and inter-switch hot standby WLSM redundancy. In order to avoid unnecessary failovers and make use of a graceful recovery feature, disable preemption for HSRP.

Graceful Tunnel Resiliency

Graceful tunnel resiliency is a high availability feature that provides near Stateful Switchover (SSO) capability. In the event of a WLSM failure, graceful tunnel resiliency maintains data traffic forwarding for all existing Mobile Nodes (MNs) that are authenticated. This is done for a configurable grace period. MN authentication and session states are refreshed without disruption to their data traffic after the WLSM reboots or a backup WLSM takes over. Only new authentications or roaming is affected when the WLSM is down or in a recovery state.

Support for 240 Mobility Groups

This feature provides increased scalability and flexibility by supporting up to 240 mobility groups. A larger number of mobility groups allows for multiple policies based on user posture validation. Also, each mobility domain may be set as a smaller group to address big flat IP subnet concerns.

No additional WLSM configuration is required for this feature.

Improved Multicast Support

Release 2.1.1 provides an IGMP snooping-based multicast solution. IGMP snooping is performed on the access point to allow forwarding of downstream multicast traffic from the native network infrastructure to clients of dynamic RADIUS-assigned mobility groups. Multicast traffic forwarding for any mobility group can be turned on or off with the CLI on the Supervisor 720.

The Catalyst 6500 series wireless LAN handles multicast traffic differently from unicast IP traffic. When a wireless user sends upstream IP multicast traffic, the access point encapsulates the packet with a GRE header and forwards the packet over the tunnel. The only exception in this scenario (upstream IP multicast traffic flow) is Internet Group Management Protocol (IGMP) join messages, which are locally bridged by the access point to the local infrastructure.

Downstream IP multicast traffic from the Supervisor 720 to the access point is not sent via the fast secure roaming tunnel. Instead, IP multicast traffic sent to the access point is forwarded using the underlying network infrastructure. Via the locally bridged IGMP messages, the access point dynamically constructs a wireless client-to-multicast group association table. This IGMP snooping operation permits flexible creation of a multicast group-to-wireless client association table at the access point and permits the access point to efficiently use bandwidth by only forwarding multicast traffic when there is a multicast-requesting client associated. However, due to the asymmetric multicast traffic flow, all network nodes between the supervisor engine and the access point must be configured to enable downstream multicast traffic to reach its destination.

RADIUS Assigned Mobility Groups

The fast secure roaming tunnels used with the Catalyst 6500 series WLSM are the components of the solution which permits Layer 3 mobility and fast secure roaming. The fast secure roaming tunnels may be assigned statically by associating a network-ID with each SSID at the access point, or dynamically per user via RADIUS authentication. The primary advantage of RADIUS-based mobility group or tunnel assignment is that it dramatically simplifies the configuration of access points because they are dynamically assigned the necessary mobility groups for users. The access point needs only to be configured for a single SSID. This permits the segmentation of different user groups on the access point (such as employees, contractors, guests, etc.) to different mobility groups and different network access policies from the Catalyst 6500 series switch.

It is also possible to combine the following deployment models to assign the desired mobility group or fast secure roaming tunnel for clients that use RADIUS authentication:

- Creation of static tunnels for clients that do not support RADIUS authentication
- RADIUS vendor-specific attributes

No extra configuration on the WLSM or Supervisor 720 is required to enable dynamic mobility group assignment. The configuration of the access point and RADIUS server control whether mobility groups are dynamically assigned at the access point using the WLSM's authentication transactions. Mobility group/ tunnel IDs must be configured at the Supervisor 720 for either static or dynamic mobility group operation.

Support for WDS Information MIB

Release 2.1.1 greatly improves MIB support for the WLSM by supporting the CISCO-WDS-INFO-MIB by introducing the capability of querying the WLSM for client, access point, and WLSE status and statistics. This information may be used to query the WLSM for client association, roaming and performance data, or custom SNMP applications.

Configuring the Wireless LAN Services Module

The initial Wireless LAN Services Module configuration consists of the following tasks:

Note The initial Wireless LAN Services Module configuration must be made through a direct connection to the console port on the module.

Configuring VLANs on the Switch

Note VLAN IDs must be the same for the switch and the module. Refer to the “Configuring VLANs” chapter in the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide* for details.

Note The wireless LAN software supports the extended-range VLANs (2 through 1005).

To configure VLANs on the switch, perform this task:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters configuration mode and selects the terminal option.
Step 2	`Router(config)# vlan vlan_ID`	Enters VLAN configuration mode and adds a VLAN. The valid range is 2 through 4094.
Step 3	`Router(config-vlan)# exit`	Updates the VLAN database and returns to privileged EXEC mode.

This example shows how to configure VLANs on the switch:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# vlan 100
Router(config-vlan)# exit
Router(config)#
```

Configuring Layer 3 Interfaces

To configure the corresponding Layer 3 VLAN interface, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface vlan vlan_ID`	Selects an interface to configure.
Step 2	`Router(config-if)# ip address ip_address subnet_mask`	Configures the IP address and IP subnet.
Step 3	`Router(config-if)# no shutdown`	Enables the interface.
Step 4	`Router(config-if)# exit`	Exits configuration mode.

This example shows how to configure the Layer 3 VLAN interface:

```
Router# configure terminal
Router(config)# interface vlan 100
Router(config-if)# ip address 10.10.1.10 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

Adding the Wireless LAN Services Module to the Corresponding VLAN

Note By default, the Wireless LAN Services Module is in trunking mode with native VLAN 1.

To add the Wireless LAN Services Module to the corresponding VLAN, perform this task:

Command	Purpose
`Router(config)# wlan module` *mod* `allowed-vlan` *vlan_ID*	Configures the VLANs allowed over the trunk to the Wireless LAN Services Module. **Note** One of the allowed VLANs must be the admin VLAN.

This example shows how to add a Wireless LAN Services Module that is installed in slot 5 to a specific VLAN:

```
Router(config)# wlan module 5 allowed-vlan 100
Router(config)# end
```

Configuring the Loopback Interface

The loopback interface is a software-only virtual interface that emulates an interface.

To configure the loopback interface, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface loopback` *number*	Configures a loopback interface and enters interface configuration mode. The *number* argument specifies the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.
Step 2	`Router(config-if)# ip address` *ip_addr* [*subnet*]	Assigns an IP network address and network mask to the interface.
Step 3	`Router(config-if)# exit`	Exits configuration mode.

The following example shows how to configure a loopback interface:

```
Router(config)# interface loopback 0
Router(config-if)# ip address 10.1.1.2 255.255.255.0
Router(config-if)# exit
```

Configuring the Wireless mGRE Tunnel

The infrastructure that enables Layer 3 mobility consists of Multipoint Generic Routing Encapsulation (mGRE) tunnels. Each tunnel has a single termination point on the Supervisor 720 module of the Catalyst 6500 that hosts the WLSM. The other logical endpoint of the tunnel exists on all access points participating in the Layer 3 mobility network. Clients that associate to a participating access point associate to a particular SSID. The SSID is mapped (either statically or dynamically via RADIUS) to a

mobility network that tunnels all client traffic to the Catalyst 6500. The Supervisor 720 maintains a database of the clients (mobile nodes) and the access points to which they are associated. Roaming from one access point to another simply requires updating the database and changing the forwarding information for that mobile node.

To configure wireless mGRE tunnels, perform this task:

	Command	Purpose
Step 1	`Router(config)# ip dhcp snooping`	(Optional) Enables DHCP snooping. **Note** This command is required if you enable DHCP snooping on the tunnel interface for untrusted wireless networks. **Note** See the "Configuring the DHCP Snooping Database" section on page 20 for information on the DHCP snooping database for untrusted networks.
Step 2	`Router(config)# interface tunnel number`	(Optional) Configures a tunnel interface and enters interface configuration mode. The *number* argument specifies the number of the tunnel interface that you want to create or configure.
Step 3	`Router(config-if)# ip address ip_addr [subnet_mask]`	Specifies the tunnel IP and the mGRE tunnel overlay subnet.
Step 4	`Router(config-if)# ip mtu bytes`	(Optional) Sets the maximum transmission unit (MTU) size, in bytes, of IP packets sent on an interface. The default value for *bytes* is 1476; the minimum is 512.
Step 5	`Router(config-if)# tunnel source loopback interface`	Configures the tunnel source. Each tunnel must have a different tunnel source.
Step 6	`Router(config-if)# tunnel mode gre multipoint`	Sets the encapsulation mode to mGRE for the tunnel interface.
Step 7	`Router(config-if)# mac-address mac_addr`	(Optional) Specifies the MAC address of the router. **Note** Entering the router MAC address allows mobile nodes to detect if their IP address is duplicated on the network. The access point uses the router MAC address to handle address resolution protocol (ARP) requests using proxy ARP. Proxy ARP is automatic and requires no user input. Enter the **show mobility status** command to display the MAC address used for proxy ARP. Enter this MAC address as *mac_addr*.
Step 8	`Router(config-if)# mobility network-id [id]`	Specifies the wireless network ID for the mGRE tunnel. Valid values for *id* are 1 through 4095.

