Configuring a Cisco Wireless Services Module and Wireless Control System

Last Revised: April 08, 2009

This document provides a technical overview of the Cisco Wireless Services Module (WiSM) and software extensions to the Supervisor 720 and Cisco Wireless Control System (WCS). It is not an extensive tutorial on wireless LAN technology or a deployment guide. You should work closely with your Cisco account representative if you need more detailed deployment information on the Cisco unified wireless network.

The guide includes the following information and procedures for configuring and deploying the Cisco WiSM:

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

Key Terms

Table 1 defines key terms used throughout this document.

Table 1 Key Terms

Term or Acronym	Definition
Cisco WiSM	Cisco wireless services module.
WLC	Cisco wireless LAN controller - Cisco devices that centrally manage lightweight access points and wireless LAN data traffic.
WCS	Cisco wireless control system - Management software that manages WLC devices and adds advanced management like location-based services
Lightweight Access Point	An access point running software that makes the access point work with the WLCs.
LWAPP	Lightweight Access Point Protocol - IETF draft protocol used in the Cisco unified wireless network architecture implementations. LWAPP defines both control and data encapsulation formats used in the Cisco unified wireless network architecture.

Cisco WiSM Concepts

The Cisco WiSM is a member of the Cisco wireless LAN controller family. It works in conjunction with Cisco Aironet lightweight access points, the Cisco WCS, and the Cisco wireless location appliance to deliver a secure and unified wireless solution that supports wireless data, voice, and video applications. The Cisco WiSM consists of two Cisco 4404 controllers; therefore, the IT staff must be aware that two separate controllers exist on a single module. The first controller is considered the WiSM-A card, while the second controller is considered the WiSM-B card. Interfaces and IP addressing have to be considered on both cards independently. WiSM-A manages 150 access points, while WiSM-B manages a separate lot of 150 access points. These controllers can be grouped together in a mobility group, forming a *cluster*.

There are multiple types of interfaces on each controller of the Cisco WiSM: three of them are pre-defined types that must be present and that are configured at setup time:

- Management interface (pre-defined and mandatory)
- AP-Manager interface (pre-defined and mandatory)
- Virtual interface (pre-defined and mandatory)
- Service-port interface (pre-defined and mandatory)
- Operator-defined interface (user-defined)

The *management interface* is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA server. If the service port is in use, the management interface must be on a different subnet than the service port.

The *AP-Manager interface* is used as the source IP address for all Layer 3 communications between the controller and the lightweight access points. The AP-Manager must have a unique IP address and should be on the same subnet as the management interface.

Note You cannot ping the AP-Manager interface.

The *virtual gateway interface* is used to support mobility management, DHCP relay, and embedded Layer 3 security, like guest web authentication and VPN termination. The virtual interface must be configured with an unassigned and unused gateway IP address. If multiple controllers are configured in a mobility group, the virtual interface must be the same on all controllers for seamless roaming.

The *service-port interface* is mapped only to the physical service port. The service port interface must have an IP address on a different subnet from the management and AP-Manager interfaces. A default-gateway cannot be assigned to the service-port interface, but static routes can be defined through the controller command-line interface for remote network access to the service port.

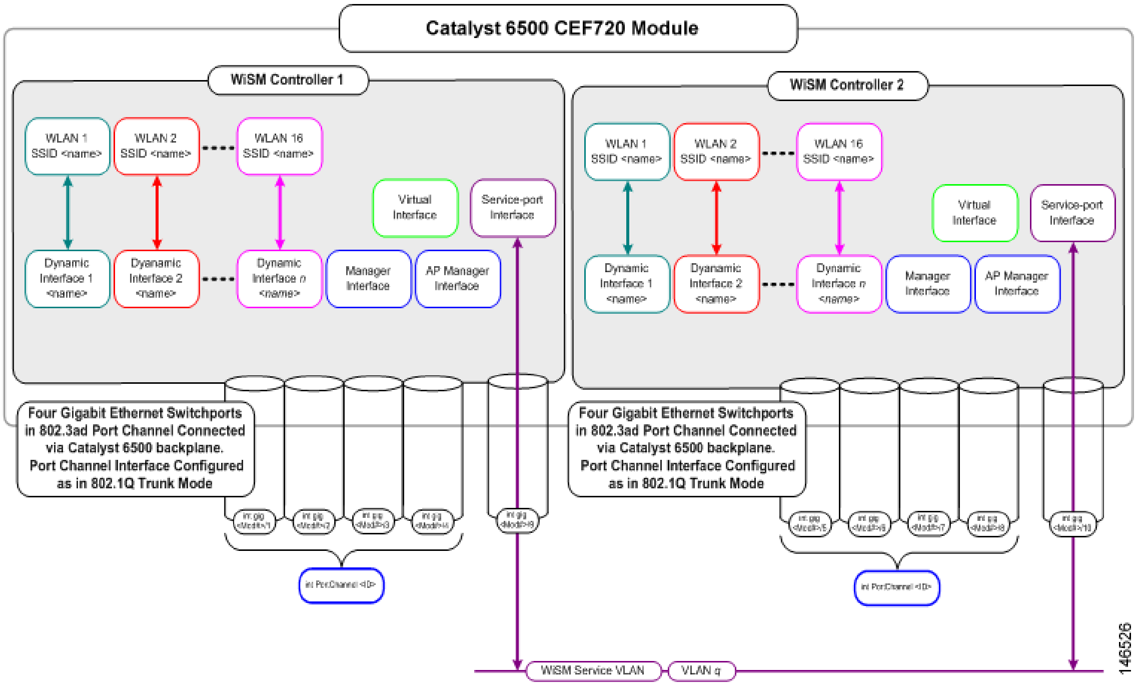
Note On the WiSM, the service port is used to synchronize the supervisor engine and the WiSM.

Each Cisco wireless LAN controller can support up to 512 *operator-defined interfaces*. Each operator-defined interface controls VLAN and other communications between controllers and all other network devices connected to an individual physical port.

Up to 16 WLANs can be configured per controller. A WLAN designation associates an SSID to an interface and is configured with security, quality of service (QoS), radio policies, and other parameters specific to the WLAN.

Figure 1 illustrates the typical relationship between the ports and the interfaces.

Figure 1 Relationship Between Ports and Interfaces



Another Cisco unified wireless network architecture concept is *mobility group*. A mobility group is a cluster of controllers. Wireless devices can roam seamlessly within a mobility group. WLC devices within a mobility group also coordinate dynamic radio management calculations for the access points within the mobility group. For Cisco WiSM, both the WiSM modules should be part of the same mobility group for seamless routing among 300 access points. Each Catalyst 6500 chassis supports five Cisco WiSMs (up to 1500 access points). Each Cisco wireless LAN controller cluster supports 12 Cisco WiSMs (up to 3600 access points).

Note The Catalyst 6500 Series Switch chassis can support up to five Cisco WiSMs without any other service module installed. If one or more service modules are installed, the chassis can support up to a maximum of four service modules (WiSMs included).

Configuration Rules

When structured as the logical network diagram shown in Figure 1, the following rules apply to configure the Cisco WiSM.

General Rules

These general rules apply:

- Both tagged and untagged VLAN interfaces are supported in any combination.
- Layer 3 LWAPP mode is the only supported mode in Cisco WiSM.
- A single access point manager interface is needed to support 150 access points per Cisco WiSM.

Interface Assignment Rules

These management interface rules apply:

- Make the management interface untagged or tagged.
- The management interface can be on the same subnet as the AP manager IP address, but must have a different IP address than the AP manager interface.

This AP manager interface rules applies:

- The AP manager interface can be on the same subnet as the management IP address, but must have a different IP address than the management interface.

These dynamic interface rules apply:

- 0, 1, or multiple dynamic interfaces may be configured on a port.
- All dynamic interfaces must be on a different VLAN/IP subnet than any other interfaces configured on the port. If the port is untagged, all dynamic interfaces must be on a different IP subnet than any other interfaces configured on the port.

Configuration Overview

The following procedures are required to set up the Cisco WiSM:

- Verifying the Hardware and Software, page 5
- Configuring Communication Between the Supervisor 720 and Cisco WiSM, page 7
- Configuring the Cisco WiSM-A, page 11 or Configuring Cisco WiSM-B, page 15

Verifying the Hardware and Software

Before configuring the Cisco WiSM, verify that the proper versions of the hardware and software are installed for the following:

- Supervisor 720
- Cisco WiSM
- Cisco Secure ACS
- Cisco Wireless Control System

Hardware Components

The Catalyst 6500 or Cisco 7600 chassis in which the Cisco WiSM is installed needs a Supervisor 720 module. The supported slots for the Cisco WiSM are shown in the *WiSM Troubleshooting FAQ* (document 70608) at this URL:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_qanda_item09186a00806e39b7.shtml

The Cisco WiSM module needs 254.94 Watts for its operation. Ensure that your Catalyst chassis provides the necessary power. All Catalyst 6500 chassis except the Catalyst 6503 require the fan tray 2 module, which in turn requires the 2500-W power supply for proper operation. The 2500-W power supplies use a 20-A circuit with a NEMA plug.

Before proceeding, ensure that the module is detected by the supervisor and that the status LED is green. If the status LED is not green, the supervisor may not have the correct software release to detect the Cisco WiSM module or to detect a hardware problem in the module. The output from a **show module** command specifies that the Cisco WiSM module is installed in slot 3.

```
Sup720#sh mod
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  3   10  WiSM WLAN Service Module            WS-SVC-WiSM-1-K9   SAD100604C4
  4   48  48-port 10/100 mb RJ45                 WS-X6148-45AF      SAL08154UT3
  5    2  Supervisor Engine 720 (Active)         WS-SUP720-3BXL     SAL0913827E

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  3  0016.4625.c838 to 0016.4625.c8471.2   12.2(14r)S5  12.2(18)SXF2 Ok
  4  0011.206d.7ef0 to 0011.206d.7f1f   1.0    5.4(2)       8.5(0.46)RFW Ok
  5  0013.7f0d.114c to 0013.7f0d.114f   4.3    8.1(3)       12.2(18)SXF2 Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
  3  Centralized Forwarding Card WS-SVC-WISM-1-K9-D SAD100605LG  1.2     Ok
  4  IEEE Voice Daughter Card    WS-F6K-FE48-AF     SAD082007YH  1.1     Ok
  5  Policy Feature Card 3       WS-F6K-PFC3BXL     SAL091597AS  1.6     Ok
  5  MSFC3 Daughterboard         WS-SUP720          SAL09158X9K  2.3     Ok
```

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

Software Components

The minimum software requirements to support Cisco WiSM module are given in Table 2:

Table 2 Software Components

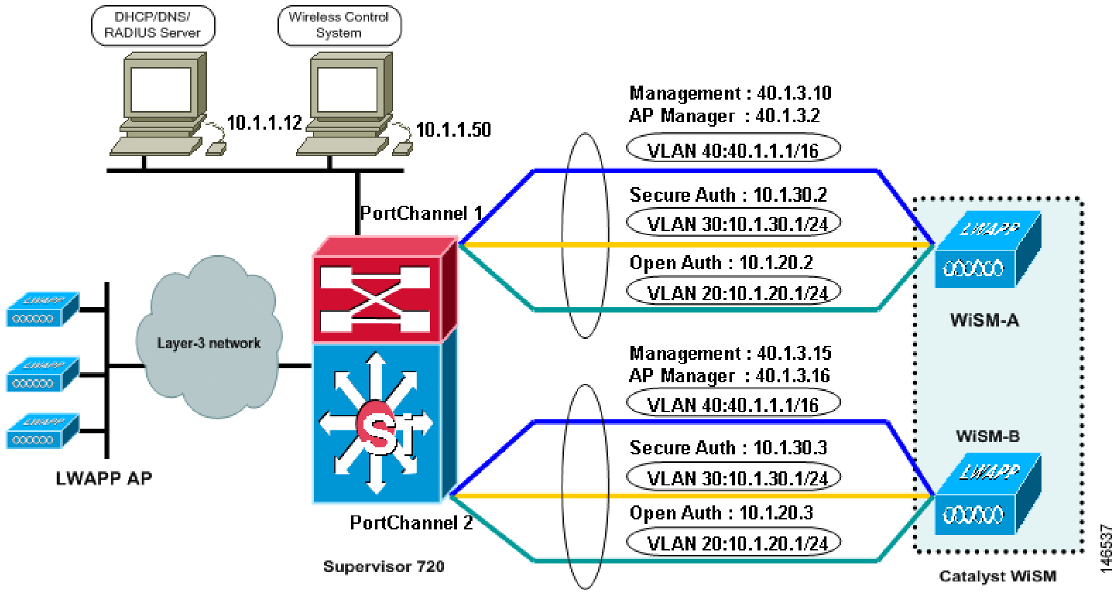
Component	Minimum Software Release
Supervisor 720	12.2(18)SXF2 [or 12.2(18)SXF5 if using Cisco IOS Software Modularity]
Cisco WiSM	3.2.78.4 (or 4.0.155.5 if using Cisco IOS Software Modularity)
Cisco Secure ACS Server	2.6 or above
Cisco Wireless Control System	3.2.33.0 or above

Note The Cisco WiSM is supported on Cisco 7609 and 7613 Series Routers running only Cisco IOS Release 12.2(18)SXF5 or higher.

Topology Example

Figure 2 illustrates the topology on which the configuration examples in this document are based.

Figure 2 Topology Example



In the configuration example, the Cisco WiSM is installed in slot 3 of the Catalyst 6506 chassis. Two WLANs are configured: one for open authentication (SSID “open”) and one for EAP authentication (SSID “secure”). Dynamic interfaces are created for the open SSID and the EAP SSID and are mapped to the appropriate VLAN. For open SSID, VLAN 20 is used; for EAP SSID, VLAN 30 is used. The management and AP-Manager interfaces are configured to use VLAN 40. All network services (AAA, DHCP, and DNS) are configured on VLAN 1. The WCS is also on VLAN 1.

Configuring Communication Between the Supervisor 720 and Cisco WiSM

If you are using a software release between 12.2.18SXF2 and 12.2.18SXF5, eight Gigabit interfaces are created ranging from Gig3/1 to Gig3/8 after the Cisco WiSM controller is detected by the Supervisor. In this case, the Cisco WiSM controller is installed in slot 3. See Configuring Communication Between the Supervisor 720 and Cisco WiSM Using 12.2.18SXF2 to 12.2.18SXF5, page 7

If you are using software release 12.2.18SXF6, you will not be able to configure the Gigabit interfaces. See Configuring Communication Between the Supervisor 720 and Cisco WiSM Using 12.2.18SXF6, page 9.