	Command	Purpose
Step 9	`Router(config-if)# mobility trust [ip-discovery]`	(Optional) Specifies the trusted network. **Note** If you enter the **mobility trust** command, do not enter the **ip dhcp snooping packets** command. A trusted network can use DHCP or static IP addresses. An untrusted network supports only DHCP clients. The default is untrusted. The ip-discovery option provides the capability to discover the IP addresses of passive wireless client devices associated to an infrastructure access point.
Step 10	`Router(config-if)# mobility broadcast`	(Optional) Specifies the mGRE tunnel to convert nonbroadcast multiaccess (NBMA) to broadcast multiaccess (BMA).
Step 11	`Router(config-if)# ip dhcp snooping packets`	(Optional) Enables DHCP snooping for the untrusted wireless network ID. **Note** If you enter the **ip dhcp snooping packets** command, do not enter the **mobility trust** command. **Note** You must enable DHCP snooping globally before enabling DHCP snooping on the tunnel interface by entering the **ip dhcp snooping** command. **Note** See the "Configuring the DHCP Snooping Database" section on page 20 for information on the DHCP snooping database for untrusted networks.
Step 12	`Router(config-if)# exit`	Exits configuration mode.

This example shows how to configure wireless mGRE tunnels:

```
Router(config)# ip dhcp snooping
Router(config)# interface tunnel 0
Router(config-if)# ip address 10.1.1.2 255.255.255.0
Router(config-if)# ip mtu 1024
Router(config-if)# tunnel source loopback 0
Router(config-if)# tunnel mode gre multipoint
Router(config-if)# mobility network-id 10
Router(config-if)# ip dhcp snooping packets
Router(config-if)# exit
```

Configuring VLANs on the Wireless LAN Services Module

When you configure VLANs on the Wireless LAN Services Module, configure one of the VLANs as an administrative VLAN. The system adds the default route through the gateway of the administrative VLAN.

Note The wireless LAN software supports only one admin VLAN. Configuring the admin VLAN is required for using the wireless domain services.

Note VLAN IDs must be the same for the switch and the module. Refer to the "Configuring VLANs" chapter in the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide* for details.

To configure VLANs on the Wireless LAN Services Module, perform this task:

	Command	Purpose
Step 1	`wlan(config)# wlan vlan vlan_ID`	Configures the wireless LAN VLANs and enters VLAN mode. **Note** If this is the admin VLAN, enter the same *vlan_ID* that you entered for the switch. (See the "Configuring VLANs on the Switch" section on page 8.)
Step 2	`wlan(config-vlan)# ipaddr ip_addr netmask`	Configures an IP address for the wireless LAN VLAN. **Note** Configure the IP address in the same subnet as the VLAN IP address.
Step 3	`wlan(config-vlan)# gateway gateway_addr`	Configures the gateway IP address. **Note** If this is the admin VLAN, enter the same IP address for the gateway as you entered for the switch. (See the "Configuring Layer 3 Interfaces" section on page 9.)
Step 4	`wlan(config-vlan)# standby [group-number] ip [ip-address]`	(Optional) Configures the Hot Standby Router Protocol (HSRP).
Step 5	`wlan(config-vlan)# route ip_addr netmask gateway ip_addr`	(Optional) Configures a static route for servers that are one or more Layer 3 hops away from the Wireless LAN Services Module.
Step 6	`wlan(config-vlan)# admin`	(Optional) Configures the VLAN as the administrative VLAN[1].

1. The administrative VLAN is for management traffic. Specify only one VLAN as the administrative VLAN.

This example shows how to configure the VLAN and specify the IP address, the subnet mask, and the global gateway, and it also specifies the VLAN as the administrative VLAN:

```
wlan(config)# wlan vlan 100 admin
wlan(config-vlan)# ipaddr 10.10.1.20 255.255.255.0
wlan(config-vlan)# gateway 10.10.1.10
wlan(config-vlan)# admin
wlan(config-vlan)# end
wlan#
```

Configuring Telnet Remote Access

To configure the Wireless LAN Services Module for Telnet remote access, perform this task:

	Command	Purpose
Step 1	`wlan(config)# aaa authentication login default line`	Creates a default authentication list for login purposes. The line password is used for the default authentication list.
Step 2	`wlan(config)# enable password password`	Specifies a local enable password.

	Command	Purpose
Step 3	`wlan(config)# line vty` *starting-line-number ending-line-number*	Identifies a range of lines for configuration and enters line configuration mode.
Step 4	`wlan(config-line)# login authentication default`	Enables password checking at login and also ensures that the default authentication list is used.
Step 5	`wlan(config-line)# password` *password*	Specifies a password on the line.

This example shows how to configure the Wireless LAN Services Module for remote access:

```
wlan(config)# aaa authentication login default line
wlan(config)# enable password cisco
wlan(config)# line vty 0 4
wlan(config-line)# login authentication default
wlan(config-line)# password cisco
wlan(config-line)# exit
wlan(config)#
```

Configuring Wireless Domain Services

To configure the Wireless LAN Services Module as the WDS device, perform this task:

	Command	Purpose
Step 1	`wlan(config)# aaa new-model`	Enables the AAA access control model.
Step 2	`wlan(config)# aaa authentication login leap-devices group radius`	Defines a group used to authenticate Extensible Authentication Protocol (LEAP) devices.
Step 3	`wlan(config)# aaa authentication login default enable`	Specifies the enable password as the login authentication method.
Step 4	`wlan(config)# radius-server host` {*hostname* | *ip_address*} [**auth-port** *port_number*][**acct-port** *port_number*]	Defines the RADIUS server used to LEAP-authenticate devices.
Step 5	`wlan(config)# radius-server key` *string*	Sets the authentication and encryption key for all RADIUS communications between the module and the RADIUS server. The **radius-server key** command has no default value; however, the key must match the encryption key used on the RADIUS server.
Step 6	`wlan(config)# wlccp authentication-server infrastructure leap-devices`	Defines a method that authenticates the other access points.
Step 7	`wlan(config)# wlccp authentication-server client any leap-devices`	Defines a method that authenticates the client devices (a client server group) and what EAP types those clients use.

This example shows how to configure the Wireless LAN Services Module as the WDS device:

```
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 10.91.104.76 auth-port 1645 acct-port 1646
wlan(config)# radius-server key cisco
wlan(config)# end
```

Configuring Local Authentication

To configure the WLSM as a local authenticator, refer to Chapter 8, "Configuring an Access Point as a Local Authenticator," in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/accsspts/i12215ja/i12215sc/s15local.htm

Configuring the Access Points

To configure the access points to use the WDS, refer to Chapter 11, "Configuring WDS, Fast Secure Roaming, and Radio Management," in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/accsspts/i12215ja/i12215sc/s15roamg.htm

Displaying Layer 3 Mobility and Wireless Network Information

To display Layer 3 mobility and wireless network information, perform these tasks from the supervisor engine:

Command	Purpose
`Router# show mobility [ap | mn | network | status]`	Displays Layer 3 mobility and wireless network information.
`Router# show mls cef adjacency [all | decap-tunnel | encap-tunnel | entry]`	Displays information about the hardware Layer 3 switching adjacency node.

This example shows the output of the various **show mobility** commands issued from a Supervisor 720:

```
Sup720...#show mobility ap
Codes: * - dynamic network ID, otherwise - static network ID

 AP IP Address   AP Mac Address  Wireless Network-ID
---------------  --------------  -------------------
10.10.0.36       0013.5f0c.41c5
10.10.0.64       000b.5f19.665f  100 101 102 103

10.10.0.65       0005.9a39.b03a
10.10.0.67       000b.fcfb.7ca6  *102


Sup720...#show mobility ap 10.10.0.67 detail
IP Address                    : 10.10.0.67
MAC Address                   : 000b.fcfb.7ca6
Participating Wireless Tunnels:
102, Dynamic (Dyanmic MN = 1)

Registered Mobile Nodes on AP :
MN Mac Address  MN IP Address  AP IP Address  Wireless Network-ID  Flags
--------------  -------------  -------------  -------------------  -----
0007.0eb9.3d78  172.16.3.26    10.10.0.67     102                  D F

Flags: D=Dynamic network ID, F=Fresh, G=Grace Period


Sup720...#show mobility mn
MN Mac Address  MN IP Address  AP IP Address  Wireless Network-ID  Flags
--------------  -------------  -------------  -------------------  -----
0007.0eb9.3d78  172.16.3.26    10.10.0.67     102                  D F

Flags: D=Dynamic network ID, F=Fresh, G=Grace Period


Sup720...#show mobility mn ip 172.16.3.26
MN Mac Address  MN IP Address  AP IP Address  Wireless Network-ID  Flags
--------------  -------------  -------------  -------------------  -----
0007.0eb9.3d78  172.16.3.26    10.10.0.67     102                  D F

Flags: D=Dynamic network ID, F=Fresh, G=Grace Period

Sup720...#show mobility network 102
Wireless Network ID               : 102
Wireless Tunnel Source IP Address  : 10.80.0.3
Wireless Network Attributes        : Trusted, Broadcast Enabled, Multicast Enabd
Wireless Network State             : Up

Registered Access Point on Wireless Network 102:
Codes: * - dynamic network ID, otherwise - static network ID

 AP IP Address   AP Mac Address  Wireless Network-ID
---------------  --------------  -------------------
10.10.0.64       000b.5f19.665f  100 101 102 103

10.10.0.67       000b.fcfb.7ca6  *102

Registered Mobile Nodes on Wireless Network 102:
MN Mac Address  MN IP Address  AP IP Address  Wireless Network-ID  Flags
--------------  -------------  -------------  -------------------  -----
0007.0eb9.3d78  172.16.3.26    10.10.0.67     102                  D F

Flags: D=Dynamic network ID, F=Fresh, G=Grace Period
```

```
Sup720...#show mobility status

Primary WLAN Module is located in Slot: 1 (HSRP State: Not Applicable)
LCP Communication status      : up
No Secondary WLAN Module in the system
WLSM recovery period remaining: 0 seconds
MAC address used for Proxy ARP: 0005.5f54.5800
Number of Wireless Tunnels    : 4
Number of Access Points       : 4
Number of Mobile Nodes        : 1

Wireless Tunnel Bindings:
Tunnel           Src IP Address   Wireless Network-ID  Flags
---------------  ---------------  -------------------  -------
Tunnel100        10.80.0.1        100                  TB  M
Tunnel101        10.80.0.2        101                  TB  M
Tunnel102        10.80.0.3        102                  TB  M
Tunnel103        10.80.0.4        103                      M

Flags: T=Trusted, B=IP Broadcast enabled, M=IP Multicast enabled
       A=TCP Adjust-mss enabled, D=Discover passive MN's IP address
```

To display Layer 3 mobility and wireless network information, perform these tasks from the Wireless LAN Services Module:

Command	Purpose
wlan# **show wlccp wds** [**aggregator** | **ap** | **mn** | **mobility** | **nm** | **statistics**]	Displays the access points or mobile nodes registered on the network.
wlan# **show wlccp wds statistics**	Displays the current WLCCP statistics.
wlan# **show wlan** [**admin-info** | **crash-info** |**mac** | **status** | **version** | **vlan**]	Displays information about the wireless LAN.

This example shows the output of the various **show wlccp wds** commands issued from the WLSM:

```
WLSM>show wlccp wds aggregator ap

RM Aggregator APs Status [Maximum APs Supported 1024]:

NUM   IPADDR        REQ   ACK   RPT    AGG-RPT
1    10.10.0.52      54    54    2965     899
2    10.10.0.65      318   318   70750    14573
3    10.10.0.54      2413  2235  86445    33665
4    10.10.0.64      522   472   14823    7106
5    10.10.0.51      37    37    10477    1874
6    10.10.0.55      1594  1594  386476   70712

Total APs: 6

WLSM>show wlccp wds aggregator statistics

RM Aggregator Statistics:
        Maximum Size of the Requests Received: 1124
        Requests Received Count: 3332
        Request Acknowledgment Sent Count: 3332
        Route Response Sent Count: 4717
        Route Response Partially Sent Count: 7

        Request Sent to APs Count: 4938
        Request to AP Send Failure Count: 0
```

```
        Request to AP Send Failure due to Unregistered APs Count: 21
        Request Acks Received Count: 4710

        RM Reports Received Count: 571948
        Aggregate RM Reports Sent Count: 128832
        General Event Reports Received Count: 0
        Oversize AP-RM Reports Drop Count: 0
        Oversize WLSE-RM Reports Drop Count: 0

        Invalid WLCCP Message Received Count: 0
        Decode Errors Count: 0
        Encode Errors Count: 0
        Malloc Errors Count: 0

RM Library Statistics:
        Protocol Errors: 0
        MIC Errors: 0
        Packet Allocation Errors: 0
        Memory Allocation Errors: 0
        Data Enqueue Errors: 0
        Zero Length Packet Errors: 0
        Most Recent Error:

WLSM>show wlccp wds ap
  HOSTNAME                          MAC-ADDR      IP-ADDR          STATE
 AP1200_25                        000b.5f19.665f  10.10.0.64      REGISTERED
 Seagle_ap1                       000b.fcfb.7ca6  10.10.0.67      REGISTERED
 Cisco_AP                         0013.5f0c.41c5  10.10.0.36      REGISTERED


WLSM>show wlccp wds mn
    MAC-ADDR       IP-ADDR          Cur-AP            STATE
0007.0eb9.3d78  172.16.3.26     000b.fcfb.7ca6      REGISTERED


WLSM>show wlccp wds mobility network-id 102

Mobile Nodes in Wireless Network 102
MAC Address    IP Address      Current AP IP   Old AP IP       State
============== =============== =============== =============== ========
0007.0eb9.3d78 172.16.3.26     10.10.0.67      10.10.0.67      REGISTERED

WLSM>show wlccp wds statistics

WDS Statistics for last 6w6d:
        Current AP count:               4
        Current MN count:               1
        AAA Auth Attempt count:         90342
        AAA Auth Success count:         650
        AAA Auth Failure count:         80486
        MAC Spoofing Block count:       0
        Roaming without AAA Auth count:  0
        Roaming with full AAA Auth count:36
        Fast Secured Roaming count:     0
        MSC Failure count:              0
        KSC Failure count:              0
        MIC Failure count:              0
        RN Mismatch count:              0

WLSM>show wlccp wds statistics roaming
MN Roamings five seconds avg: 5; one minute avg: 3; five minutes avg: 3
Start time: 07:44:18.199 UTC Tue Apr 19 2005
 WNID      Total   NO Auth  AAA Auth   Fast Secured   5Sec   1Min   5Min
All        1200       400       500            300     10      6      3
```

```
WLSM# show wlccp wds statistics roaming detail
MN Roamings five seconds avg: 5; one minute avg: 3; five minutes avg: 3
Start time: 07:44:18.199 UTC Tue Apr 19 2005
 WNID   Total Roams  NO Auth AAA Auth   Fast Secured  5Sec RPS  1Min RPS 5Min RPS
   1         300       100       100            100     15        10       5
   2         400       200       100            100     20         3       2
   3         500       100       300            100      5         7       4
 All        1200       400       500            300     10         6       3


WLSM>show wlan admin-info
WLAN administration VLAN: 100
WLAN administration IP address: 10.100.0.2
WLAN administration gateway: 10.100.0.1


WLSM>show wlan status fdu
FDU cpu is alive!
FDU cpu utilization:
    % process util   : 0             % interrupt util : 0

    proc cycles : 0x50A9C824D        int cycles  : 0x69A38D20F
    total cycles: 0x8DC6B0A35DB68
    % process util (5 sec)   : 0             % interrupt util (5 sec) : 0
    % process util (1 min)  : 0             % interrupt util (1 min): 0
    % process util (5 min)  : 0             % interrupt util (5 min) : 0


WLSM>show wlan version
Cisco IOS Software, SVCWLAN Software (SVCWLAN-K9W7Y9-M), Version 2.1.1]
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 16-Nov-05 10:05 by wnbubld

ROM: System Bootstrap, Version 12.2(11)YS1 RELEASE SOFTWARE

REQ_TME_WLSM uptime is 6 weeks, 6 days, 2 hours, 43 minutes
System returned to ROM by power-on
System restarted at 14:46:50 UTC Thu Nov 24 2005
System image file is "tftp://255.255.255.255/unknown"
AP Version 2.1(1)


wlan# show wlan vlan
VLAN index 200 (admin VLAN)
   IP addr 200.1.1.2 NetMask 255.255.255.0   Gateway 200.1.1.1
```

Configuring the DHCP Snooping Database

Wireless clients, or mobile nodes, assigned to an untrusted wireless network must be configured to use DHCP to obtain IP addresses from a DHCP server. The switch should have DHCP snooping enabled on the tunnel corresponding to the wireless network. Because the DHCP snooping database is not synchronized between the active and standby Supervisor 720, Cisco recommends that you store the DHCP snooping database on an external server. Storing the database on an external server allows the standby Supervisor to retrieve the accumulated states if a switchover occurs.

To configure DHCP snooping database options, perform these tasks:

Command	Purpose
`Router(config)# ip dhcp snooping database {url}`	Specifies the URL that stores the DHCP snooping database entries; *url* takes the following forms: • **tftp:**//*host*/*filename* • **ftp:**//*user*:*password*@*host*/*filename* • **rcp:**//*user*@*host*/*filename* • **bootflash:**/*filename*[1]
`Router(config)# ip dhcp snooping database write-delay seconds`	Specifies (in seconds) the duration for which the database transfer should be delayed after the database changes. The default is 300 seconds. The range is from 15 to 86400 seconds.

1. Due to issues with storing the DHCP snooping database on the bootflash device, as documented in caveat CSCee23185, and the limited storage capacity on the bootflash device, we recommend that you store the database on an external server. When a file is stored in a remote location that is accessible through FTP, TFTP, or RCP, a redundant supervisor engine configured with RPR or SSO takes over the database when a switchover occurs.

This example shows how to specify the database URL using TFTP:

```
Router(config)# ip dhcp snooping database tftp://90.90.90.90/snooping-rp2
```

This example shows how to specify the amount of time before writing DHCP snooping entries:

```
Router(config)# ip dhcp snooping database write-delay 15
```

Note When you configure RPR and RPR+ redundancy, you must store the DHCP snooping database to an external server. Otherwise, mobile nodes in an untrusted network will lose connectivity after the supervisor engine switchover.