Configuring Communication Between the Supervisor 720 and Cisco WiSM Using 12.2.18SXF2 to 12.2.18SXF5

```
! -- Create the vlan in the Supervisor 720 to communicate with the management and
ap-manager ports of the Cisco WiSM controller.

Sup720(config)# vlan 40
Sup720(config)# description Management VLAN for WiSM

! -- Assign an appropriate IP address and subnet mask for VLAN 40

Sup720(config)# interface Vlan40
Sup720(config-if)# ip address 40.1.1.1 255.255.0.0
Sup720(config-if)# no shutdown
Sup720(config-if)# exit
! - Create two port-channel interfaces for the two independent controllers in the Cisco
WiSM and assign vlan 40 as the native interface.

Sup720(config)# interface Port-channel 1
Sup720(config-if)# switchport
Sup720(config-if)# switchport trunk encapsulation dot1q
Sup720(config-if)# switchport trunk native vlan 40
Sup720(config-if)# switchport mode trunk
Sup720(config-if)# mls qos trust dscp
Sup720(config-if)# spanning-tree portfast
Sup720(config)# interface Port-channel 2
Sup720(config-if)# switchport
Sup720(config-if)# switchport trunk encapsulation dot1q
Sup720(config-if)# switchport trunk native vlan 40
Sup720(config-if)# switchport mode trunk
Sup720(config-if)# mls qos trust dscp
Sup720(config-if)# spanning-tree portfast

! -- Configure the below Giga-bit interfaces as trunk ports with vlan 40 as the native
vlan (please make sure that native vlan is not getting tagged while doing the Cisco WiSM
configuration).
```

The Gigabit interfaces 3/1 to 4 correspond to the first controller in Cisco WiSM and should be a member of channel group one.

```
Sup720(config)# interface range GigabitEthernet3/1-4
Sup720(config-if)# switchport
Sup720(config-if)# switchport trunk encapsulation dot1q
Sup720(config-if)# switchport mode trunk
Sup720(config-if)# switchport trunk native vlan 40
Sup720(config-if)# spanning-tree portfast
Sup720(config-if)# channel-group 1 mode on
Sup720(config-if)# no shutdown
Sup720(config-if)# exit
```

Similarly, the Gigabit interfaces 3/5-8 correspond to the second controller in Cisco WiSM and should be a member of channel group two.

```
Sup720(config)# interface range GigabitEthernet3/5-8
Sup720(config-if)# switchport
Sup720(config-if)# switchport trunk encapsulation dot1q
Sup720(config-if)# switchport mode trunk
Sup720(config-if)# switchport trunk native vlan 40
Sup720(config-if)# spanning-tree portfast
Sup720(config-if)# channel-group 2 mode on
Sup720(config-if)# no shutdown
Sup720(config-if)# exit

! - Create a vlan in the Supervisor 720, this vlan is local to the chassis and is used for
communication between Cisco WiSM and Catalyst Supervisor 720 over a Gigabit interface on
the Supervisor and service-port in the Cisco WiSM.

Sup720(config)# vlan 192

! -- Assign an appropriate IP address and subnet mask for VLAN 192

Sup720(config)# interface Vlan 192
Sup720(config-if)# ip address 192.168.10.1 255.255.255.0
Sup720(config-if)# no shutdown
Sup720(config-if)# exit
```

Create a DHCP scope for the service port of the Cisco WiSM in Supervisor 720 or on a standalone DHCP server. Then associate the above VLAN for the service port.

```
Sup720(config)# ip dhcp pool wism-service-port
Sup720(dhcp-config)#network 192.168.10.0 255.255.255.0
Sup720(dhcp-config)#default-router 192.168.10.1


! -- Configure the following command to use vlan 192 to communicate with the service-port.


Sup720(config)# wism service-vlan 192
```

Use the **show wism status** command to verify that the Cisco WiSM received an IP address from the DHCP server.

```
Sup720#sh wism status

Service Vlan : 192, Service IP Subnet : 192.168.10.1/255.255.255.0
      WLAN
Slot  Controller  Service IP       Management IP    SW Version Status
----+-----------+----------------+-------------------------+-----------+---------------
3       1      192.168.10.3       169.254.1.1    3.2.63.0       Oper-Up
3       2      192.168.10.4       169.254.1.1    3.2.63.0       Oper-Up

Sup720#
```

Configuring Communication Between the Supervisor 720 and Cisco WiSM Using 12.2.18SXF6

Note The configuration methods used for SXF2-5 are still relevant for SXF6 and later. The new configuration methods are intended to ease the tasks and to reduce mistakes from manual configurations.

Note By making the process automatic, the configurations are not as flexible as configuring the interfaces and port channels manually. Continue to use the manual LAG to make changes in the Gigabit interfaces configuration.

Note Using auto-configuration may limit the ability to make essential network changes and may require you to disable, reconfigure, and re-enable your wireless network.

```
! -- Create the vlan in the Supervisor 720 to communicate with the management and
ap-manager ports of the Cisco WiSM controller.

Sup720(config)# vlan 40
Sup720(config)# description Management VLAN for WiSM

! -- Assign an appropriate IP address and subnet mask for VLAN 40
Sup720(config-if)# interface Vlan40
Sup720(config-if)# description Management VLAN for WiSM
Sup720(config-if)# ip address 40.1.1.1 255.255.0.0
Sup720(config-if)# no shutdown
Sup720(config-if)# exit
```

The Supervisor automatically creates two port-channel interfaces for the two independent controllers in the Cisco WiSM as soon as the module is detected. Usually the port-channels have a high number such as 287 and 288 as shown below.

```
Sup720#sh ip int brief|  inc Port
Port-channel1287          unassigned    YES unset  administratively down down
Port-channel1288          unassigned    YES unset  administratively down down
```

The following commands can be used to configure the port-channel with native and allowed VLANs. In this case, VLAN 40 is added as the native VLAN.

Note Ensure that the native VLAN is not tagged while doing the Cisco WiSM configuration.

```
Sup720(config)# wism module 3 controller 1 ?
    allowed-vlan
    native-vlan
Sup720(config)# wism module 3 controller 1 native-vlan 40
Sup720(config)# wism module 3 controller 2 native-vlan 40
```

Note If you have a WiSM trunk that includes VLANs in the range of 1 to 1000 and you intend to use only 1 to 10, enter the following command:

```
no wism module x controller y allowed-vlan 11-1000
```

The Gigabit interface 3/1 to 4 corresponding to the first controller in the Cisco WiSM are automatically assigned to channel group 287 and the necessary commands are added automatically.

```
interface GigabitEthernet3/1-4
    switchport
    switchport trunk encapsulation dot1q
    switchport trunk native vlan 40
    switchport mode trunk
    switchport nonegotiate
    no ip address
    no snmp trap link-status
    mls qos trust cos
    no cdp enable
    channel-group 287 mode on
end
```

Similarly, the Gigabit interfaces 3/5 to 8 corresponding to the second controller in the Cisco WiSM should be members of channel group 288.

```
interface GigabitEthernet3/5-8
    switchport
    switchport trunk encapsulation dot1q
    switchport trunk native vlan 40
    switchport mode trunk
    switchport nonegotiate
    no ip address
    no snmp trap link-status
    mls qos trust cos
    no cdp enable
    channel-group 288 mode on
end
```

Additionally, Cisco recommends allowing only VLANs that are configured in the Cisco WiSM through the port-channel and Gigabit interfaces with the following command. Later in the example, VLAN30 is created in the Cisco WiSM and mapped to a secure SSID.

```
Sup720(config)# wism module 3 controller 1 allowed-vlan 30,40
Sup720(config)# wism module 3 controller 2 allowed-vlan 30,40

! - Create a vlan in the Supervisor 720, this vlan is local to the chassis and is used for
communication between Cisco WiSM and Catalyst Supervisor 720 over a Gigabit interface on
the Supervisor and service-port in the Cisco WiSM.

Sup720(config)# vlan 192

! -- Assign an appropriate IP address and subnet mask for VLAN 192

Sup720(config)# interface Vlan 192
Sup720(config-if)# ip address 192.168.10.1 255.255.255.0
Sup720(config-if)# no shutdown
Sup720(config-if)# exit
```

Create a DHCP scope for the service port of the Cisco WiSM in the Supervisor 720 or on a standalone DHCP server. Then associate the above VLAN for the service port.

```
Sup720(config)# ip dhcp pool wism-service-port
Sup720(dhcp-config)#network 192.168.10.1 255.255.255.0
Sup720(dhcp-config)#default-router 192.168.10.1
```

```
! -- Configure the following command to use vlan 192 to communicate with the service-port.
Sup720(config)# wism service-vlan 192
```

Use the **show wism status** command to verify that the Cisco WiSM received an IP address from the DHCP server.

```
Sup720#show wism status

Service Vlan :  192, Service IP Subnet  192.168.10.1/255.255.255.0
        WLAN
Slot    Controller  Service IP     Management IP      SW Version   Status
----+--------------+----------------+--------------------+------------+--------------
3       1           192.168.10.3      0.0.0.0           4.0.155.5
Service Port Up
3       2           192.168.10.4      0.0.0.0           4.0.155.5

Sup720#show wism mod 3 controller 2 status

WiSM Controller 2 in Slot 3
Operational Status of the Controller  : Oper-Up
Service VLAN                          : 192
Service Port                          : 10
Service Port Mac Address              : 0011.92ff.8742
Service IP Address                    : 192.168.10.4
Management IP Address                 : 40.1.3.15
Software Version                      : 4.0.155.5
Port Channel Number                   : 288
Allowed vlan list                     : 30,40
Native VLAN ID                        : 40
WCP Keep Alive Missed                 : 0
```

Configuring the Cisco WiSM-A

The initial configuration of the Cisco WiSM controller consists of initiating a session from the supervisor. The Cisco WiSM controller is inserted into the appropriate slot and powered up. After the administrator establishes a session with the Cisco WiSM, the basic configuration is completed with the help of the setup script. With the completion of basic configuration, the administrator can configure the Cisco WiSM controller through the console CLI or through the Cisco WiSM controller web-interface. An administrator needs to configure WiSM-A and WiSM-B separately in the Cisco WiSM module, initially from the CLI and then from the web interface. Refer to Configuring Cisco WiSM-B, page 15 for steps for configuring the WiSM-B.

The system name, Cisco WiSM controller administrative user credentials, the management, the AP manager, virtual interfaces, the mobility group name, one SSID, a RADIUS server, and other options are configured by the setup script. For the management interface, leave the VLAN untagged because it corresponds to the native VLAN on the switch trunk port. For a Cisco WiSM controller, an untagged VLAN is assigned VLAN number 0, which may not correspond to the VLAN number on the switchport. In our example, the switchport's native VLAN is VLAN number 40; but on the Cisco WiSM controller, the management interface is assigned to VLAN 0. In our example, the default values for the other options are accepted.

The syntax for the **session** command to access to Cisco WiSM from the supervisor is as follows:

```
Sup720t# session  slot <Module # > processor < Proc #>
```

In this example, the module is installed in slot 3, and processor number one is configured first (such as, WiSM-A).

```
Sup720# sess slot 3 proc 1
```

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

You can also type **exit** at the remote prompt to end the session.

```
Trying 192.168.10.3 ... Open

(WiSM-slot3-1)
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_ff:87:23]:
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Service Interface IP Address Configuration [none][DHCP]: dhcp
Management Interface IP Address: 40.1.3.10
Management Interface Netmask: 255.255.0.0
Management Interface Default Router: 40.1.1.1
Management Interface VLAN Identifier (0 = untagged):
Management Interface DHCP Server IP Address: 10.1.1.12
AP Transport Mode [layer2][LAYER3]: layer3
AP Manager Interface IP Address: 40.1.3.2
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.1.1.12):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: mobile-1
Network Name (SSID): secure-1
Allow Static IP Addresses [YES][no]: no
Configure a RADIUS Server now? [YES][no]: yes
Enter the RADIUS Server's Address: 10.1.1.12
Enter the RADIUS Server's Port [1812]:
Enter the RADIUS Server's Secret: cisco
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: YES
Enable 802.11a Network [YES][no]: YES
Enable 802.11g Network [YES][no]: YES
Enable Auto-RF [YES][no]:
Configuration saved!
```

The following command verifies the status of all of the above interfaces in the Cisco WiSM.

```
(WiSM-slot3-1) >show interface summary
Interface Name                Port    Vlan Id    IP Address     Type       Ap Mgr
_______________               _____   ________   ___________    ____       ______
ap-manager                    LAG     untagged  40.1.3.2        Static     Yes
management                    LAG     untagged   40.1.3.10      Static     No
service-port                  N/A     N/A        192.168.10.3   Static     No
virtual                       N/A     N/A        1.1.1.1        Static     No
```

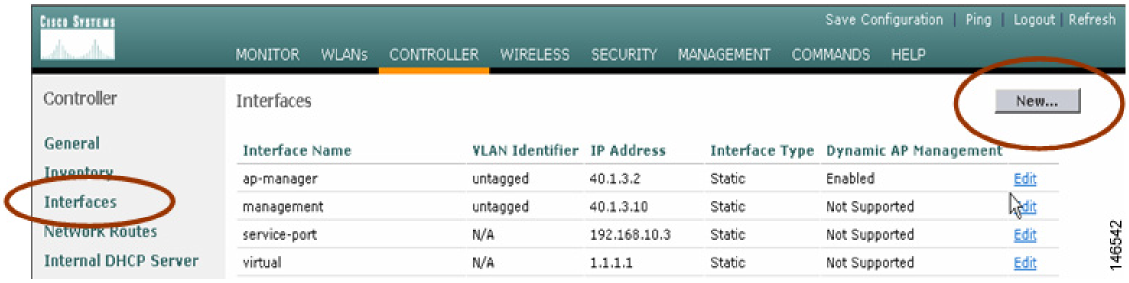
After executing the above configuration on the Cisco WiSM, execute the following commands in the Supervisor 720 to verify the status of the controller.

```
Sup720#show wism status
Service Vlan : 192, Service IP Subnet : 192.168.10.1/255.255.255.0
      WLAN
Slot  Controller  Service IP       Management IP    SW Version  Status
----+-----------+----------------+----------------+-----------+---------------
3     1           192.168.10.3     40.1.3.10        3.2.63.0 Oper-Up
3     2           192.168.10.4     169.254.1.1  3.2.63.0     Oper-Up

Sup720#show wism mod 3 cont 1 status

WiSM Controller 1 in Slot 3
Operational Status of the Controller : Oper-Up
Service VLAN                          : 192
Service Port                              : 9
Service Port Mac Address                     : 0011.92ff.8722
Service IP Address                        : 192.168.10.3
Management IP Address                     : 40.1.3.10
Software Version                          : 3.2.63.0
WCP Keep Alive Missed                     :0
```

Use the web interface for all configuration of the Cisco WiSM from this point forward. Open the controller web interface by opening the IE browser and point it to the management interface IP address. Only HTTPS is on by default. The URL is https://<management_IP>.

Step 1 Create dynamic interfaces for both VLAN 20 and VLAN 30 through the controller web interface. Navigate to Controller > Interfaces and click the **New** button (see Figure 3).

Figure 3 Controller > Interfaces

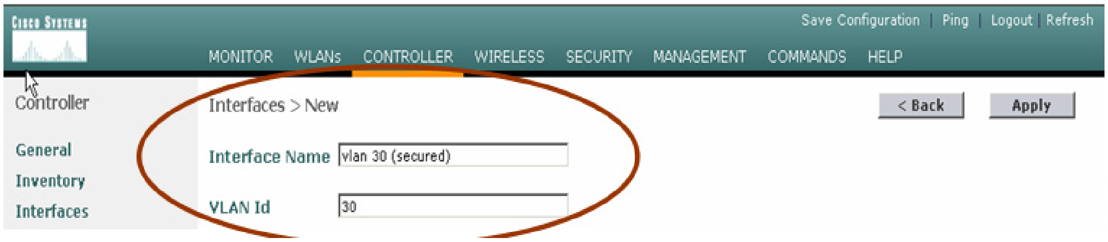


Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	
ap-manager	untagged	40.1.3.2	Static	Enabled	Edit
management	untagged	40.1.3.10	Static	Not Supported	Edit
service-port	N/A	192.168.10.3	Static	Not Supported	Edit
virtual	N/A	1.1.1.1	Static	Not Supported	Edit

Enter an interface name and VLAN tag. Click **Apply**. Figure 4 illustrates the configuration of the VLAN 30 interface.

Figure 4 Entering an Interface Name and VLAN Tag



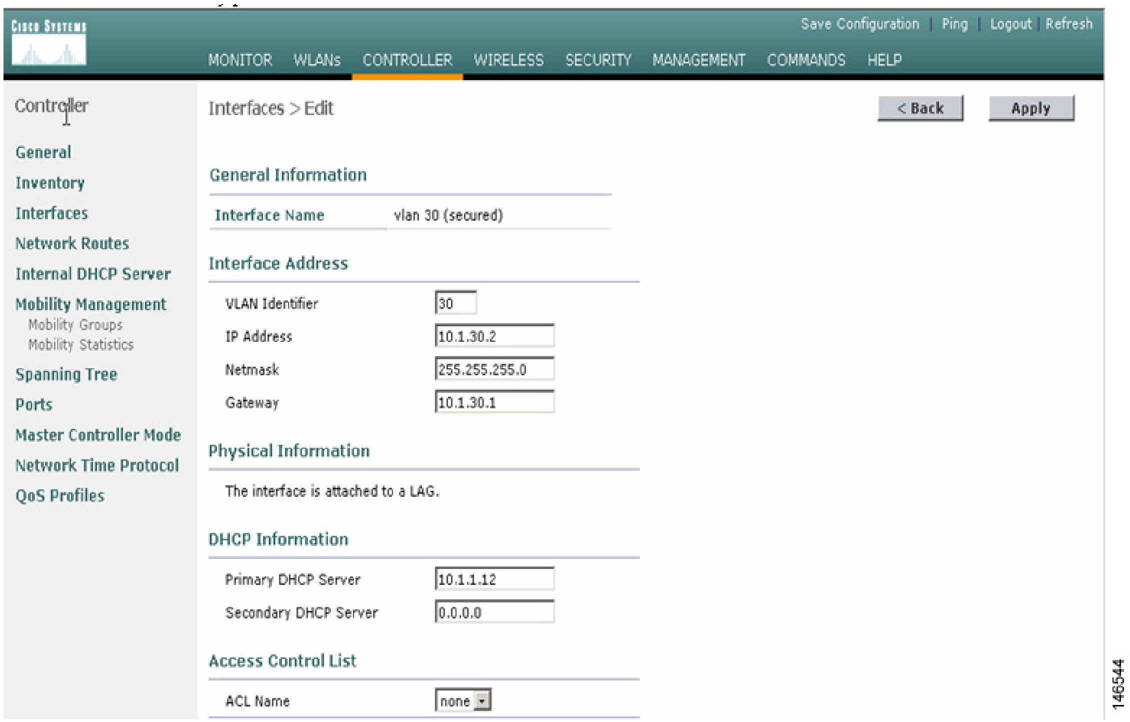
Interfaces > New

Interface Name: vlan 30 (secured)

VLAN Id: 30

Step 2 Enter the appropriate information in the next form and click **Apply** (see Figure 5). The primary DHCP server parameter is mandatory.