When you configure SSO redundancy, tunnel endpoints for mobile nodes are always synchronized to the standby supervisor engine. As a result, mobile nodes do not lose connectivity after a supervisor engine switchover, even if DHCP snooping database entries are not stored externally. However, after the switchover, the DHCP snooping database is emptied. Therefore, it is always advisable to have the DHCP snooping database to be stored externally for all modes of redundancy so that it will be retrieved automatically by the new active supervisor engine.

Configuring Graceful Tunnel Resiliency

To configure graceful tunnel resiliency, you need to configure the wireless LAN recovery time on the Supervisor 720. This parameter is set to 0 by default. Setting the recovery time to a value establishes the period of time that the Supervisor 720 maintains data communications with authenticated mobile nodes. If a WLSM failure occurs, the graceful recovery begins and the recovery timer starts.

When the WLSM comes back online, it reauthenticates the mobile nodes at a specific rate determined by the **wlccp wds recovery rate** value, which is the number of mobile nodes the WLSM reauthenticates per second. The default value is 40 authentications per second.

No configuration is required on the access points.

To enable and set the wireless LAN recovery time on the Supervisor 720, begin from the Privileged EXEC mode and perform this task:

	Command	Purpose
Step 1	Router #**configure terminal**	Enters configuration mode.
Step 1	Router (config)# **wlan recovery time** *seconds*	Specifies the recovery time or grace period in seconds for client operation without refreshing wireless LAN session context after a WLSM failure occurs. The default is 0 (which disables the feature) and the range is 0–65535 seconds.
Step 1	WLSM (config)# **end**	Exit configuration mode.
Step 1	WLSM# **write mem**	Saves configuration to NVRAM.

To verify or change the WLSM recovery rate setting, open the WLSM console, begin from Privileged EXEC mode, and perform this task:

	Command	Purpose
Step 1	WLSM# **configure terminal**	Enters configuration mode.
Step 2	WLSM (config)# **wlccp wds recovery rate** *seconds*	Specifies the number of MN re-authentications per second that the AAA server processes after a WLSM comes back online. The recovery rate throttles the load on the AAA server in the event of a WLSM failover. The default is 40 seconds and the range is 0–1000 seconds.
Step 3	WLSM (config)# **end**	Exit configuration mode.
Step 4	WLSM# **write mem**	Saves configuration to NVRAM.

Use the **show mobility mn** command to check the output on the Supervisor 720 during a recovery period, as shown in the following example:

```
Router# show mobility mn
MN Mac Address  MN IP Address  AP IP Address  Wireless Network-ID  Flags
--------------  -------------  -------------  -------------------  -----
0007.0eb9.3d78  172.16.3.26    10.10.0.67     102                G

Flags: D=Dynamic network ID, F=Fresh, G=Grace Period
```

You can check the status of a mobile node using the **show dot11 associations** command on the access point. This mobile node would be shown in a *rediscover* state, as shown in the following example:

```
ap# show dot11 associations
802.11 Client Stations on Dot11Radio0:

SSID: [test]
MAC Address        IP Address     Device         Name       Parent     State
0007.0eb9.3d78     10.10.0.67     350-client     testap1    self       Rediscover
```

Configuring Two WLSMs on One Chassis

To configure two WLSMs on the same chassis, use the **standby ip** command to activate HSRP on each WDS. Beginning in the Privileged EXEC mode, perform this task:

	Command	Purpose
Step 1	WLSM# **config terminal**	Enters configuration mode.
Step 2	WLSM (config)# **wlan vlan** *x*	Accesses the VLAN used for Supervisor 720 and WLSM communications.
Step 3	WLSM (config-vlan)# **standby** *group #* **ip** *ip address*	Configures the standby HSRP group and virtual IP address.
Step 4	WLSM (config-vlan)# **end**	Exit configuration mode.
Step 5	WLSM# **write mem**	Save config to NVRAM.

WLSM Graceful Tunnel Resiliency Performance Limitations

Performance is limited during the graceful recovery process. During the period that the WLSM is down, you can expect the following limitations:

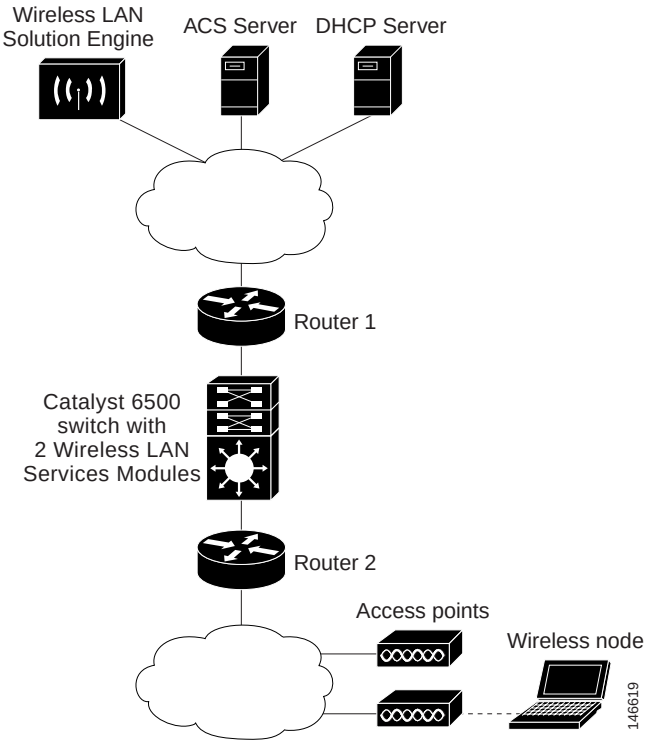
- No new authentications are allowed.
- If a client attempts to roam, it is deauthenticated.
- When the WLSM is back up, fast roaming (CCKM) is not available and client roaming requires a full reauthentication until the WLSM mobile node session context is refreshed.

Previous versions of wireless LAN software supported only one WLSM per chassis. Release 2.1.1 supports two WLSMs per chassis, and combined with graceful tunnel resiliency, provides a near intra-chassis WLSM switchover. In a two-WLSM per chassis configuration, only one WLSM can be active; the other is designated the standby WLSM. If the active WLSM fails, the standby WLSM takes over. Because the switchover takes place almost instantaneously, you should experience no traffic loss.

Configuration Examples

Figure 3 shows the configuration for Supervisor 720 and two WLSMs in a single chassis. The Supervisor 720 configuration is a selected portion from a complete configuration; however the WLSM configuration is complete.

Figure 3 Two WLSMs in a Single Chassis



Supervisor 720 configuration

```
upgrade fpd auto
version 12.2
service timestamps debug datetime msec show-timezone
service timestamps log datetime msec show-timezone
service password-encryption
service internal
service counters max age 10
!
hostname interswitch-rp1
!
boot system flash disk0:
enable password 7 1042081B
!
no aaa new-model
clock timezone PST -8
wlan module 3 allowed-vlan 100
wlan module 9 allowed-vlan 100
wlan recovery time 300
ip subnet-zero
!
```

```
!
!
ip dhcp snooping database tftp://90.90.90.91/snooping-rp1.txt
ip dhcp snooping database write-delay 15
ip dhcp snooping database timeout 10
ip dhcp snooping
ipv6 mfib hardware-switching replication-mode ingress
vtp domain cathay
vtp mode transparent
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
no mls acl tcam share-global
mls cef error action freeze
!
!

!
redundancy
mode sso
main-cpu
auto-sync running-config
auto-sync standard
spanning-tree mode pvst
!
power redundancy-mode combined
error-detection packet-buffer action none
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
port-channel per-module load-balance
!
!
interface Loopback62
ip address 62.0.0.1 255.255.255.255
!
interface Loopback63
ip address 63.0.0.1 255.255.255.255
!
interface Tunnel251
ip address 113.0.0.1 255.0.0.0
ip helper-address 83.0.0.100
no ip redirects
ip directed-broadcast
tunnel source Loopback63
tunnel mode gre multipoint
mobility network-id 251
mobility trust
mobility multicast
!
interface Tunnel300
ip address 115.0.0.1 255.0.0.0
ip helper-address 83.0.0.100
no ip redirects
ip directed-broadcast
ip dhcp snooping packets
tunnel source Loopback62
tunnel mode gre multipoint
mobility network-id 300
mobility multicast

interface Vlan100
ip address 100.0.0.100 255.0.0.0
```

WLSM 1 configuration

```
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname wlsm1-mod-3
!
boot-start-marker
boot-end-marker
!
logging buffered 8000000 debugging
enable password lab
!
username cisco password 0 cisco
spd headroom 512
aaa new-model
!
!
aaa authentication login CONSOLE none
aaa authentication login SHAREDAAA group radius none
aaa authentication login locally local
aaa session-id common
ip subnet-zero
!
!
ip tftp source-interface Ethernet0/0.100
!
wlan vlan 100
ipaddr 100.0.0.201 255.0.0.0
gateway 100.0.0.100
admin
standby 1 ip 100.0.0.25
!
!
!
!
no crypto isakmp enable
!
buffers huge size 46080
!
!
interface Ethernet0/0
mac-address 000d.29f0.c2f9
no ip address
no cdp enable
hold-queue 2048 in
!
interface Ethernet0/0.100
encapsulation dot1Q 100
ip address 100.0.0.201 255.0.0.0
no cdp enable
standby 1 ip 100.0.0.25
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.0.0.100
ip http server
no ip http secure-server
!
!
```

```
snmp-server view iso iso included
snmp-server view isoview iso included
snmp-server community public view iso RW
snmp-server enable traps tty
no cdp run
radius-server host 20.1.0.1 auth-port 1645 acct-port 1646 key cisco123
!
control-plane
!
!
wlccp authentication-server infrastructure SHAREDAAA
wlccp authentication-server client any SHAREDAAA
wlccp wds interface Ethernet0/0.100
!
line con 0
exec-timeout 0 0
transport preferred all
transport output all
stopbits 1
line 1 3
no exec
transport preferred all
transport input all
transport output none
flowcontrol software
line vty 0 4
login authentication locally
transport preferred all
transport input all
transport output all
```

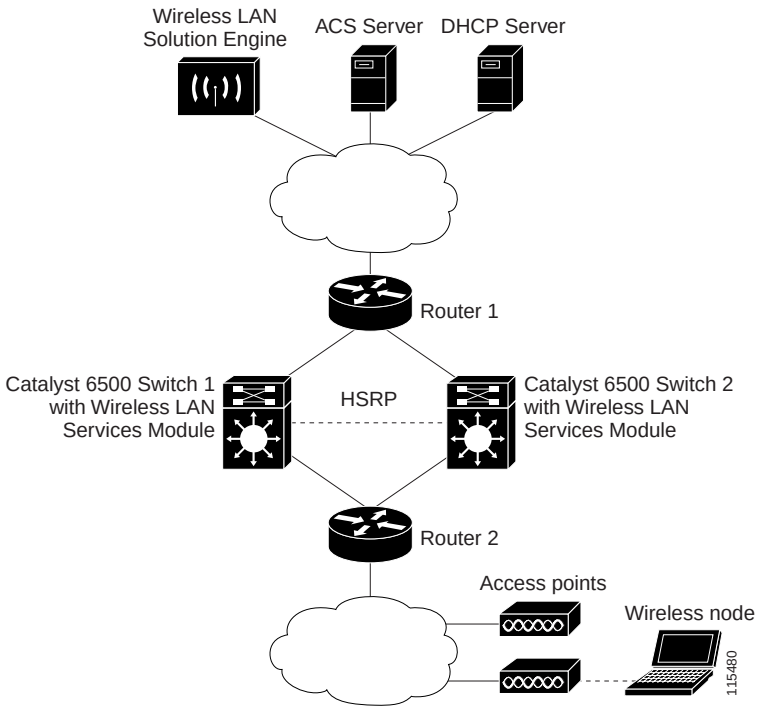
WLSM 2 configuration

```
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname wlsm2-mod-4
!
boot-start-marker
boot-end-marker
!
logging buffered 8000000 debugging
enable password lab
!
username cisco password 0 cisco
spd headroom 512
aaa new-model
!
!
aaa authentication login CONSOLE none
aaa authentication login SHAREDAAA group radius none
aaa authentication login locally local
aaa session-id common
ip subnet-zero
!
!
ip tftp source-interface Ethernet0/0.100
!
```

```
wlan vlan 100
ipaddr 100.0.0.202 255.0.0.0
gateway 100.0.0.100
admin
standby 1 ip 100.0.0.25
!
!
!
!
no crypto isakmp enable
!
buffers huge size 46080
!
!
interface Ethernet0/0
mac-address 000d.29f0.d4fa
no ip address
no cdp enable
hold-queue 2048 in
!
interface Ethernet0/0.100
encapsulation dot1Q 100
ip address 100.0.0.202 255.0.0.0
no cdp enable
standby 1 ip 100.0.0.25
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.0.0.100
ip http server
no ip http secure-server
!
!
snmp-server view iso iso included
snmp-server view isoview iso included
snmp-server community public view iso RW
snmp-server enable traps tty
no cdp run
radius-server host 20.1.0.1 auth-port 1645 acct-port 1646 key cisco123
!
control-plane
!
!
wlccp authentication-server infrastructure SHAREDAAA
wlccp authentication-server client any SHAREDAAA
wlccp wds interface Ethernet0/0.100
!
line con 0
exec-timeout 0 0
transport preferred all
transport output all
stopbits 1
line 1 3
no exec
transport preferred all
transport input all
transport output none
flowcontrol software
line vty 0 4
login authentication locally
transport preferred all
transport input all
transport output all
```

Figure 4 shows an interswitch redundancy configuration. The two switches are connected in a back-to-back configuration using f1/38 on Switch 1 and f2/38 on Switch 2. The access points communicate with the Wireless LAN Services Module through IP address 100.0.0.25, which is the HSRP IP address configured on both Wireless LAN Services Modules.

Figure 4 Sample Interswitch HSRP Topology (One WLSM per Switch)



Switch 1 Configuration

This example shows the configuration of the Wireless LAN Services Module configured with HSRP:

```
wlan vlan 100
ipaddr 100.0.0.200 255.0.0.0
gateway 100.0.0.100
admin
standby 1 ip 100.0.0.25
!
```

This example shows the configuration of the tunnel interface on the Supervisor Engine 720:

```
interface Tunnel252
ip address 113.0.0.1 255.0.0.0
ip helper-address 90.90.90.90
no ip redirects
ip dhcp snooping packets
tunnel source Loopback62
tunnel mode gre multipoint
mobility network-id 252
end
```

This example shows the configuration of the loopback interface. The loopback interface is configured as the source IP address for the tunnel between the Supervisor Engine 720 and the access point:

```
interface Loopback62
ip address 62.0.0.1 255.255.255.255
end
```

This example shows the configuration of VLAN 100. The IP address assigned to VLAN 100 is used as the default gateway on the Wireless LAN Services Module. The Wireless LAN Services Module sends packets destined for the ACS server to the default gateway IP address:

```
interface Vlan100
ip address 100.0.0.100 255.0.0.0
end
```

This example shows the configuration of the interface between the Supervisor Engine 720 in Switch 1 and the Supervisor Engine 720 in Switch 2. This interface can be a trunk or access port. This port carries the VLAN that is used for HSRP. In this example, the two Wireless LAN Services Module use VLAN 100 and HSRP IP address 100.0.0.25.

```
interface FastEthernet1/38
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,6,100
switchport mode trunk
end
```

Switch 2 Configuration

This example shows the configuration of the Wireless LAN Services Module configured with HSRP:

```
wlan vlan 100
ipaddr 100.0.0.250 255.0.0.0
gateway 100.0.0.150
admin
standby 1 ip 100.0.0.25
```

This example shows the configuration of the tunnel interface on the Supervisor Engine 720:

```
interface Tunnel252
ip address 113.0.0.2 255.0.0.0
ip helper-address 90.90.90.90
no ip redirects
ip dhcp snooping packets
tunnel source Loopback62
tunnel mode gre multipoint
mobility network-id 252
mobility trust
end
```

This example shows the configuration of the loopback interface. The loopback interface is configured as the source IP address for the tunnel between the Supervisor Engine 720 and the access point:

```
interface Loopback62
ip address 62.0.0.2 255.255.255.255
end
```

This example shows the configuration of VLAN 100. The IP address assigned to VLAN 100 is used as the default gateway on the Wireless LAN Services Module. The Wireless LAN Services Module sends packets destined for the ACS server to the default gateway IP address:

```
interface Vlan100
ip address 100.0.0.150 255.0.0.0
end
```

This example shows the configuration of the interface between the Supervisor Engine 720 in Switch 2 and the Supervisor Engine 720 in Switch 1. This interface can be a trunk or access port. This port carries the VLAN that is used for HSRP. In this example, the two Wireless LAN Services Module use VLAN 100 and HSRP IP address 100.0.0.25.

```
interface FastEthernet2/38
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,6,100
switchport mode trunk
end
```

Use the **show wlccp wds mobility** command to verify HSRP status:

```
WLSM> show wlccp wds mobility

LCP link status: up
HSRP state: Active
Total # of registered AP: 3
Total # of registered MN: 2

Tunnel Bindings:
Network ID    Tunnel IP         MTU      EPOC ID    FLAGS
==========  ===============  =========  =========  =======
  100       10.80.0.1            1476          0  TB M
  101       10.80.0.2            1476          0  TB M
  102       10.80.0.3            1476          0  TB M
  103       10.80.0.4            1476          0     M

Flags:T=Trusted, B=IP Broadcast enabled, S=TCP MSS Adjust,
      M=IP Multicast enabled, I=MN IP Discovery, N=Nonexistent
```

Use the **show mobility status** command to check the redundancy status of each WLSM on the Supervisor 720:

```
Sup720...#show mobility status

Primary WLAN Module is located in Slot: 1 (HSRP State: Active)
LCP Communication status      : up
Secondary WLAN Module is located in Slot: 2(HSRP State: Standby)
LCP Communication status      : up
WLSM recovery period remaining: 0 seconds
MAC address used for Proxy ARP: 0005.5f54.5800
Number of Wireless Tunnels    : 4
Number of Access Points       : 3
Number of Mobile Nodes        : 1
```

```
Wireless Tunnel Bindings:
Tunnel           Src IP Address   Wireless Network-ID  Flags
---------------  ---------------  -------------------  -------
Tunnel100        10.80.0.1        100                  TB  M
Tunnel101        10.80.0.2        101                  TB  M
Tunnel102        10.80.0.3        102                  TB  M
Tunnel103        10.80.0.4        103                      M
Flags: T=Trusted, B=IP Broadcast enabled, M=IP Multicast enabled
       A=TCP Adjust-mss enabled, D=Discover passive MN's IP address
```

Use the **show redundancy states** command to check the redundancy status on the Supervisor 720:

```
Sup720...#show redundancy states
       my state = 13   -ACTIVE
     peer state = 8    -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 6
Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State = sso

     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up

   client count = 60
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 9000 milliseconds
         keep_alive count = 0
    keep_alive threshold = 18
           RF debug mask = 0x0
```

Note Additional information about supervisor engine redundancy is covered in the "Configuring Supervisor Engine Redundancy" chapter in the *Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2 SX*.