Figure 5 Controller > Interfaces > Edit



Interfaces > Edit

General Information

Interface Name vlan 30 (secured)

Interface Address

VLAN Identifier 30

IP Address 10.1.30.2

Netmask 255.255.255.0

Gateway 10.1.30.1

Physical Information

The interface is attached to a LAG.

DHCP Information

Primary DHCP Server 10.1.1.12

Secondary DHCP Server 0.0.0.0

Access Control List

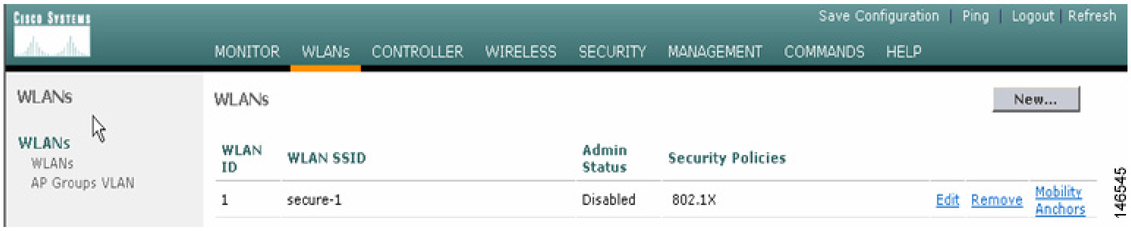
ACL Name none

Repeat this process for each dynamic interface.

Navigate to WLANs > WLANs > WLANs interface to configure WLANs. The WLAN configured with the setup script *secure-1* should be listed (see Figure 6). The WLAN is by default mapped to the management interface and is moved to the VLAN 30 interface in the example.

Step 3 Choose the **Edit** link (see Figure 6).

Figure 6 Choosing Edit

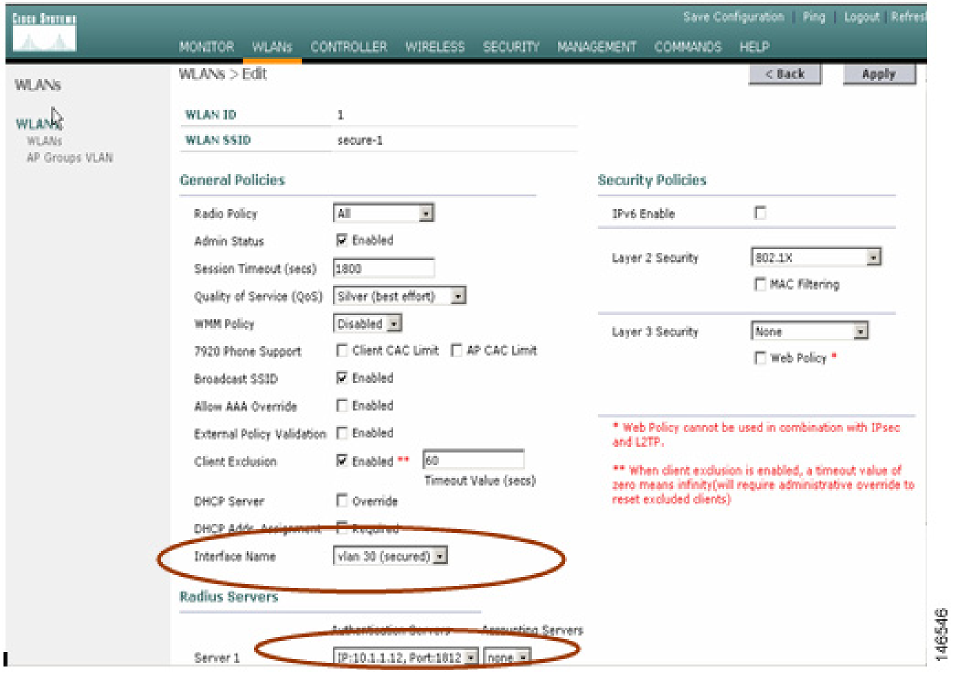

Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
New...
146545

WLANs

WLAN ID	WLAN SSID	Admin Status	Security Policies			
1	secure-1	Disabled	802.1X	Edit	Remove	Mobility Anchors

Step 4 Change the Interface Name parameter to the appropriate VLAN. Other security parameters, such as the appropriate RADIUS server and encryption settings, must also be configured. After the configuration is complete, click **Apply** (see Figure 7).

Figure 7 Completing the Configuration



WLANs > Edit

WLAN ID	1
WLAN SSID	secure-1

General Policies

Radio Policy	All
Admin Status	☑ Enabled
Session Timeout (secs)	1800
Quality of Service (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Phone Support	□ Client CAC Limit □ AP CAC Limit
Broadcast SSID	☑ Enabled
Allow AAA Override	□ Enabled
External Policy Validation	□ Enabled
Client Exclusion	☑ Enabled ** 60 Timeout Value (secs)
DHCP Server	□ Override
DHCP Addr. Assignment	□ Required
Interface Name	vlan 30 (secured)

Security Policies

IPv6 Enable	□
Layer 2 Security	802.1X □ MAC Filtering
Layer 3 Security	None □ Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:10.1.1.12, Port:1812	none

Step 5 Add a WLAN for the open SSID by clicking **New** and completing the configuration form as appropriate.

Configuring Cisco WiSM-B

Establish a session with Cisco WiSM-B from the supervisor and use the initial script to configure the controller.

```
Sup720# sess slot 3 proc 2
```

The default escape character is Ctrl-^ and then x. You can also type **exit** at the remote prompt to end the session.

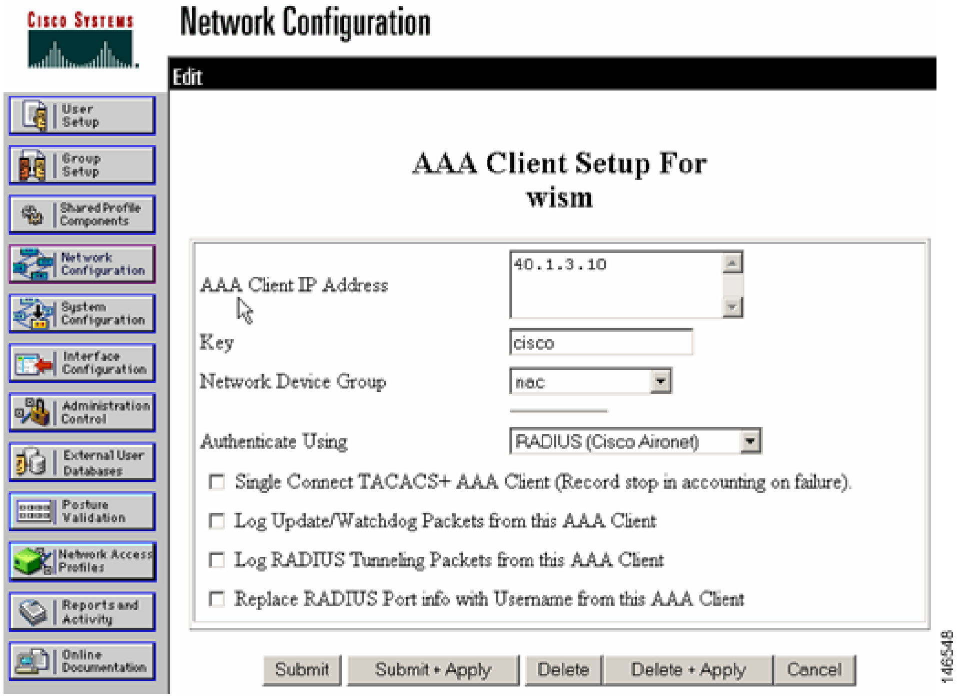
```
Trying 192.168.10.4... Open
(WiSM-slot3-2)
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_0f:f5:a3]:
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Service Interface IP Address Configuration [none][DHCP]: dhcp
Management Interface IP Address: 40.1.3.15
Management Interface Netmask: 255.255.0.0
Management Interface Default Router: 40.1.1.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.1.1.12
AP Transport Mode [layer2][LAYER3]: layer3
AP Manager Interface IP Address: 40.1.3.16
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.1.1.12):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: mobile-1
Network Name (SSID): secure-1
```

```
Allow Static IP Addresses [YES][no]: no
Configure a RADIUS Server now? [YES][no]: yes
Enter the RADIUS Server's Address: 10.1.1.12
Enter the RADIUS Server's Port [1812]:
Enter the RADIUS Server's Secret: cisco
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
Enable Auto-RF [YES][no]:

Configuration saved!

Resetting system with new configuration...

Sup720#show wism status

Service Vlan : 192, Service IP Subnet : 192.168.10.1/255.255.255.0
      WLAN
Slot  Controller  Service IP       Management IP    SW Version  Status
----+-----------+----------------+----------------+-----------+---------------
3     1           192.168.10.3     40.1.3.10        3.2.63.0    Oper-Up
3     2           192.168.10.4     40.1.3.15        3.2.63.0    Oper-Up
```

Configuring the RADIUS Server for WPA/WPA-2 Authentication

The Cisco WiSM must be defined on the RADUIS server as an AAA client, which allows the Cisco WiSM to authenticate credentials to its database. Using the Cisco Secure ACS RADIUS server, choose **Network Configuration**, define the IP address of the Cisco WiSM management interface and the shared RADIUS key, and specify **RADIUS** (Cisco Aironet) as the authentication type as shown in Figure 8.

Figure 8 Specifying Authentication Type



AAA Client Setup For wism

AAA Client IP Address: 40.1.3.10

Key: cisco

Network Device Group: nac

Authenticate Using: RADIUS (Cisco Aironet)

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

□ Log Update/Watchdog Packets from this AAA Client

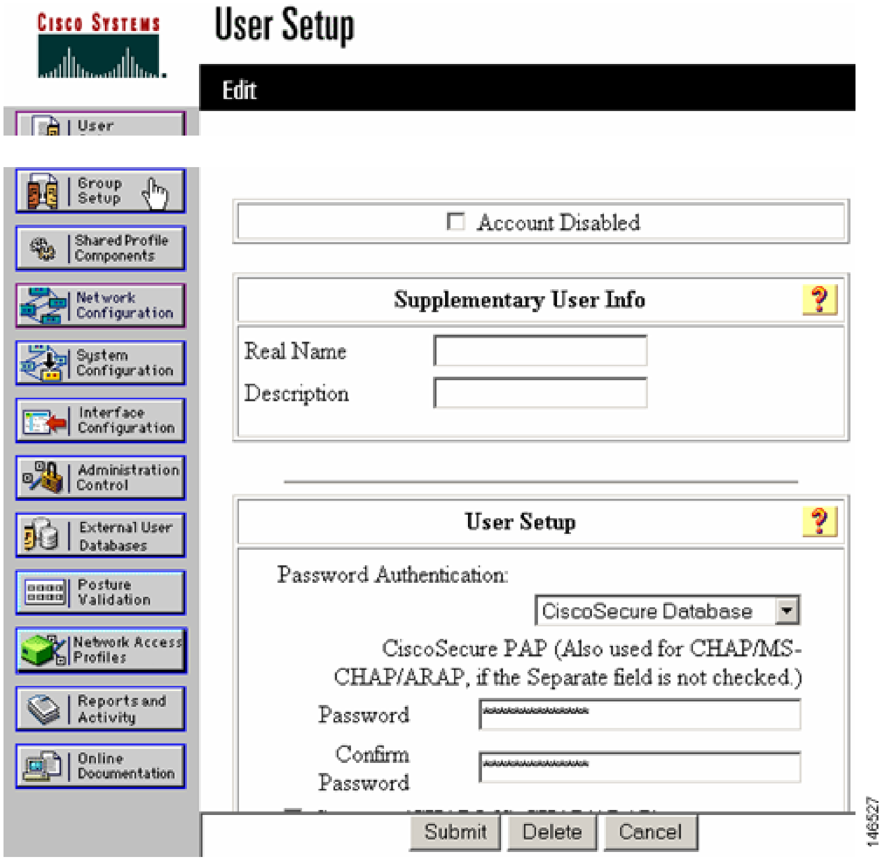
□ Log RADIUS Tunneling Packets from this AAA Client

□ Replace RADIUS Port info with Username from this AAA Client

Make sure the second controller is also added in the ACS server as a separate NAS.

Create some users in the ACS server for initial testing as shown in Figure 9. To configure the Cisco Secure ACS server so that all authentication requests are forwarded to the domain controller or other external database, refer to the Cisco secure configuration guide.

Figure 9 Creating Users in ACS



☐ Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password ***************

Confirm Password ***************

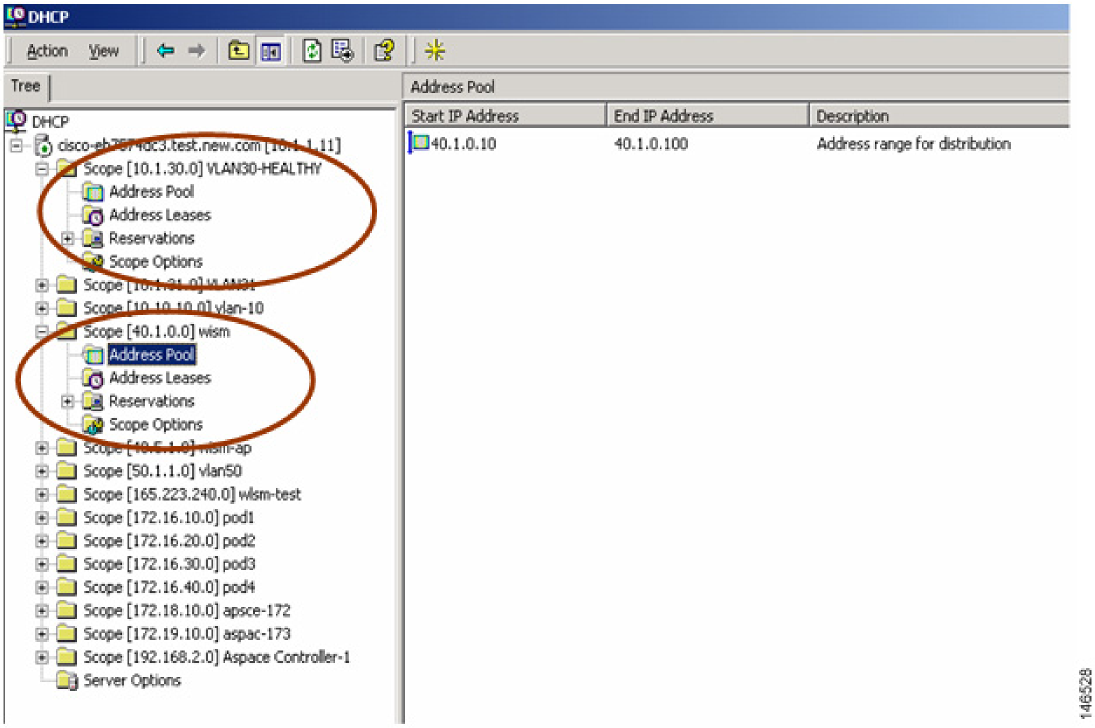
Configuring the Infrastructure for Access Point Placement

To make the access points register with the controller, put the access points in the same network as the management interface of the Cisco WiSM, in this case, VLAN 40. The example below shows how to configure one port in the switch where the access point is connected.

```
Sup720(config)# interface FastEthernet6/5
Sup720(config-if)# switchport
Sup720(config-if)# switchport access vlan 40
Sup720(config-if)# exit
```

Create the necessary scope in the DHCP server so that the access points can obtain an IP address before registering with the Cisco WiSM. Similarly, create a scope in the DHCP server for the clients to obtain an IP address after it is authenticated from the AAA server. Figure 10 shows scopes for VLAN 40 (used by access points) and VLAN 30 (used by wireless clients).