HSRP Configuration Guidelines for Interswitch Topology

The above HSRP examples observe these guidelines:

- NAT tables are not synchronized between the switches; therefore, NAT tables are lost after an interswitch failover.
- In this example, an external DHCP server is mandatory so that the mobile nodes receive the same IP address after an interswitch failover.
- Configure the DHCP server so that it sends both tunnel IP addresses as the default gateways. Although you can specify either of the IP addresses as the default gateway, it is beneficial to the mobile client to see both gateways when they display their IP configuration.
- The Wireless LAN Services Module communicates with the ACS server, the DHCP server, and the Wireless LAN Solution Engine by using the VLAN IP address of the wireless LAN and not the HSRP IP address. Since Router 1 might have equal-cost routes to the VLAN IP subnet of the wireless LAN (100.0.0.0/8), you should configure static routes on Router 1 to reach the VLAN IP addresses of the wireless LAN. For example, Router 1 should point to Switch 1 to reach the Wireless LAN Services Module wireless LAN VLAN IP address in Switch 1, and Router 1 should also point to Switch 2 to reach the Wireless LAN Services Module wireless LAN VLAN IP address in Switch 2.

Note If you do not configure the static routes, Router 1 can still use dynamic routing to send packets to the active Wireless LAN Services Module. However, Router1 sees equal-cost routes for the Wireless LAN Services Module VLAN subnet and uses both switches to send packets to the active Wireless LAN Services Module. As a result, some packets travel an extra hop through the switch with the standby Wireless LAN Services Module. Also, if one of the switches crashes, Router 1 will not know about it immediately, and there is a chance that some packets may be lost during this period.

- The loopback62 interface on both switches is configured with a host route IP address. This IP address is used as the destination IP address for the GRE packets for mobile nodes in tunnel 252. As a result, Router 2 should know the host-specific routes to reach these IP addresses. If OSPF is used, then there will not be any issues because OSPF by default advertises loopback addresses as host routes, and Router 2 can send the tunnel packets to the correct switch.

  For example, if Switch 1 has the active Wireless LAN Services Module, then the access point sends packets to 62.0.0.1, and if Switch 2 has the active Wireless LAN Services Module, then the access point sends packets to 62.0.0.2. Router 2 should know that to reach 62.0.0.1, it need to send packets to Switch 1, and to reach Switch 2, it should send packets to 62.0.0.2.

  Another option is to configure the IP address for the loopback62 interface for each switch in a different subnet, so that Router 2 sees the different subnets from only one switch.

- When using route processor redundancy (RPR) or stateful switchover (SSO), the **standby ip** configuration in the examples is adequate; there is no need to configure other HSRP options.

- When using route processor redundancy plus (RPR+), you should change the default HSRP timer configuration to avoid unnecessary transitions between the Wireless LAN Services Modules after an RPR+ switchover.

  For example, Wireless LAN Services Module 2 (with IP address 100.0.0.250) is the active module and Wireless LAN Services Module 1 (with IP address 100.0.0.200) is the standby module. The HSRP timers are set to the default (hello timer of 3 seconds and holdtime timer of 10 seconds). If an RPR+ switchover occurs on Switch 2, Wireless LAN Services Module 1 becomes active. However, from the Wireless LAN Services Module 2 point of view, it is still active and keeps sending HSRP hellos, but the hellos will not reach Wireless LAN Services Module 1. Once the system is stabilized after the RPR+ switchover, Wireless LAN Services Module 2 starts seeing the hellos from Wireless LAN Services Module 1. Because Wireless LAN Services Module 2 is already in active state and its IP address is higher than that of Wireless LAN Services Module 1, Wireless LAN Services Module 2 sends a coup message to Wireless LAN Services Module 1, which returns to standby state.

  To avoid this unnecessary transition of states, enter the **standby** *group_number* **timers** *hellotime holdtime* command under wireless LAN VLAN configuration on both the Wireless LAN Services Modules to increase the HSRP timers. (For example, set the hello timer to 60 seconds, and set the holdtime timer to 180 seconds.)

Recovering a Lost Password

Note You can download the password recovery script from the Cisco.com software center.

Note You must have access to the supervisor engine to perform the WLSM password recovery procedures. To recover the enable password on the supervisor engine, refer to the software configuration guide for your software platform.

Note To run the password recovery script, the WLSM must be in the application partition (AP).

To recover a lost password on the WLSM, perform this task:

	Command	Purpose
Step 1	`Router> enable`	Initiates enable mode enable.
Step 2	`Router# copy tftp: pclc#`*`mod`*`-fs:`	Downloads the script to the specified module. **Note** You can locate this special image from the Cisco.com software center. The image name ends with **passwd.recovery**.*x.x.x*.**bin** where *x.x.x* is the image version number.
Step 3	`wlan(config)# enable password` *password*	Specifies a local enable password.
Step 4	`wlan(config)# line vty` *starting-line-number ending-line-number*	Identifies a range of lines for configuration and enters line configuration mode.
Step 5	`wlan(config-line)# login`	Enables password checking at login.
Step 6	`wlan(config-line)# password` *password*	Specifies a password on the line.
Step 7	`wlan(config-line)# end`	Exits line configuration mode.
Step 8	`wlan# copy system:running-config nvram:startup-config`	Saves the configuration to NVRAM.
Step 9	`Router# hw-module module` *mod* `reset cf:4`	Resets the module.

This example shows how to recover a lost password on the WLSM that is installed in slot 5:

```
Router> enable
Password:
Router# copy tftp: pclc#5-fs:
Address or name of remote host []? 10.1.1.100
Source filename []? image/c6svc-wlan-k9w7.passwd.recovery.1.1.1.bin
Destination filename [image/c6svc-wlan-k9w7.passwd.recovery.1.1.1.bin]?
Accessing tftp://10.1.1.100/image/c6svc-wlan-k9w7.passwd.recovery.1.1.1.bin...
Loading image/c6svc-wlan-k9w7.passwd.recovery.1.1.1.bin from 10.1.1.100(via Vlan999):!
[OK - 435 bytes]

435 bytes copied in 0.092 secs (4728 bytes/sec)
22:49:10:%SVCLC-SP-5-STRRECVD:mod 5:<MP upgrade/Password Recovery started.>
22:49:10:%SVCLC-SP-5-STRRECVD:mod 5:<Uncompress of the file succeeded. Continuing
upgrade/recovery.>
```

```
22:49:10:%SVCLC-SP-5-STRRECVD:mod 5:<This file appears to be a Password Recovery image.
Continuing.>
22:49:10:%SVCLC-SP-5-STRRECVD:mod 5:<Extraction of password recovery image succeeded.>
22:49:10:%SVCLC-SP-5-STRRECVD:mod 5:<Continuing with password recovery.>

22:49:10:%SVCLC-SP-5-STRRECVD:mod 5:<System in password recovery mode.>
22:49:10:%SVCLC-SP-5-STRRECVD:mod 5:<Please recover configuration and reset board.>

Router#
```

From the Wireless LAN Services Module console port:

```
wlan> enable
wlan# configure termial
    Enter configuration commands, one per line.  End with CNTL/Z.
wlan(config)# enable password cisco
wlan(config)# line vty 0 4
wlan(config-line)# login
% Login disabled on line 4, until 'password' is set
% Login disabled on line 5, until 'password' is set
% Login disabled on line 6, until 'password' is set
% Login disabled on line 7, until 'password' is set
% Login disabled on line 8, until 'password' is set
wlan(config-line)# password cisco
wlan(config-line)# end
wlan# copy system:running-config nvram:startup-config
```

From the supervisor engine:

```
Router# hw-module module 5 reset cf:4
```

Upgrading the Images

The compact Flash on the Wireless LAN Services Module has two bootable partitions: application partition (AP) and maintenance partition (MP). By default, the application partition boots every time. The application partition contains the binaries necessary to run the wireless LAN image. The maintenance partition is booted if you need to upgrade the application partition.

You can upgrade both the application software and the maintenance software. However, you are not required to upgrade both images at the same time. Refer to the release notes for the Wireless LAN Services Module for the latest application partition and maintenance partition software versions.

The entire application and maintenance partitions are stored on the FTP or TFTP server. The images are downloaded and extracted to the application partition or maintenance partition depending on which image is being upgraded.

To upgrade the application partition, change the boot sequence to boot the module from the maintenance partition. To upgrade the maintenance partition, change the boot sequence to boot the module from the application partition. Set the boot sequence for the module using the supervisor engine CLI commands. The maintenance partition downloads and installs the application image. The supervisor engine must be executing the run-time image to provide network access to the maintenance partition.

Before starting the upgrade process, you will need to download the application partition image or maintenance partition image to the TFTP server.

A TFTP or FTP server is required to copy the images. The TFTP server should be connected to the switch, and the port connecting to the TFTP server should be included in any VLAN on the switch.

These sections describe how to upgrade the images:

- Upgrading the Application Software, page 36
- Upgrading the Maintenance Software, page 40

Upgrading the Application Software

How you upgrade the application software depends on whether you are using Cisco IOS software or the Catalyst operating system software.

The following sections describe how to upgrade the application software from the CLI for each switch operating system:

- Cisco IOS Software, page 36
- Catalyst Operating System Software, page 38

Cisco IOS Software

Note Do not reset the module until the image is upgraded. The total time to upgrade the image takes up to eight minutes.

To upgrade the application partition software, perform this task:

	Command	Purpose
Step 1	`Router# hw-module module mod reset cf:1`	Reboots the module from the maintenance partition. **Note** It is normal to see messages such as "Press Key" on the module console after entering this command.
Step 2	`Router# show module mod`	Displays that the maintenance partition for the module has booted.
Step 3	`Router# copy tftp: pclc#mod-fs:`	Downloads the image.
Step 4	`Router# hw-module module mod reset`	Resets the module.
Step 5	`Router# show module mod`	Displays that the application partition for the module has booted.

This example shows how to upgrade the application partition software:

```
Router# hw-module module 3 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning: Device list is not verified.

Proceed with reload of module? [confirm]y

% reset issued for module 3

02:11:18: SP: The PC in slot 3 is shutting down. Please wait ...
02:11:31: SP: PC shutdown completed for module 3
02:11:31: %C6KPWR-SP-4-DISABLED: power to module in slot 3 set off (Reset)
02:14:21: SP: OS_BOOT_STATUS(3) MP OS Boot Status: finished booting
02:14:28: %DIAG-SP-6-RUN_MINIMUM: Module 3: Running Minimum Online Diagnostics...
02:14:34: %DIAG-SP-6-DIAG_OK: Module 3: Passed Online Diagnostics
```

```
02:14:34: %OIR-SP-6-INSCARD: Card inserted in slot 3, interfaces are now online

Router# show module 3

Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  3    1  Wireless LAN Module (MP)               WS-SVC-WLAN-1-K9   SAD0744000Y

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  3  0003.fead.14b4 to 0003.fead.14bb   2.0   7.2(1)       2.1(0.4)m    Ok

Mod Online Diag Status
--- -------------------
3 Pass

Router# copy tftp: pclc#3-fs:
Address or name of remote host []? 10.1.1.1

Source filename []? c6svc-wlan-k9w7.2-x-y.bin

Destination filename [c6svc-wlan-k9w7.2-x-y.bin]?

Accessing tftp://10.1.1.1/c6svc-wlan-k9w7.2-x-y.bin...
Loading c6svc-wlan-k9w7.2-x-y.bin from 10.1.1.1 (via Vlan2):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

<output truncated>

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 14918353 bytes]

14918353 bytes copied in 643.232 secs (23193 bytes/sec)
Router#
02:29:23: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has started>
02:29:23: %SVCLC-SP-5-STRRECVD: mod 3: <Do not reset the module till upgrade completes!!>
02:36:07: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has succeded>
02:36:07: %SVCLC-SP-5-STRRECVD: mod 3: <You can now reset the module>>

Router# hw-module module 3 reset
Device BOOT variable for reset = <empty>
Warning:Device list is not verified.

Proceed with reload of module? [confirm]y
% reset issued for module 3
Router#
02:36:57:SP:The PC in slot 3 is shutting down. Please wait ...
02:37:17:SP:PC shutdown completed for module 3
02:37:17:%C6KPWR-SP-4-DISABLED:power to module in slot 3 set off (Reset)
02:38:39:SP:OS_BOOT_STATUS(3) AP OS Boot Status:finished booting
02:39:27:%DIAG-SP-6-RUN_COMPLETE:Module 3:Running Complete Online Diagnostics...
02:39:29:%DIAG-SP-6-DIAG_OK:Module 3:Passed Online Diagnostics
02:39:29:%OIR-SP-6-INSCARD:Card inserted in slot 3, interfaces are now online
```

```
Router# show module 3

Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  3    1  Wireless LAN Module                    WS-SVC-WLAN-1-K9   SAD0744000Y

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  3  0003.fead.14b4 to 0003.fead.14bb   2.0   7.2(1)       2.x(y)       Ok

Mod Online Diag Status
--- -------------------
  3 Pass
```

Catalyst Operating System Software

Note Do not reset the module until the image is upgraded. The total time to upgrade the image takes up to eight minutes.

To upgrade the application partition software, perform this task:

	Command	Purpose
Step 1	`Console (enable) set boot device cf:1 mod`	Sets the module to boot the maintenance partition.
Step 2	`Console (enable) reset mod`	Resets the module to the maintenance partition. **Note** The SUP_OSBOOTSTATUS system message shows that the maintenance partition (MP) has booted.
Step 3	`Console (enable) show module [mod]`	Displays that the maintenance partition for the module has booted.
Step 4	`Console (enable) session [mod]`	Access the MSFC from the switch CLI using a Telnet session[1].
Step 5	`Router# copy tftp: pclc#mod-fs:`	Downloads the image.
Step 6	`Router# exit`	Exits the MSFC CLI and returns to the switch CLI.
Step 7	`Console (enable) set boot device cf:4 mod`	Sets the module to boot the application partition.
Step 8	`Console (enable) reset mod`	Resets the module to the application partition. **Note** The SUP_OSBOOTSTATUS system message shows that the application partition (AP) has booted.
Step 9	`Console (enable) show module [mod]`	Displays that the application partition for the module has booted.

1. To access the MSFC from the switch CLI directly connected to the supervisor engine console port, enter the **switch console** *mod* command. To exit from the MSFC CLI and return to the switch CLI, press **Ctrl-C** three times at the Router> prompt.

This example shows how to upgrade the application partition software:

```
Console> (enable) set boot device cf:1 6
Device BOOT variable = cf:1
Memory-test set to PARTIAL
Warning:Device list is not verified but still set in the boot string.
Console> (enable)
```

```
Console> (enable) reset 6 cf:1
This command will reset module 6.
Unsaved configuration on module 6 will be lost
Do you want to continue (y/n) [n]? y
Module 6 shut down in progress, please don't remove module until shutdown completed.
Console> (enable) Module 6 shutdown completed. Module resetting...
2003 Jan 17 08:34:07 %SYS-3-SUP_OSBOOTSTATUS:MP OS Boot Status:finished booting
2003 Jan 17 08:34:23 %SYS-5-MOD_OK:Module 6 is online
2003 Jan 17 08:34:23 %DTP-5-TRUNKPORTON:Port 6/1 has become dot1q trunk
Console> (enable) show module 6
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
6   6    1     Secure Socket Layer Module WS-SVC-SSL-1        no  ok

Mod Module-Name          Serial-Num
--- -------------------- -----------
6                        SAD063801FY

Mod MAC-Address(es)                        Hw     Fw         Sw
--- -------------------------------------- ------ ---------- -----------------
6   00-01-64-46-a1-d2                      0.401  7.2(1)     1.2(0.15)m

Console> (enable) session 15
Trying Router-15...
Connected to Router-15.
Type ^C^C^C to switch back...
Router>

Router# copy tftp: pclc#6-fs:
copy tftp: pclc#6-fs:
Address or name of remote host []? 10.1.1.1

Source filename []? c6svc-ssl-k9y9.1-x-y.bin

Destination filename [c6svc-ssl-k9y9.1-x-y.bin]?

Accessing tftp://10.1.1.1/c6svc-ssl-k9y9.1-x-y.bin...
Loading c6svc-ssl-k9y9.1-x-y.bin from 10.1.1.1 (via Vlan2):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

<output truncated>

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 14918353 bytes]

14918353 bytes copied in 643.232 secs (23193 bytes/sec)
Router#
02:29:23: %SVCLC-SP-5-STRRECVD: mod 6: <Application upgrade has started>
02:29:23: %SVCLC-SP-5-STRRECVD: mod 6: <Do not reset the module till upgrade completes!!>
02:36:07: %SVCLC-SP-5-STRRECVD: mod 6: <Application upgrade has succeded>
02:36:07: %SVCLC-SP-5-STRRECVD: mod 6: <You can now reset the module>>
Router# exit
Console> (enable) set boot device cf:4 6
Device BOOT variable = cf:4
Memory-test set to PARTIAL
Warning:Device list is not verified but still set in the boot string.
Console> (enable) reset 6
This command will reset module 6.
Unsaved configuration on module 6 will be lost
Do you want to continue (y/n) [n]? y
Module 6 shut down in progress, please don't remove module until shutdown completed.
Console> (enable) Module 6 shutdown completed. Module resetting...
```

```
2003 Jan 17 08:36:58 %SYS-3-SUP_OSBOOTSTATUS:AP OS Boot Status:finished booting
2003 Jan 17 08:37:51 %SYS-5-MOD_OK:Module 6 is online
2003 Jan 17 08:37:51 %DTP-5-TRUNKPORTON:Port 6/1 has become dot1q trunk
```

Upgrading the Maintenance Software

How you upgrade the maintenance software depends on whether you are using Cisco IOS software or the Catalyst operating system software.