Figure 10 Creating a Scope in DHCP



Start IP Address	End IP Address	Description
40.1.0.10	40.1.0.100	Address range for distribution

After the access point gets an IP address from the DHCP server, it tries to discover the Cisco WiSM and register with it. To verify that if the access points are registered with the Cisco WiSM, do a **show ap summary** command on the Cisco WiSM.

```
(WiSM-slot3-1) > show ap sum

AP Name         Slots   AP Model    Ethernet MAC       Location          Port

__________      _____   ________    _______________    ______________    ____

AP1-cc:50       2      AP1030       00:0b:85:23:cc:50  default_location   29
ap:01:88:e0     2      AP-1200      00:0b:85:01:88:e0  pod3               29
```

View the detailed configuration of the access point by entering the **show ap config general <AP name>** command.

```
(WiSM-slot3-1) > show ap config general AP1-cc:50

Cisco AP Identifier.............................. 5
Cisco AP Name.................................... AP1-cc:50
AP Regulatory Domain............................. 80211bg: -A 80211a: -A
Switch Port Number .............................. 29
MAC Address...................................... 00:0b:85:23:cc:50
IP Address Configuration......................... DHCP
IP Address....................................... 40.1.0.14
IP NetMask....................................... 255.255.0.0
Gateway IP Addr.................................. 40.1.1.1
Cisco AP Location................................ default_location
Cisco AP Group Name..............................
Primary Cisco Switch.............................
Secondary Cisco Switch...........................
Tertiary Cisco Switch............................
Administrative State ............................ ADMIN_DISABLED
Operation State ................................. REGISTERED
```

```
Mirroring Mode ................................. Disabled
AP Mode ........................................ Local
Remote AP Debug ................................ Disabled
S/W  Version ................................... 3.2.63.0
Boot  Version .................................. 2.1.78.0
Mini IOS Version ......--More-- or (q)uit
..........................      --
Stats Reporting Period ......................... 180
LED State....................................... Enabled
ILP Pre Standard Switch......................... Disabled
ILP Power Injector.............................. Disabled
Number Of Slots................................. 2
AP Model........................................ AP1030
AP Serial Number................................ WCN0916004Q
AP Certificate Type............................. Manufacture Installed
```

Configuring the WCS and Adding the Cisco WiSM

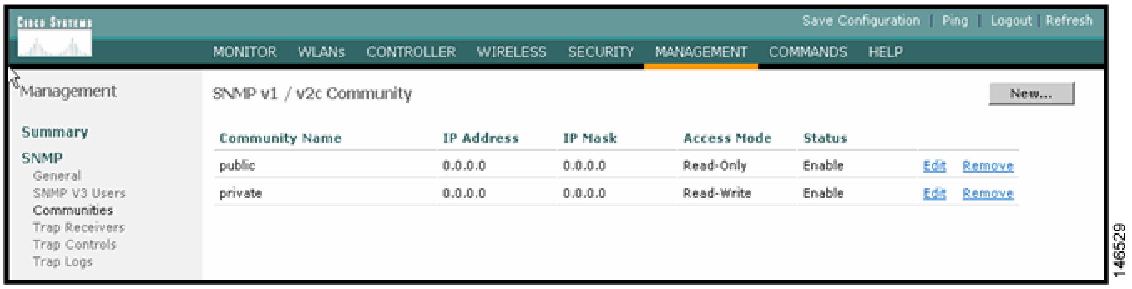
WCS is the management software used to manage WLC devices and provide advanced management tools like wireless coverage display and location-based services. WCS uses SNMP to manage WLC devices, so the WLC devices need to have SNMP configured correctly.

Step 1 Open the WCS web interface using the URL https://<wcs-ip-address>.

In this example, SNMPv2 is used. Configure SNMPv2 through the Cisco WiSM web interface by navigating to Management > SNMP > Communities. The Cisco WiSM defaults are read-only community *public* and read-write community *private* (see Figure 10).

Step 2 Add new communities or modify as necessary. In the example, the defaults are used.

Figure 11 Adding or Modifying Communities

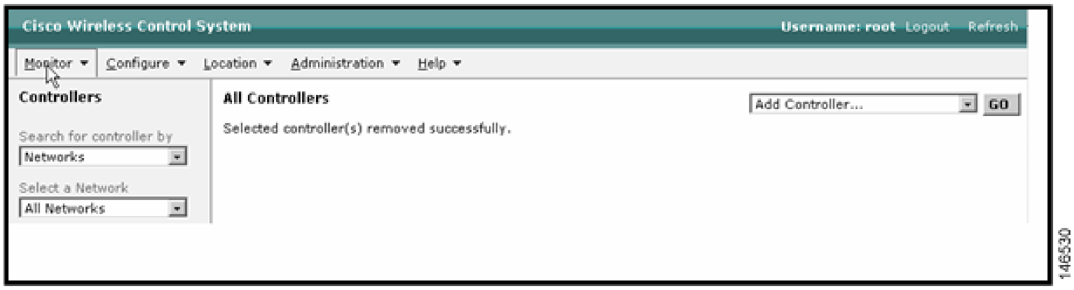


SNMP v1 / v2c Community

Community Name	IP Address	IP Mask	Access Mode	Status		
public	0.0.0.0	0.0.0.0	Read-Only	Enable	Edit	Remove
private	0.0.0.0	0.0.0.0	Read-Write	Enable	Edit	Remove

Step 3 Add Cisco WiSMs to WCS by navigating to Configure > Controllers on the WCS interface. Choose **Add controller** from the drop-down box on the right-hand side, then click **Go** (see Figure 11).

Figure 12 Adding Controllers


Cisco Wireless Control System
Username: root Logout Refresh
Monitor Configure Location Administration Help
GO
146530

Controllers

Search for controller by: Networks

Select a Network: All Networks

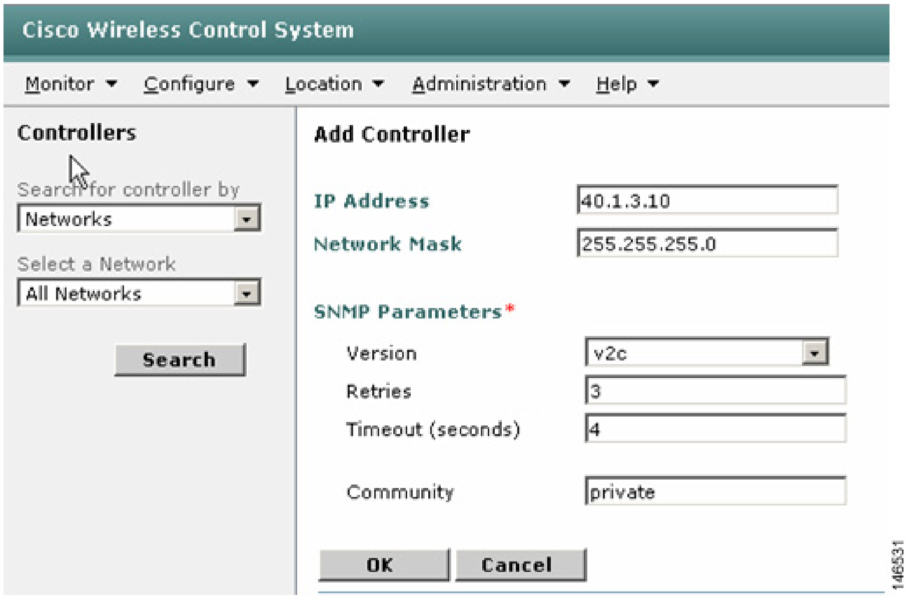
All Controllers

Add Controller...

Selected controller(s) removed successfully.

Step 4 Enter the IP address of the WiSM-A management interface and configure the appropriate SNMP parameters. Click **OK**. The WCS should find the Cisco WiSM. If the WCS cannot find the Cisco WiSM, verify the IP reachability from the WCS to the WLC and the SNMP community configuration (see Figure 12).

Figure 13 Verifying IP Reachability


Cisco Wireless Control System
Monitor Configure Location Administration Help
Search
OK
Cancel
146531

Controllers

Search for controller by: Networks

Select a Network: All Networks

Add Controller

IP Address: 40.1.3.10

Network Mask: 255.255.255.0

SNMP Parameters*

Version: v2c

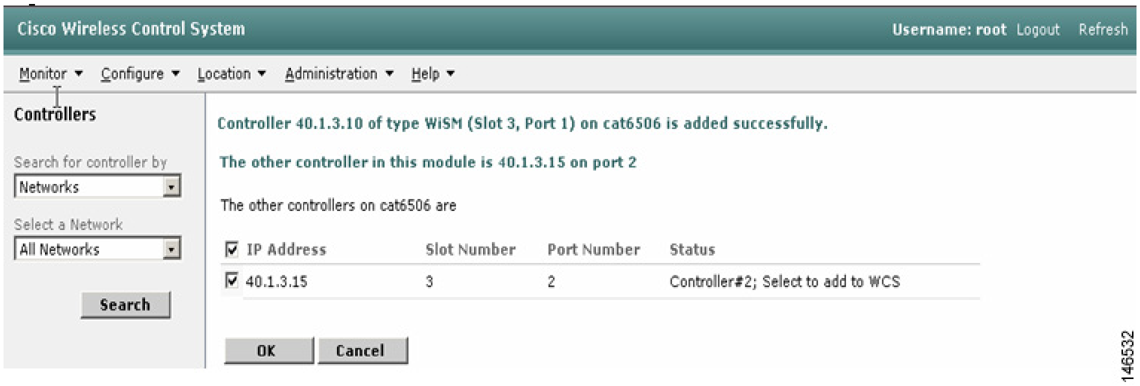
Retries: 3

Timeout (seconds): 4

Community: private

Step 5 After the first controller is discovered by the WCS, the remaining controllers in the chassis are detected by WCS with the help of the WCP (see Figure 13).

Figure 14 WCS Detecting Controllers



Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Controllers
Search for controller by
Networks
Select a Network
All Networks
Search
OK
Cancel
146532

Controller 40.1.3.10 of type WiSM (Slot 3, Port 1) on cat6506 is added successfully.

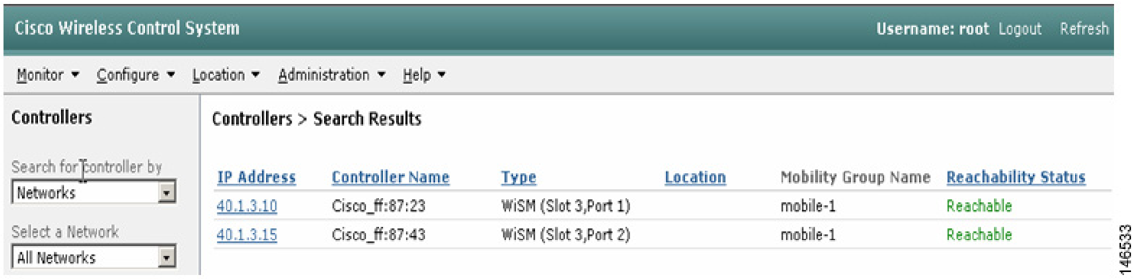
The other controller in this module is 40.1.3.15 on port 2

The other controllers on cat6506 are

☑ IP Address	Slot Number	Port Number	Status
☑ 40.1.3.15	3	2	Controller#2; Select to add to WCS

Step 6 Choose controllers to add to the WCS software (see Figure 15).

Figure 15 Choosing Controllers to Add



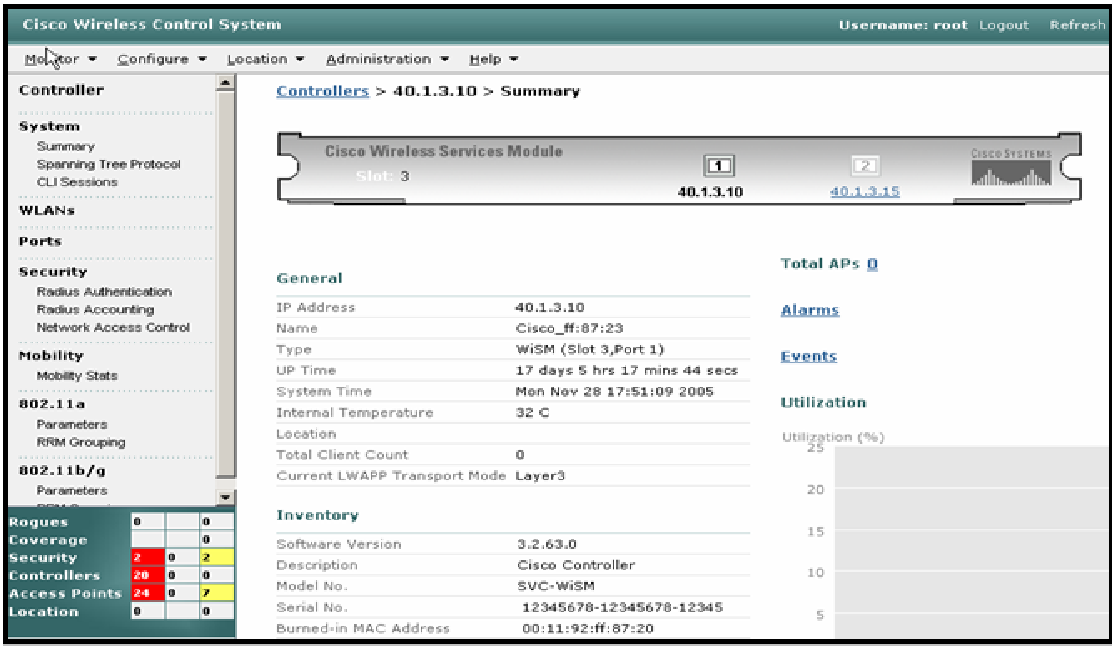
Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Controllers
Search for controller by
Networks
Select a Network
All Networks
146533

Controllers > Search Results

IP Address	Controller Name	Type	Location	Mobility Group Name	Reachability Status
40.1.3.10	Cisco_ff:87:23	WiSM (Slot 3,Port 1)		mobile-1	Reachable
40.1.3.15	Cisco_ff:87:43	WiSM (Slot 3,Port 2)		mobile-1	Reachable

Step 7 After the controller is successfully added in the WCS software, click the IP address of the controller to see the controller details (see Figure 16).

Figure 16 Controller Details



Controllers > 40.1.3.10 > Summary

Rogues	0		0
Coverage			0
Security	2	0	2
Controllers	20	0	0
Access Points	24	0	7
Location	0		0

General

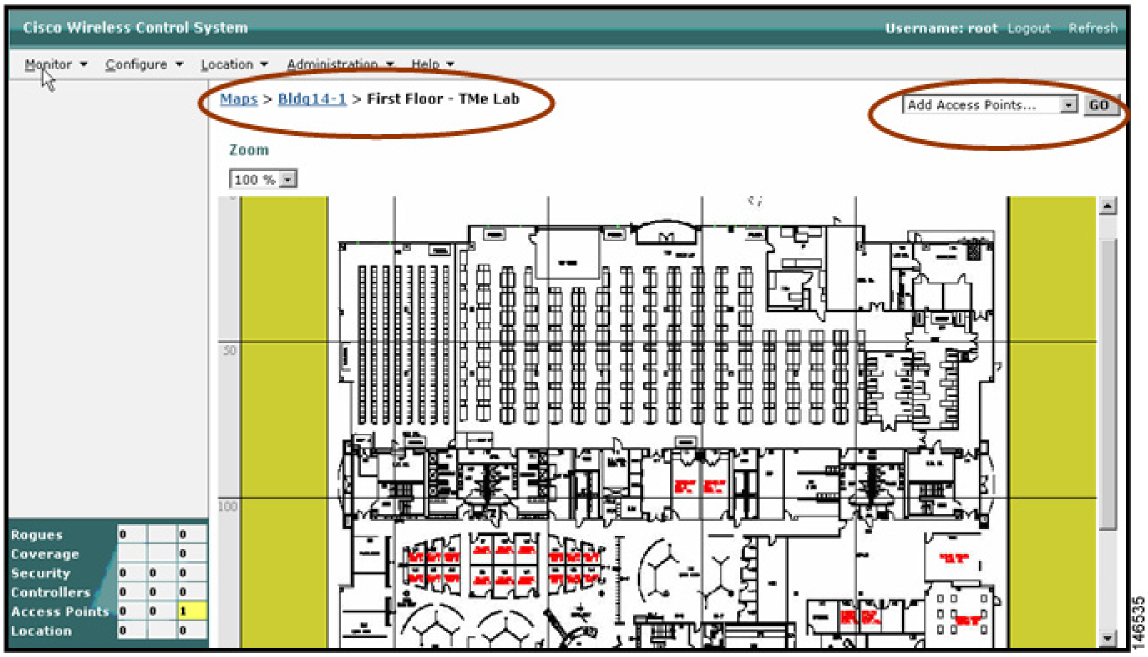
IP Address	40.1.3.10
Name	Cisco_ff:87:23
Type	WiSM (Slot 3,Port 1)
UP Time	17 days 5 hrs 17 mins 44 secs
System Time	Mon Nov 28 17:51:09 2005
Internal Temperature	32 C
Location	
Total Client Count	0
Current LWAPP Transport Mode	Layer3

Inventory

Software Version	3.2.63.0
Description	Cisco Controller
Model No.	SVC-WiSM
Serial No.	12345678-12345678-12345
Burned-in MAC Address	00:11:92:ff:87:20

Step 8 Import a floor plan and place the access points (see Figure 16). Refer to the WCS configuration guide for details on importing floor plans.