The following sections describe how to upgrade the maintenance software from the CLI for each switch operating system:

- Cisco IOS Software, page 40
- Catalyst Operating System Software, page 41

Cisco IOS Software

Note Do not reset the module until the image is upgraded. The total time required to upgrade the image may be as much as eight minutes.

To upgrade the maintenance partition software, perform this task:

	Command	Purpose
Step 1	`Router#` **`hw-module module`** *`mod`* **`reset`**	Reboots the module from the application partition.
Step 2	`Router#` **`copy tftp: pclc#`***`mod`***`-fs:`**	Downloads the image.
Step 3	`Router#` **`hw-module module`** *`mod`* **`reset cf:1`**	Resets the module in the maintenance partition.
Step 4	`Router#` **`show module`** *`mod`*	Displays that the maintenance partition for the module has booted.

This example shows how to upgrade the maintenance partition software:

```
Router# hw-module module 3 reset
Device BOOT variable for reset = <empty>
Warning:Device list is not verified.
Proceed with reload of module? [confirm]y
% reset issued for module 3
Router#
02:36:57:SP:The PC in slot 3 is shutting down. Please wait ...
02:37:17:SP:PC shutdown completed for module 3
02:37:17:%C6KPWR-SP-4-DISABLED:power to module in slot 3 set off (Reset)
1w0d:SP:OS_BOOT_STATUS(3) AP OS Boot Status:finished booting
1w0d:%OIR-SP-6-INSCARD:Card inserted in slot 3, interfaces are now online
Router# copy tftp:pclc#3-fs:
Address or name of remote host []? 10.1.1.1
Source filename []? mp.3-x-y.bin.gz
Destination filename [mp.3-x-y.bin.gz]?
Accessing tftp://10.1.1.1/mp.3-x-y.bin.gz...
Loading mp.3-x-y.bin.gz from 10.1.1.1 (via Vlan2):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 10380103 bytes]
```

```
10380103 bytes copied in 76.952 secs (134891 bytes/sec)
Router#
1w0d: %SVCLC-SP-5-STRRECVD: mod 3: <MP upgrade/Password Recovery started.>
1w0d: %SVCLC-SP-5-STRRECVD: mod 3: <Uncompress of the file succeeded. Continuing
upgrade/recovery.>
1w0d: %SVCLC-SP-5-STRRECVD: mod 3: <This file appears to be a MP upgrade. Continuing
upgrade.>
1w0d: %SVCLC-SP-5-STRRECVD: mod 3: <Install of the MBR succeeded . Continuing upgrade.>
1w0d: %SVCLC-SP-5-STRRECVD: mod 3: <Install of GRUB succeeded. Continuing upgrade.>
1w0d: %SVCLC-SP-5-STRRECVD: mod 3: <Copying of MP succeeded. Continuing upgrade.>
1w0d: %SVCLC-SP-5-STRRECVD: mod 3: <fsck of MP partition succeeded.>
1w0d: %SVCLC-SP-5-STRRECVD: mod 3: <Upgrade of MP was successful. You can now boot MP.>

Router# hw-module module 3 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning: Device list is not verified.

Proceed with reload of module? [confirm]y
% reset issued for module 3
Router#
1w0d: SP: The PC in slot 3 is shutting down. Please wait ...
1w0d: SP: PC shutdown completed for module 3
1w0d: %C6KPWR-SP-4-DISABLED: power to module in slot 3 set off (Reset)
1w0d: SP: OS_BOOT_STATUS(3) MP OS Boot Status: finished booting
1w0d: %DIAG-SP-6-RUN_MINIMUM: Module 3: Running Minimum Diagnostics...
1w0d: %DIAG-SP-6-DIAG_OK: Module 3: Passed Online Diagnostics
1w0d: %OIR-SP-6-INSCARD: Card inserted in slot 3, interfaces are now online

Router# show module 3
Mod Ports Card Type                              Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  3    1  Wireless LAN Module (MP)               WS-SVC-WLAN-1-K9   SAD0744000Y

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  3  0003.fead.14b4 to 0003.fead.14bb   2.0   7.2(1)       3.x(y)mp     Ok

Mod Online Diag Status
--- -------------------
3 Pass
```

Catalyst Operating System Software

Do not reset the module until the image is upgraded. The total time to upgrade the image takes up to 8 minutes. To upgrade the maintenance partition software, perform this task:

	Command	Purpose
Step 1	`Console (enable) set boot device cf:4 mod`	Sets the module to boot the application partition.
Step 2	`Console (enable) reset mod`	Resets the module to the application partition. **Note** The SUP_OSBOOTSTATUS system message shows that the application partition (AP) has booted.
Step 3	`Console (enable) show module [mod]`	Displays that the maintenance partition for the module has booted.
Step 4	`Console (enable) session [mod]`	Access the MSFC from the switch CLI using a Telnet session[1].

	Command	Purpose
Step 5	Router# **copy tftp: pclc#*mod*-fs:**	Downloads the image.
Step 6	Router# **exit**	Exits the MSFC CLI and returns to the switch CLI.
Step 7	Console (enable) **set boot device cf:1** *mod*	Sets the module to boot the maintenance partition.
Step 8	Console (enable) **reset** *mod*	Resets the module to the maintenance partition. **Note** The SUP_OSBOOTSTATUS system message shows that the maintenance partition (MP) has booted.
Step 9	Console (enable) **show module** [*mod*]	Displays that the application partition for the module has booted.

1. To access the MSFC from the switch CLI directly connected to the supervisor engine console port, enter the **switch console** *mod* command. To exit from the MSFC CLI and return to the switch CLI, press **Ctrl-C** three times at the Router> prompt.

This example shows how to upgrade the maintenance partition software:

```
Console> (enable) set boot device cf:4 6
Device BOOT variable = cf:4
Memory-test set to PARTIAL
Warning:Device list is not verified but still set in the boot string.
Console> (enable) reset 6
This command will reset module 6.
Unsaved configuration on module 6 will be lost
Do you want to continue (y/n) [n]? y
Module 6 shut down in progress, please don't remove module until shutdown completed.
Console> (enable) Module 6 shutdown completed. Module resetting...
2003 Jan 17 08:36:58 %SYS-3-SUP_OSBOOTSTATUS:AP OS Boot Status:finished booting
2003 Jan 17 08:37:51 %SYS-5-MOD_OK:Module 6 is online
2003 Jan 17 08:37:51 %DTP-5-TRUNKPORTON:Port 6/1 has become dot1q trunk
Console> (enable) session 15
Trying Router-15...
Connected to Router-15.
Type ^C^C^C to switch back...
Router>
Router# copy tftp:pclc#6-fs:
Address or name of remote host []? 10.1.1.1
Source filename []? mp.1-2-0-16.bin.gz
Destination filename [mp.1-2-0-16.bin.gz]?
Accessing tftp://10.1.1.1/mp.1-2-0-16.bin.gz...
Loading mp.1-2-0-16.bin.gz from 10.1.1.1 (via Vlan2):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output truncated>

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 9818951 bytes]

9818951 bytes copied in 164.388 secs (59730 bytes/sec)
ssl-proxy>
1w0d:%SVCLC-SP-6-STRRECVD:mod 6:<MP upgrade started. Do not reset the card.>
1w0d:%SVCLC-SP-6-STRRECVD:mod 6:<Upgrade of MP was successful. You can now boot MP.>
Router# exit
Console> (enable) set boot device cf:1 6
Device BOOT variable = cf:1
Memory-test set to PARTIAL
Warning:Device list is not verified but still set in the boot string.
Console> (enable)
Console> (enable) reset 6 cf:1
This command will reset module 6.
Unsaved configuration on module 6 will be lost
```

```
Do you want to continue (y/n) [n]? y
Module 6 shut down in progress, please don't remove module until shutdown completed.
Console> (enable) Module 6 shutdown completed. Module resetting...
2003 Jan 17 08:34:07 %SYS-3-SUP_OSBOOTSTATUS:MP OS Boot Status:finished booting
2003 Jan 17 08:34:23 %SYS-5-MOD_OK:Module 6 is online
2003 Jan 17 08:34:23 %DTP-5-TRUNKPORTON:Port 6/1 has become dot1q trunk
```

Related Documentation

For more detailed installation and configuration information, refer to the following publications:

- *Release Notes for Catalyst 6500 Series Wireless LAN Services Module*
- *Catalyst 6500 Series Wireless LAN Services Module Installation and Verification Note*
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Switch Software Configuration Guide*
- *Catalyst 6500 Series Switch Command Reference*
- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*
- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Instructions for ordering documentation using the Ordering tool are at this URL:

  http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/