Figure 17 Importing a Floor Plan

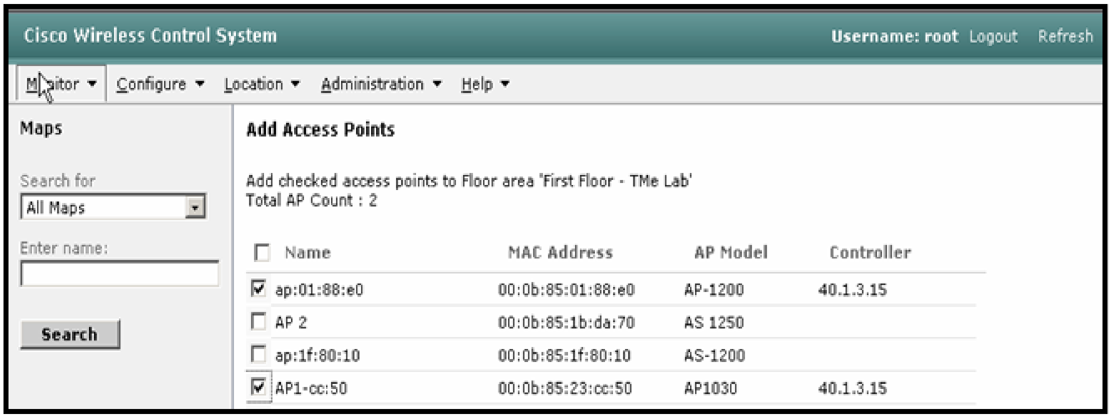

Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Add Access Points... GO
Zoom
100 %
50
100
146535

Maps > Bldg14-1 > First Floor - TMe Lab

Rogues	0		0
Coverage			0
Security	0	0	0
Controllers	0	0	0
Access Points	0	0	1
Location	0		0

Step 9 Choose access points to place on the floor map (see Figure 17).

Figure 18 *Placing Access Points onto Floorplan*


Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Maps
Search for
All Maps
Enter name:
Search
146536

Add Access Points

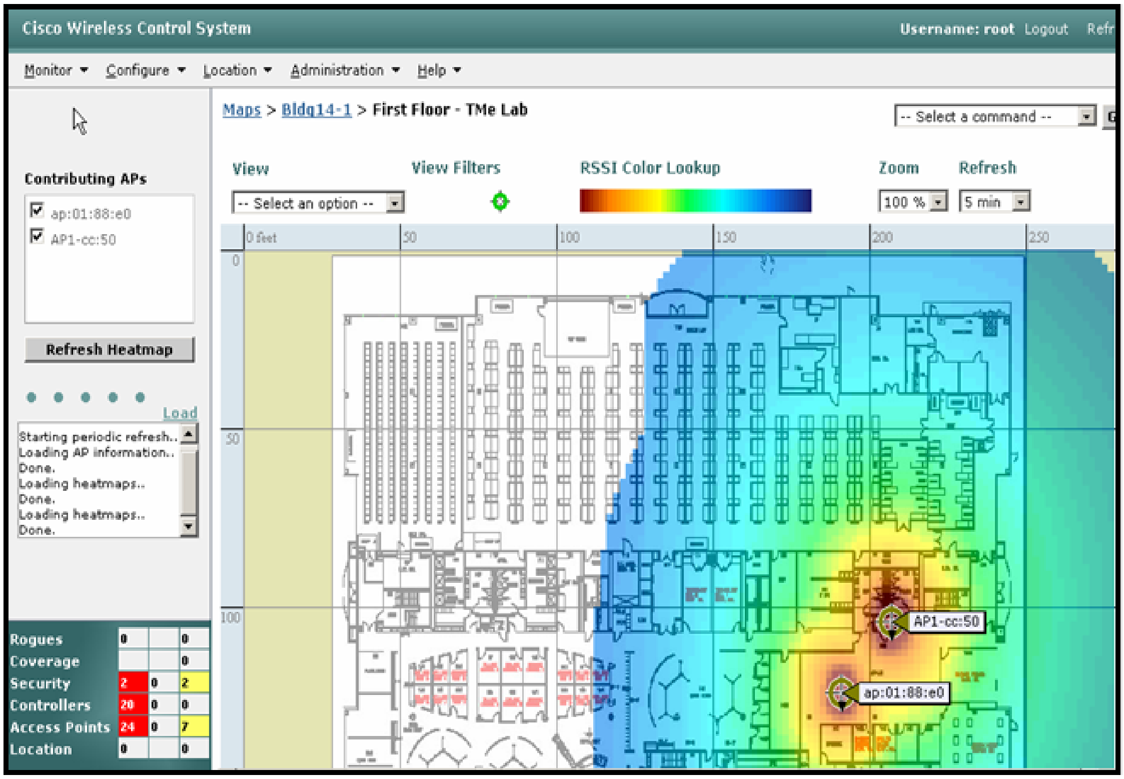
Add checked access points to Floor area 'First Floor - TMe Lab'
Total AP Count : 2

☐	Name	MAC Address	AP Model	Controller
☑	ap:01:88:e0	00:0b:85:01:88:e0	AP-1200	40.1.3.15
☐	AP 2	00:0b:85:1b:da:70	AS 1250	
☐	ap:1f:80:10	00:0b:85:1f:80:10	AS-1200	
☑	AP1-cc:50	00:0b:85:23:cc:50	AP1030	40.1.3.15

Step 10 After the access points are available for placement, drag and drop them on the appropriate locations on the floor map.

Step 11 Save the location of the access points in the floor map. You can see the coverage area of the access points in Figure 19.

Figure 19 *Access Point Coverage Area*



Contributing APs

☑ ap:01:88:e0
☑ AP1-cc:50

```
Starting periodic refresh..
Loading AP information..
Done.
Loading heatmaps..
Done.
Loading heatmaps..
Done.
```

Rogues	0		0
Coverage			0
Security	2	0	2
Controllers	20	0	0
Access Points	24	0	7
Location	0		0

Configuring DHCP Options 43

Refer to the following appendices in the *Deploying Cisco 440X Series Wireless LAN Controllers* for various Option 43 configurations:

- For details on how to use vendor-specific options to facilitate controller discovery by the access point, refer to Appendix C:

  http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html#wp1068287

- For details on configuring vendor-specific DHCP Options (Option 43) in the Cisco IOS DHCP server, refer to Appendix D:

  http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html#wp1069100

- For details on configuring vendor-specific DHCP Options (Option 43) in the Windows 2000 and 2003 DHCP Server, refer to Appendix E:

  http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html#wp1069651

Upgrading WLC Software

You can upgrade WLC software any of three ways:

- Through the WLC CLI
- Through the WLC Web Interface
- Through WCS

Upgrading WLC Software Using the WLC CLI

To upgrade a WLC through the controller CLI, follow these steps:

Step 1 Copy the code file onto a TFTP server's root directory.

Step 2 Start the TFTP server if not already running.

Step 3 Login to the WLC CLI and enter the following commands:

```
> transfer download serverip <TFTP Server IP>
> transfer download path <path>
> transfer download filename <code filename>
> transfer download start
```

Note that if you put the code in the TFTP root directory, the “path” parameter is optional.

Step 4 Once the code is successfully downloaded and written to the WLC flash, be sure to save the WLC configuration:

```
> save config
```

Step 5 Reboot the WLC with the following command:

```
> reset system
```

Upgrading WLC Software Using the WLC Web Interface

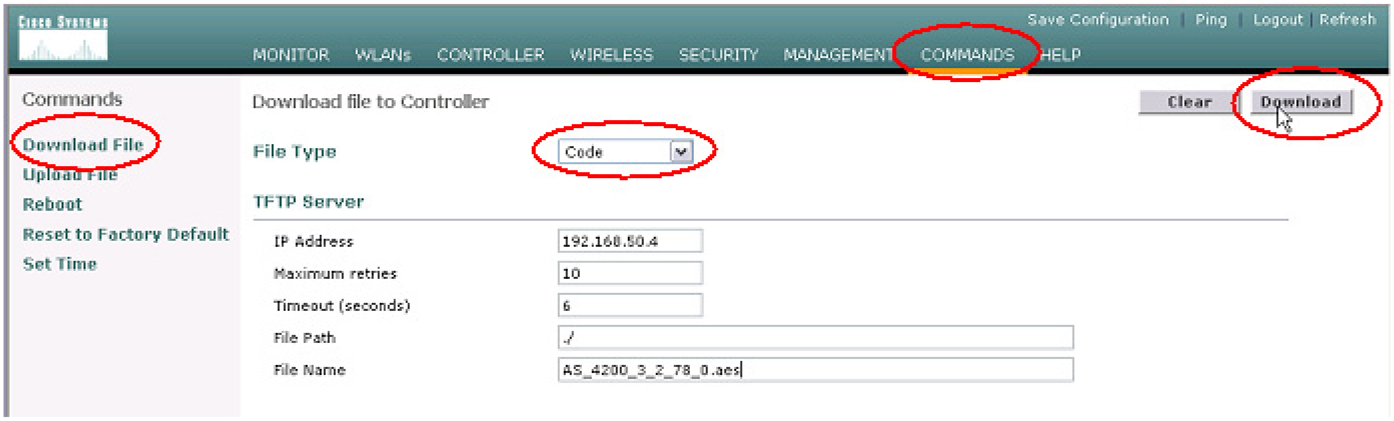
To upgrade a controller through the WLC GUI, follow these steps:

Step 1 Copy the code file onto a TFTP server's root directory.

Step 2 Start the TFTP server if not already running.

Step 3 Navigate through the GUI to **Commands | Download File**. Select **Code** as the File Type, and then enter the TFTP server parameters in the appropriate fields. If you copied the code to the TFTP server root, then enter a period (**.**) in the File Path Field. Click **Download** in the upper right-hand corner to initiate the TFTP download (see Figure 20).

Figure 20 WLC Code Download


Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Commands
Download File
Upload File
Reboot
Reset to Factory Default
Set Time
Clear
Download

Download file to Controller

File Type: Code

TFTP Server

IP Address: 192.168.50.4

Maximum retries: 10

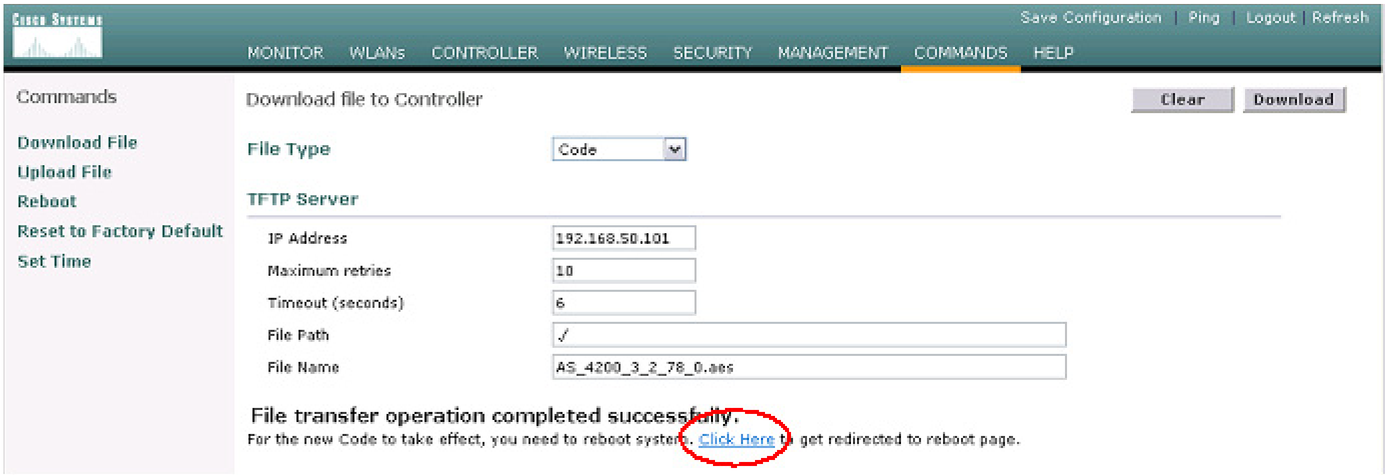
Timeout (seconds): 6

File Path: ./

File Name: AS_4200_3_2_78_0.aes

Step 4 Once the file transfer is successfully completed, you need to reboot the controller to load the new code. You will see a **Click Here** link at the bottom of the page (see Figure 21). Click on the link to continue the process.

Figure 21 WLC Code Download


Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Commands
Download File
Upload File
Reboot
Reset to Factory Default
Set Time
Clear
Download

Download file to Controller

File Type: Code

TFTP Server

IP Address: 192.168.50.101

Maximum retries: 10

Timeout (seconds): 6

File Path: ./

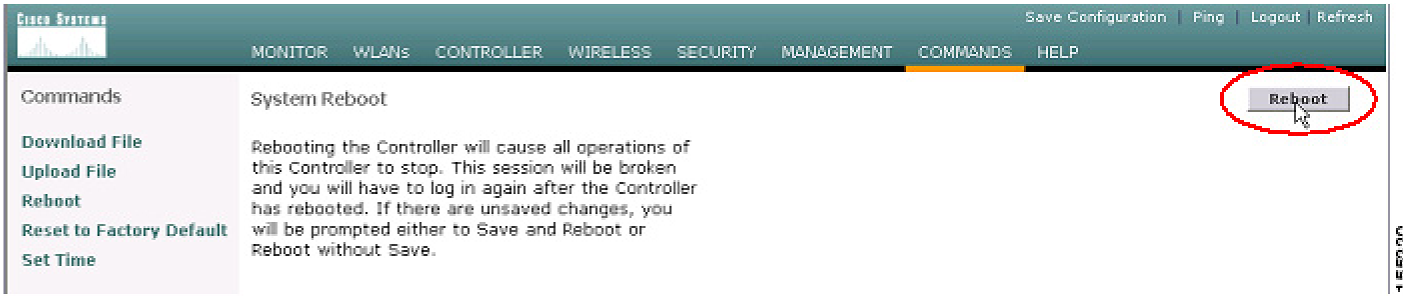
File Name: AS_4200_3_2_78_0.aes

File transfer operation completed successfully.

For the new Code to take effect, you need to reboot system. Click Here to get redirected to reboot page.

Step 5 At the next screen, you will see a system reboot warning. Read the warning carefully, then click **Reboot** (see Figure 22).

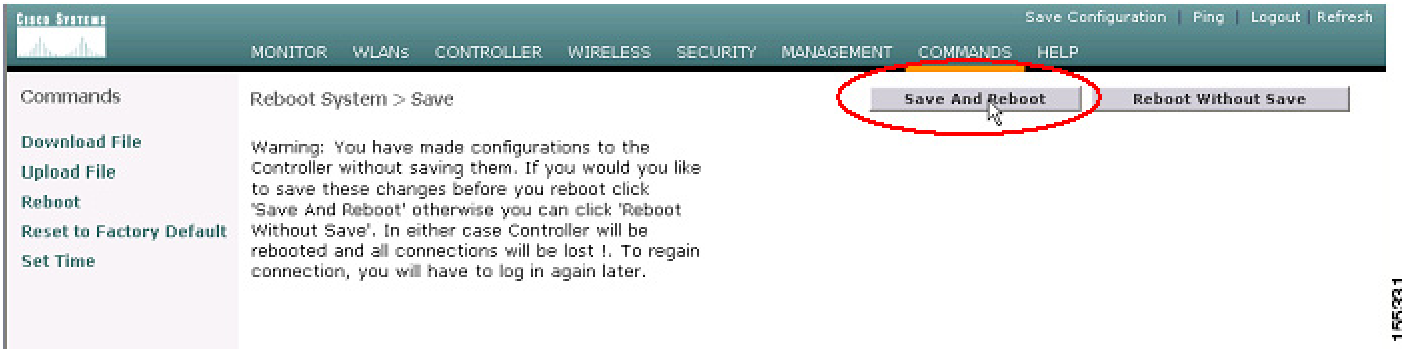
Figure 22 WLC Code Download--Controller Reboot



Rebooting the Controller will cause all operations of this Controller to stop. This session will be broken and you will have to log in again after the Controller has rebooted. If there are unsaved changes, you will be prompted either to Save and Reboot or Reboot without Save.

Step 6 Be sure to save the WLC configuration by clicking **Save and Reboot** (see Figure 23).

Figure 23 WLC Save and Reboot



Warning: You have made configurations to the Controller without saving them. If you would you like to save these changes before you reboot click 'Save And Reboot' otherwise you can click 'Reboot Without Save'. In either case Controller will be rebooted and all connections will be lost !. To regain connection, you will have to log in again later.

When the WLC reboots, you will eventually lose browser connectivity with the controller. Wait a couple of minutes and then refresh the page. A successful page refresh indicates a completed update.

Upgrading WLC Software Using the WCS

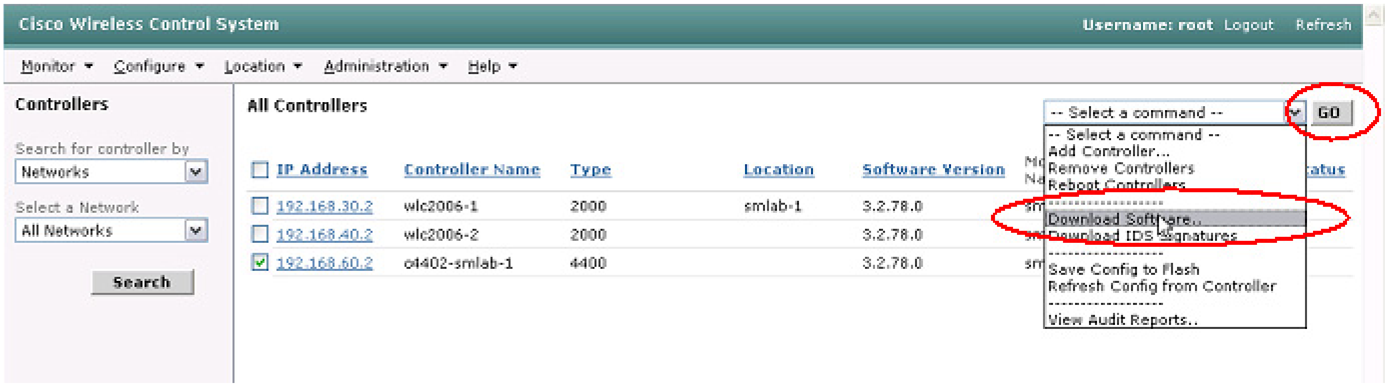
To upgrade a WLC using WCS, follow these steps:

Step 1 You can initiate a software upgrade to a WLC from either an external TFTP server or from the TFTP server embedded in WCS. In the case of an external TFTP server, copy the WLC code to the TFTP root. With WCS, the file can be copied to the TFTP root directory configured at install time or in a directory on the WCS host machine.

Step 2 Navigate in the WCS interface to **Configure | Controllers** (see Figure 24).

Step 3 Select one or more WLCs by checking the appropriate check-boxes. Note that you can upgrade WLCs from a single WLC family at a time. Select the **Download Software** option from the drop-down box and click **Go** (see Figure 24).

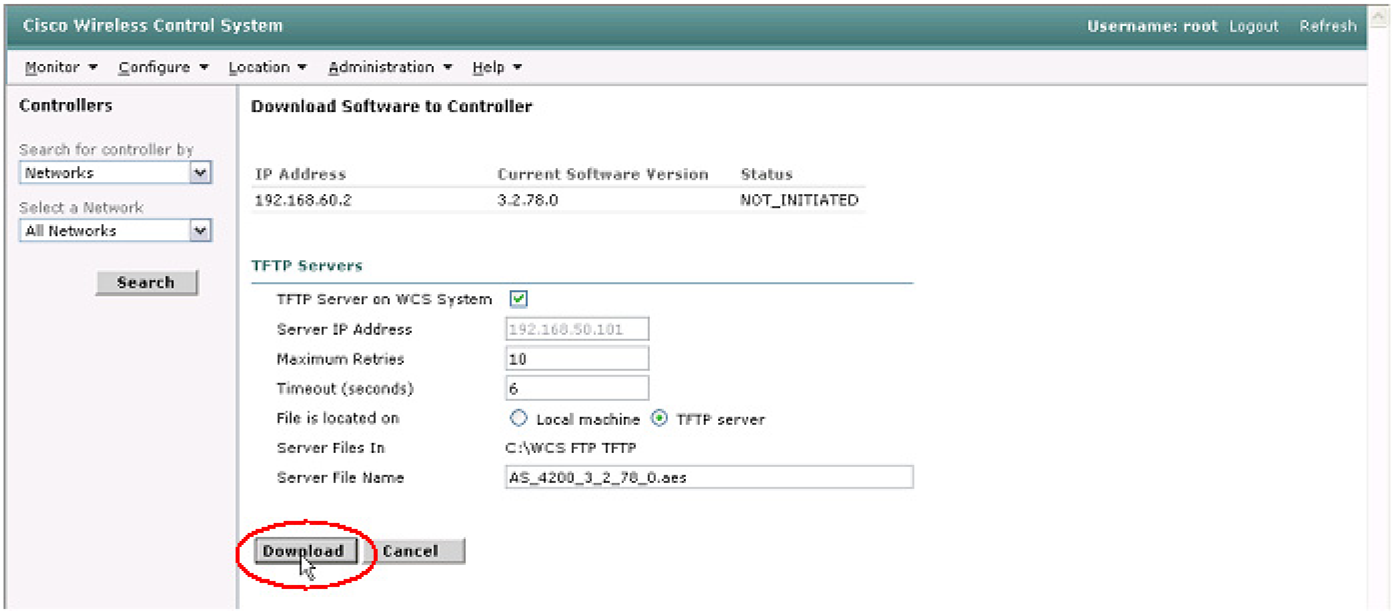
Figure 24 WCS Software Download to WLC



□	IP Address	Controller Name	Type	Location	Software Version
□	192.168.30.2	wlc2006-1	2000	smlab-1	3.2.78.0
□	192.168.40.2	wlc2006-2	2000		3.2.78.0
☑	192.168.60.2	c4402-smlab-1	4400		3.2.78.0

Step 4 Configure the appropriate parameters. Consult the online help for details on the TFTP server fields. When you have configured the appropriate parameters, click **Download** (see Figure 25).

Figure 25 WCS Software Download to WLC


Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Controllers
Search for controller by
Networks
Select a Network
All Networks
Search
Download Software to Controller
Download
Cancel

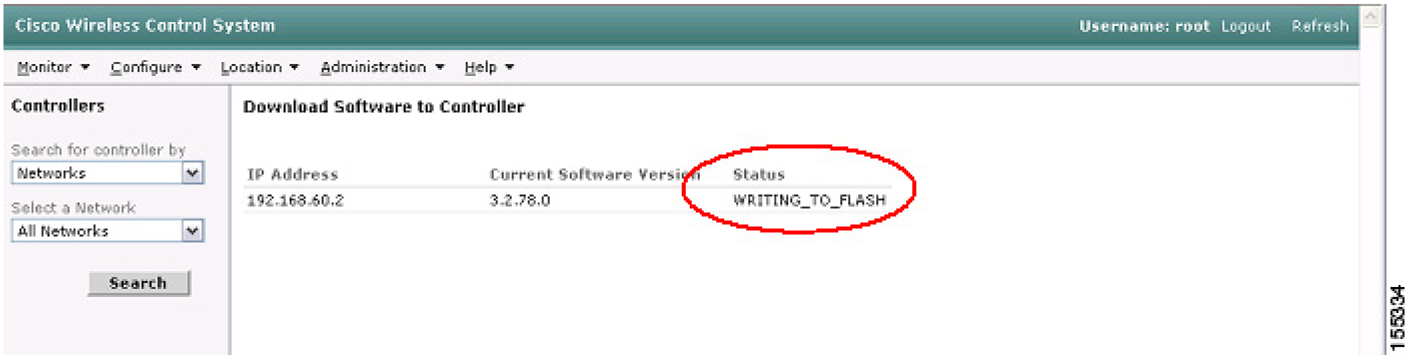
IP Address	Current Software Version	Status
192.168.60.2	3.2.78.0	NOT_INITIATED

TFTP Servers

TFTP Server on WCS System	☑
Server IP Address	192.168.50.101
Maximum Retries	10
Timeout (seconds)	6
File is located on	○ Local machine ● TFTP server
Server Files In	C:\WCS FTP TFTP
Server File Name	AS_4200_3_2_78_0.aes

While the code is downloading and the WLC upgrading, you will see status messages in the WCS interface (see Figure 26).

Figure 26 WCS Software Download Status



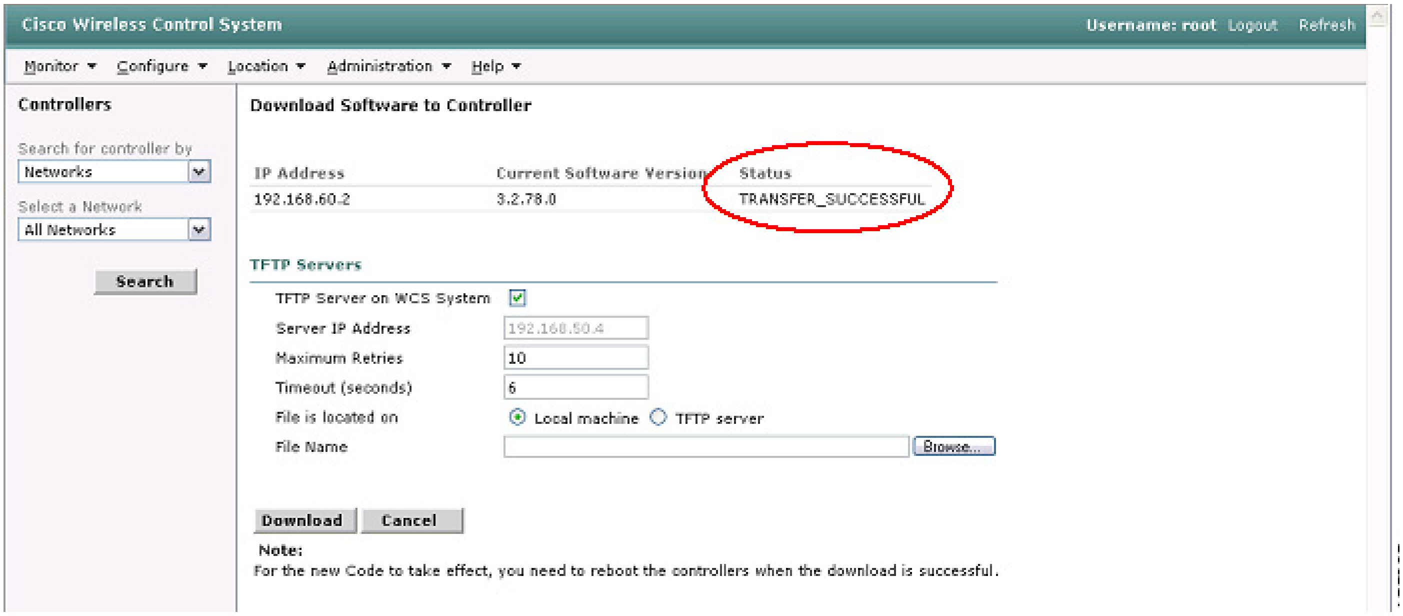
Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Controllers
Search for controller by
Networks
Select a Network
All Networks
Search
155334

Download Software to Controller

IP Address	Current Software Version	Status
192.168.60.2	3.2.78.0	WRITING_TO_FLASH

Step 5 When the code download is successful, you will see a TRANSFER_SUCCESSFUL message (see Figure 27).

Figure 27 WCS Software Download Success



Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Controllers
Search for controller by
Networks
Select a Network
All Networks
Search
Browse...
Download
Cancel

Download Software to Controller

IP Address	Current Software Version	Status
192.168.60.2	3.2.78.0	TRANSFER_SUCCESSFUL

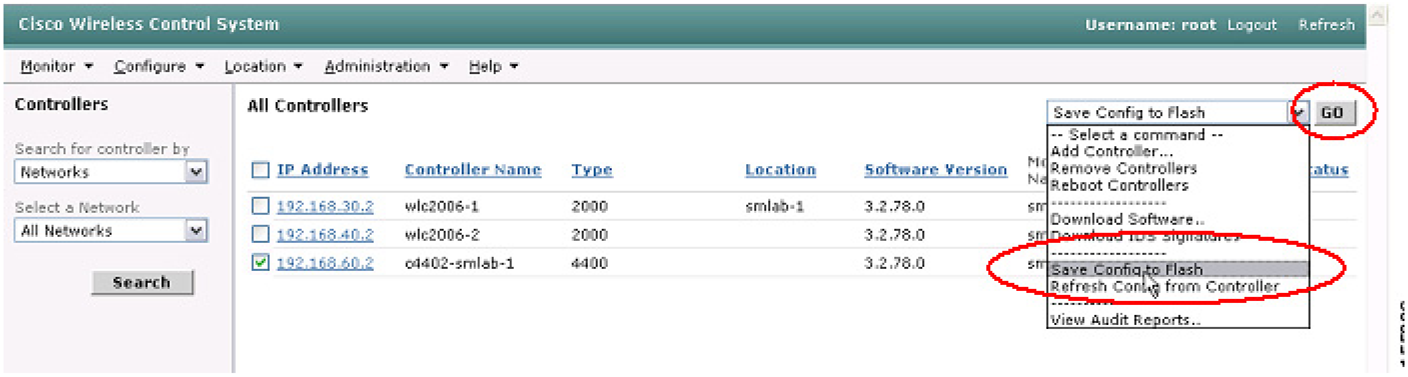
TFTP Servers

TFTP Server on WCS System	☑
Server IP Address	192.168.50.4
Maximum Retries	10
Timeout (seconds)	6
File is located on	● Local machine ○ TFTP server
File Name	

Note:
For the new Code to take effect, you need to reboot the controllers when the download is successful.

Step 6 When the code is successfully loaded on the controllers, you must reboot them to load the new code. You should first save the WLC configurations and to do so, navigate to the **Configure | Controllers** interface. Select the controllers, and then choose **Save Config to Flash** from the drop-down box on the right-hand side, and finally click **Go** (see Figure 28).

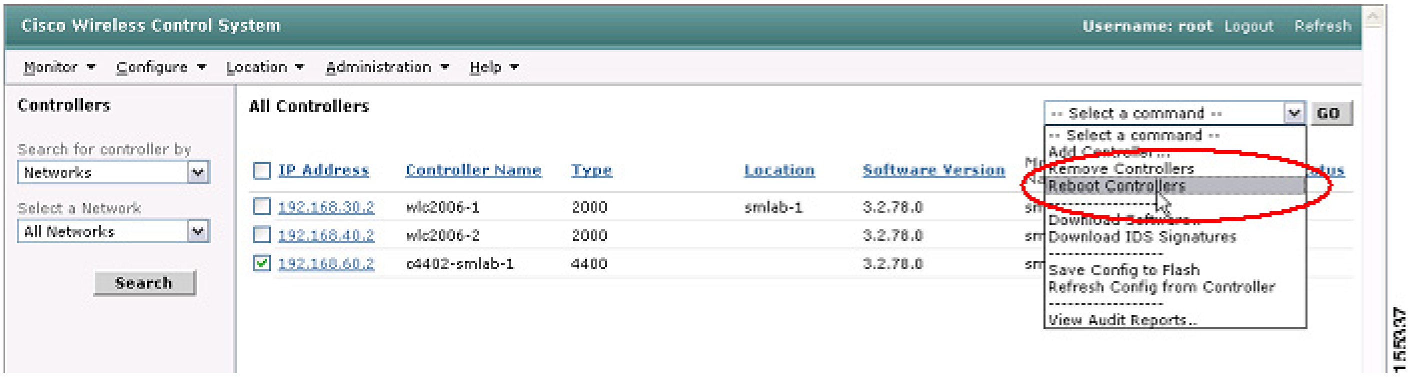
Figure 28 WCS Save Configuration to WLC Flash



☐	IP Address	Controller Name	Type	Location	Software Version	Mo Na	...atus
☐	192.168.30.2	wlc2006-1	2000	smlab-1	3.2.78.0	sm	
☐	192.168.40.2	wlc2006-2	2000		3.2.78.0	sm	
☑	192.168.60.2	c4402-smlab-1	4400		3.2.78.0	sm	

Step 7 After the configuration(s) have been successfully saved, select the controllers and then choose **Reboot Controllers** from the drop-down box on the right-hand side and then click **Go** (see Figure 29).

Figure 29 WCS Reboot WLC



☐	IP Address	Controller Name	Type	Location	Software Version	Mo Na	...tus
☐	192.168.30.2	wlc2006-1	2000	smlab-1	3.2.78.0	sm	
☐	192.168.40.2	wlc2006-2	2000		3.2.78.0	sm	
☑	192.168.60.2	c4402-smlab-1	4400		3.2.78.0	sm	

Best Practices for Upgrading WLC Software

A controller can download a new image without disrupting service but it needs to be rebooted manually to load the new code. Once the new code is loaded on reboot, the upgrade of all access point code is automatically triggered. Cisco controllers currently upgrade four access points at a time. Take this into account when allotting a change window for upgrading your WLC.

To compute the minimum change window, use this formula:

```
Change Window = Controller reboot time + (Number of APs / 4 )* 3 minutes per AP
```

Let's take a worst-case example. Suppose we have a Cisco 4404 controller with 100 access points joined to it. The controller reboot time is approximately 3.5 minutes. So our minimum change window is:

```
4.5 minutes + (100 APs / 4) * 3 minutes per AP = 78.5 minutes = 1 hour 18.5 minutes.
```

You should allow yourself some time for troubleshooting.

As another best practice, if you have multiple WLC devices in the network, **you should keep the software revisions consistent across all WLC devices.** This is because an access point down-revs its code when it joins a WLC with a lower code revision than what is currently running on the access point.

This is an issue that leads to increased downtime each time an access point joins a new controller. Keep this in mind when you have multiple controllers in the network and redundancy deployed. You should account for this change in your planned service window.

Recovering a Password

To recover a password, refer to:

http://www.cisco.com/en/US/products/ps6308/products_password_recovery09186a008071faa7.shtml

WLC Controller Configuration Backup and Restore

Backup and restore operations for a WLC's configurations can be performed from both the WLC itself and the WCS.

Note If you forget your username and password, you cannot backup your configuration unless you have stored it on an FTP server and are able to retrieve it using the controller GUI or Cisco WCS.

Caution If you have not stored the username and password, you must reset the username and password. Refer to http://www.cisco.com/en/US/products/ps6308/products_password_recovery09186a008071faa7.shtml

Managing WLC Configurations Using the WLC Web Interface

Follow these steps to backup WLC Configurations from the WLC Web Interface:

Step 1 Start a TFTP server if necessary.

Step 2 Navigate in the WLC to **Commands | Upload File** (see Figure 30).

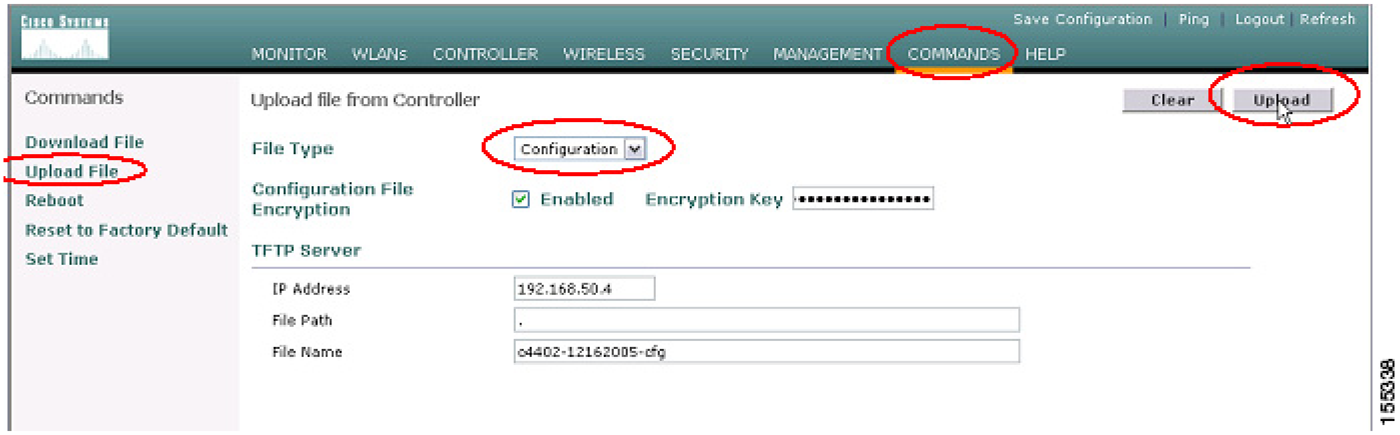
Step 3 From the File Type drop-down box, select **Configuration** (see Figure 30).

Step 4 If you want to encrypt the configuration file, check the **Configuration File Encryption Enabled** box and then enter a value in the **Encryption Key** field. The encryption key must be at least 16 characters in length (see Figure 30).

Step 5 Enter the TFTP Server **IP address**, **File Path**, and **File Name** in the appropriate fields (see Figure 30).

Step 6 Click on the **Upload** button (see Figure 30).

Figure 30 ***WCS Configuration Upload***



Upload file from Controller

File Type	Configuration
Configuration File Encryption	☑ Enabled Encryption Key ••••••••••••••••

TFTP Server

IP Address	192.168.50.4
File Path	.
File Name	c4402-12162005-cfg

Step 7 When the upload is successful, you will see a message that says, "File transfer operation completed successfully."

Follow these steps to reload a configuration to a WLC:

Step 1 Start a TFTP server and load the backed up controller configuration to the TFTP server.

Step 2 Navigate in the WLC to **Commands | Download File** (see Figure 31).

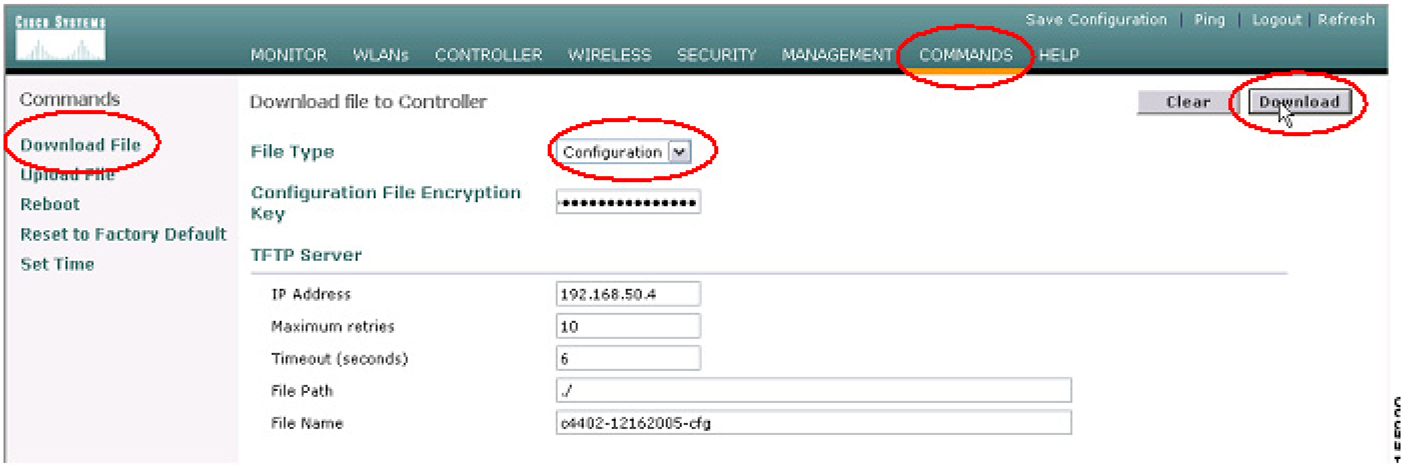
Step 3 From the File Type drop-down box, select **Configuration** (see Figure 31).

Step 4 If necessary, enter the file encryption key in the **Configuration File Encryption Key** field (see Figure 31).

Step 5 Enter the TFTP Server **IP address**, **File Path**, and **File Name** in the appropriate fields (see Figure 31).

Step 6 Click **Download** (see Figure 31).

Figure 31 ***WCS Configuration Download to WLC***



Download file to Controller

File Type	Configuration
Configuration File Encryption Key	••••••••••••••••

TFTP Server

IP Address	192.168.50.4
Maximum retries	10
Timeout (seconds)	6
File Path	./
File Name	c4402-12162005-cfg

Step 7 The WLC will reboot after it successfully loads the configuration.

Managing WLC Configurations Using WCS

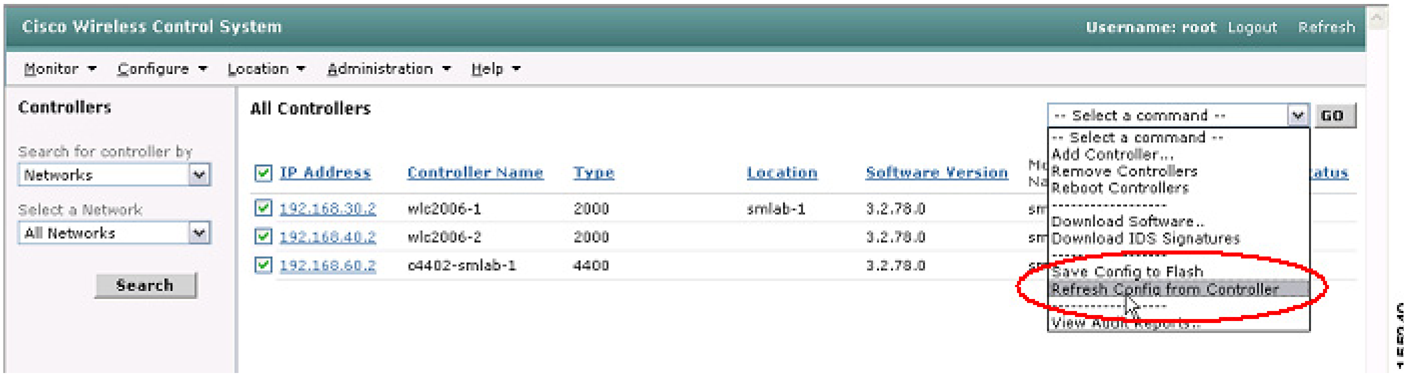
When a controller is added to WCS, its complete configuration is pulled from the WLC and stored locally. When you use the WCS to change a WLC configuration, it is automatically updated in the WCS database.

If you make a change from on the WLC independent of WCS, you can refresh the configuration on WCS using the following steps:

Step 1 Navigate in WCS to **Configure | Controllers**.

Step 2 Select one or more WLCs. Select **Refresh Config from Controller** from the drop-down box and click **GO** (see Figure 32).

Figure 32 WCS Refresh Configuration from WLC


Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
-- Select a command -- GO
-- Select a command --
Add Controller...
Remove Controllers
Reboot Controllers
Download Software..
Download IDS Signatures
Save Config to Flash
Refresh Config from Controller
View Audit Reports..
Search

Controllers

Search for controller by: Networks

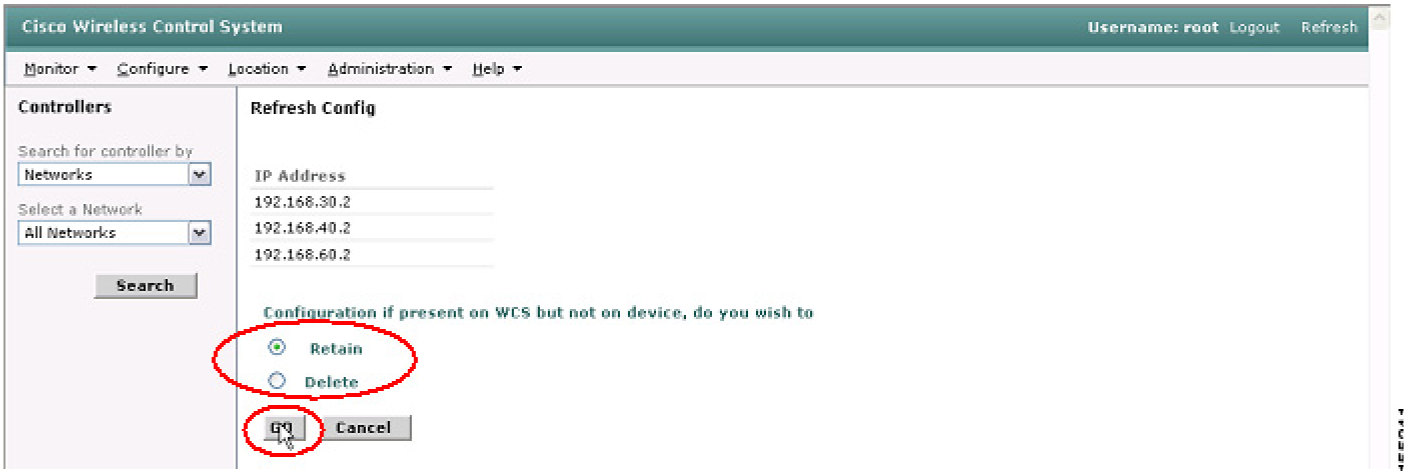
Select a Network: All Networks

All Controllers

☑ IP Address	Controller Name	Type	Location	Software Version	Mo Na	atus
☑ 192.168.30.2	wlc2006-1	2000	smlab-1	3.2.78.0	sm	
☑ 192.168.40.2	wlc2006-2	2000		3.2.78.0	sm	
☑ 192.168.60.2	c4402-smlab-1	4400		3.2.78.0	sm	

Step 3 You will also be provided an option to either retain or delete configurations that are on WCS but not the controller. Typically, you would want to select the retain option (in case there's a need to roll-back to previous configurations). Click on **Go** to initiate the configuration refresh from the WLC (see Figure 33).

Figure 33 WCS Retain Configuration


Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Search
Go
Cancel

Controllers

Search for controller by: Networks

Select a Network: All Networks

Refresh Config

IP Address
192.168.30.2
192.168.40.2
192.168.60.2

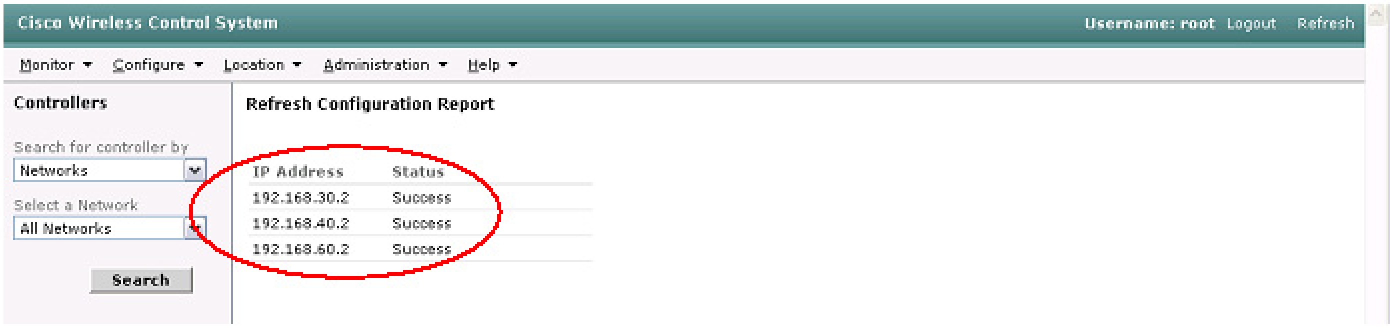
Configuration if present on WCS but not on device, do you wish to

● Retain

○ Delete

Step 4 When the configurations have been successfully refreshed from the controllers, you will see a "Success" status message (see Figure 34).

Figure 34 WCS Refresh Configuration Success


Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Controllers
Search for controller by
Networks
Select a Network
All Networks
Search

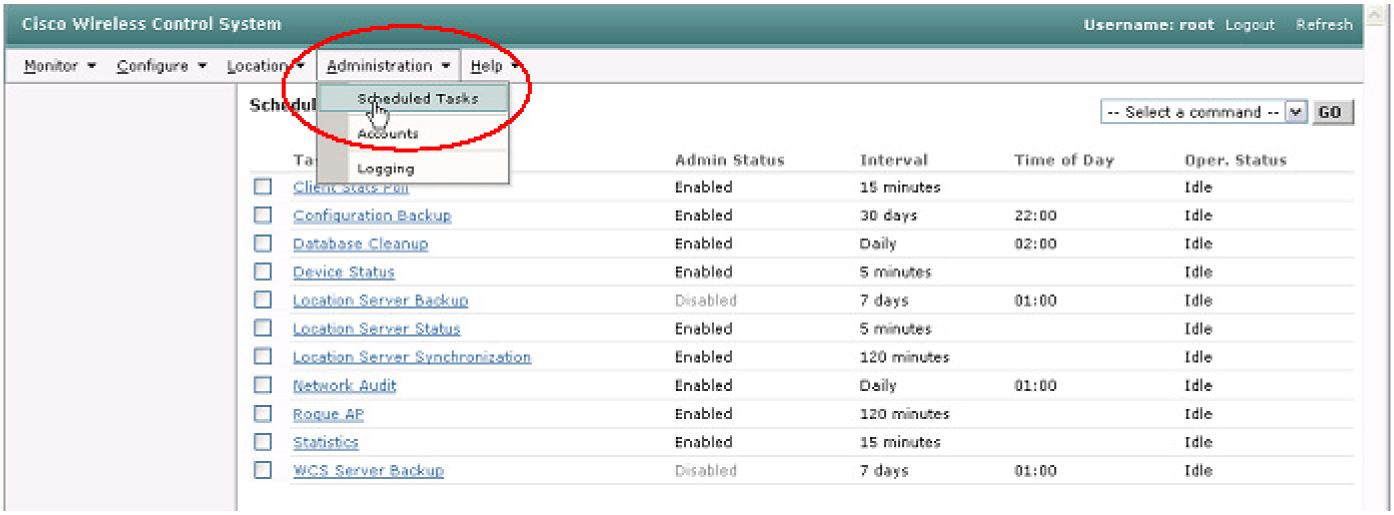
Refresh Configuration Report

IP Address	Status
192.168.30.2	Success
192.168.40.2	Success
192.168.60.2	Success

The WCS can also perform scheduled and full on-demand configuration backups:

Step 1 Navigate in WCS to **Administration | Scheduled Tasks** (see Figure 35).

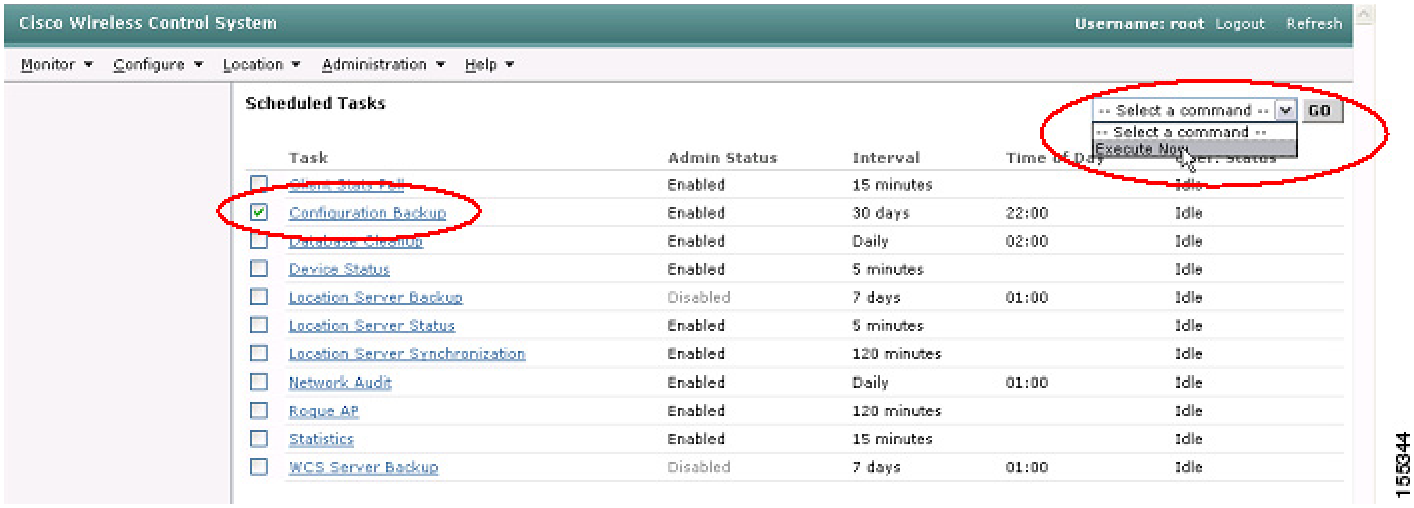
Figure 35 WCS Scheduled Configuration Backup


Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Scheduled Tasks
Accounts
Logging
Schedul
-- Select a command -- GO

	Ta	Admin Status	Interval	Time of Day	Oper. Status
□	Client Stats Poll	Enabled	15 minutes		Idle
□	Configuration Backup	Enabled	30 days	22:00	Idle
□	Database Cleanup	Enabled	Daily	02:00	Idle
□	Device Status	Enabled	5 minutes		Idle
□	Location Server Backup	Disabled	7 days	01:00	Idle
□	Location Server Status	Enabled	5 minutes		Idle
□	Location Server Synchronization	Enabled	120 minutes		Idle
□	Network Audit	Enabled	Daily	01:00	Idle
□	Rogue AP	Enabled	120 minutes		Idle
□	Statistics	Enabled	15 minutes		Idle
□	WCS Server Backup	Disabled	7 days	01:00	Idle

Step 2 To do a configuration backup on demand, select the **Configuration Backup** check-box and then select **Execute Now** from the drop-down box and click **Go** (see Figure 36). The backed-up configurations will be stored in the WCS TFTP root directory and labeled with the WLC Management Interface IP address and a timestamp.

Figure 36 WCS Scheduled Configuration Backup

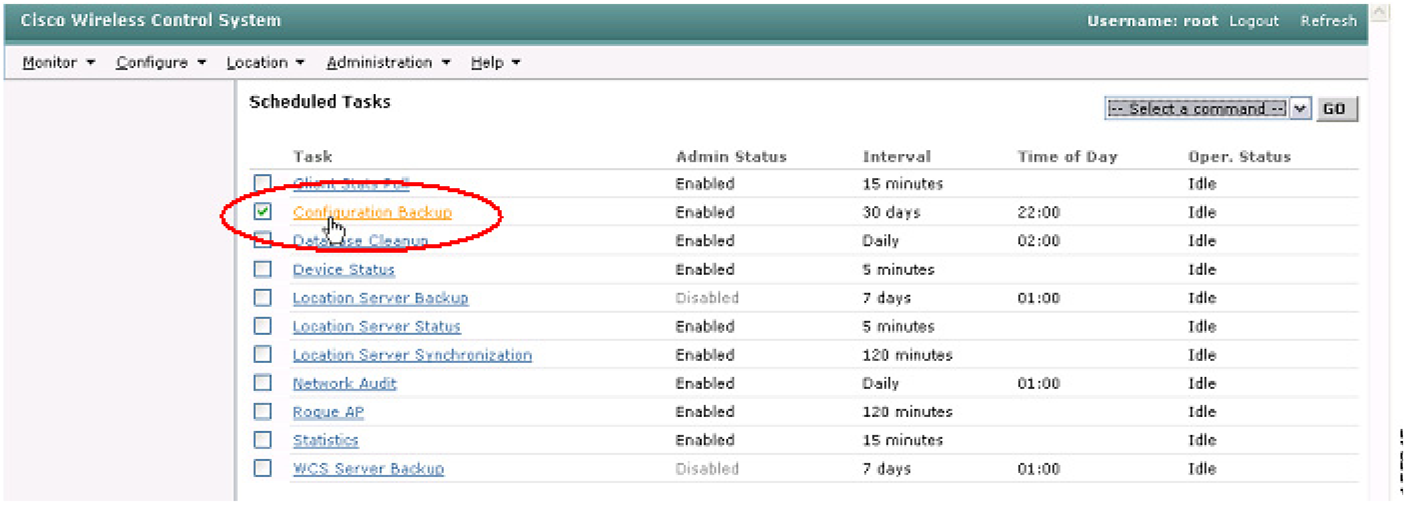

Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
-- Select a command -- GO
-- Select a command --
Execute Now
155344

Scheduled Tasks

	Task	Admin Status	Interval	Time of Day	Oper. Status
□	Client Stats Poll	Enabled	15 minutes		Idle
☑	Configuration Backup	Enabled	30 days	22:00	Idle
□	Database Cleanup	Enabled	Daily	02:00	Idle
□	Device Status	Enabled	5 minutes		Idle
□	Location Server Backup	Disabled	7 days	01:00	Idle
□	Location Server Status	Enabled	5 minutes		Idle
□	Location Server Synchronization	Enabled	120 minutes		Idle
□	Network Audit	Enabled	Daily	01:00	Idle
□	Rogue AP	Enabled	120 minutes		Idle
□	Statistics	Enabled	15 minutes		Idle
□	WCS Server Backup	Disabled	7 days	01:00	Idle

Step 3 To schedule regular configuration backups, select the **Configuration Backup** link to access the configuration screen (see Figure 37).

Figure 37 WCS Scheduled Configuration Backup


Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
-- Select a command -- GO

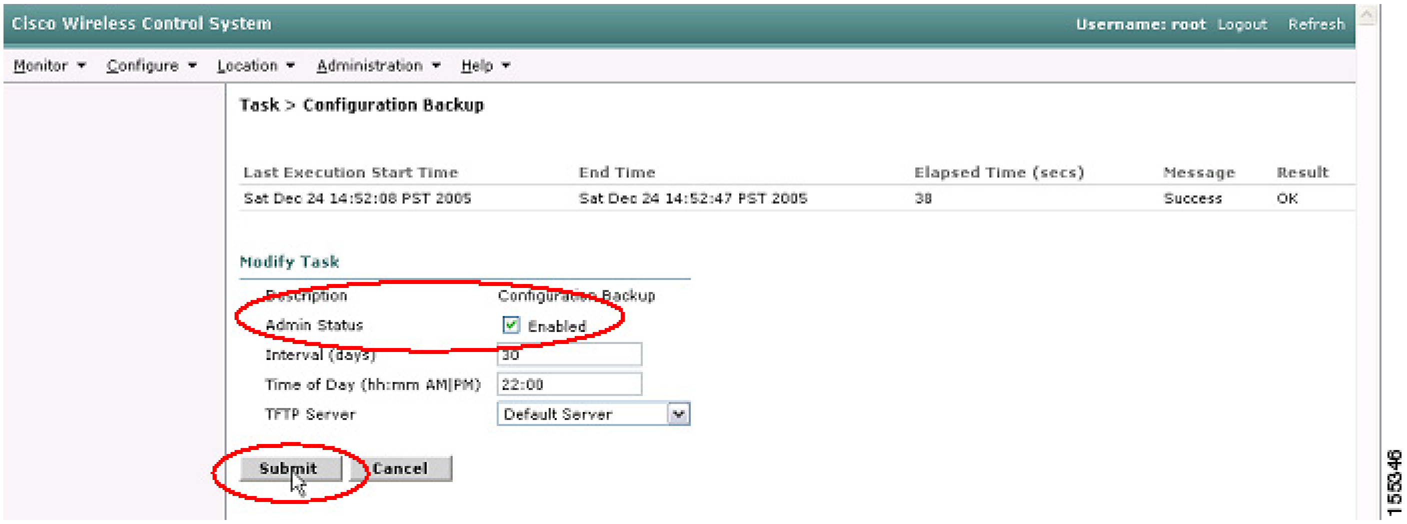
Scheduled Tasks

	Task	Admin Status	Interval	Time of Day	Oper. Status
□	Client Stats Poll	Enabled	15 minutes		Idle
☑	Configuration Backup	Enabled	30 days	22:00	Idle
□	Database Cleanup	Enabled	Daily	02:00	Idle
□	Device Status	Enabled	5 minutes		Idle
□	Location Server Backup	Disabled	7 days	01:00	Idle
□	Location Server Status	Enabled	5 minutes		Idle
□	Location Server Synchronization	Enabled	120 minutes		Idle
□	Network Audit	Enabled	Daily	01:00	Idle
□	Rogue AP	Enabled	120 minutes		Idle
□	Statistics	Enabled	15 minutes		Idle
□	WCS Server Backup	Disabled	7 days	01:00	Idle

Step 4 Check the **Admin Status** check-box and then fill in the appropriate values for **Interval**, **Time of Day**, and **TFTP Server** (see Figure 38).

Step 5 Click **Submit** to commit the changes (see Figure 38).

Figure 38 WCS Scheduled Configuration Backup


Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Submit
Cancel
155346

Task > Configuration Backup

Last Execution Start Time	End Time	Elapsed Time (secs)	Message	Result
Sat Dec 24 14:52:08 PST 2005	Sat Dec 24 14:52:47 PST 2005	38	Success	OK

Modify Task

Description	Configuration Backup
Admin Status	☑ Enabled
Interval (days)	30
Time of Day (hh:mm AM|PM)	22:00
TFTP Server	Default Server

When you want to reset a WLC configuration from the WCS, you may use the Configure | Controllers interface. Select the WLC and then select the appropriate templates to apply to the WLC

Integrating Cisco WiSM and Firewall Service Module

This section includes the following topics:

- Firewall Services Module Overview, page 36
- How the FWSM Works, page 37
- Firewall and Cisco WiSM Implementation Configuration, page 38

Firewall Services Module Overview

The Firewall Services Module (FWSM) is a high-performance, high-speed firewall that can operate up to 5 Gbps. It resides in a single Catalyst 6500 slot and uses VLANs through the backplane to interface with hosts within its domain.

The FWSM supports a maximum of 250 logical (VLAN) interfaces. The FWSM uses VLAN interfaces as its entry and exit points into the networks it serves. The interface schema used is the same as that in the Cisco PIX firewall. Each interface is assigned a security level from 0 to 100, where the lowest security level is 0, and the highest security level is 100. By default, the FWSM has an inside and an outside VLAN interface.

The inside interface has an assigned security level of 100, and the outside interface has an assigned security level of 0. The other logical interfaces that can be created on the FWSM are arbitrarily assigned a security level deemed appropriate by the administrator. These interfaces are often referred to as demilitarized zone (DMZ) interfaces. The definition of what security level is assigned to a particular interface is based on the security policies of that organization.

How the FWSM Works

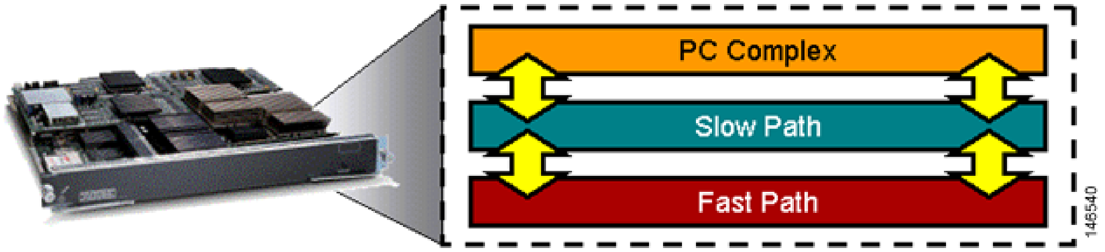
The main feature of the FWSM architecture is the Adaptive Security Algorithm (ASA). The ASA algorithm establishes some fundamental rules that dictate how the FWSM operates. These rules include the following:

- Data flows from one interface to any other interface only if an ACL permits that flow
- No data can pass between interfaces with the same security level
- No packets can traverse the firewall without a connection and state
- Outbound connections are allowed if the access lists permit
- Inbound connections are allowed if access lists permit and have either a dynamic or static translation slot. In order to access the servers in the high security network, a static command is used.
- TCP sequence numbers are random for the inside hosts
- Simple Mail Transfer Protocol (SMTP) FIXUP and TCP intercept functionality are applied only to servers that are in the high security network

The firewall performs the following three levels of processing (see Figure 39):

- PC complex
- Slow path
- Fast path

Figure 39 Firewall Levels of Processing



PC complex is primarily responsible for any L7 processing and associated management tasks such as the following:

- Telnet into the FWSM
- SSH into the FWSM
- Processing SNMP
- OSPF route processing
- URL and FTP logging
- Generating Syslog messages
- TFTP configuration

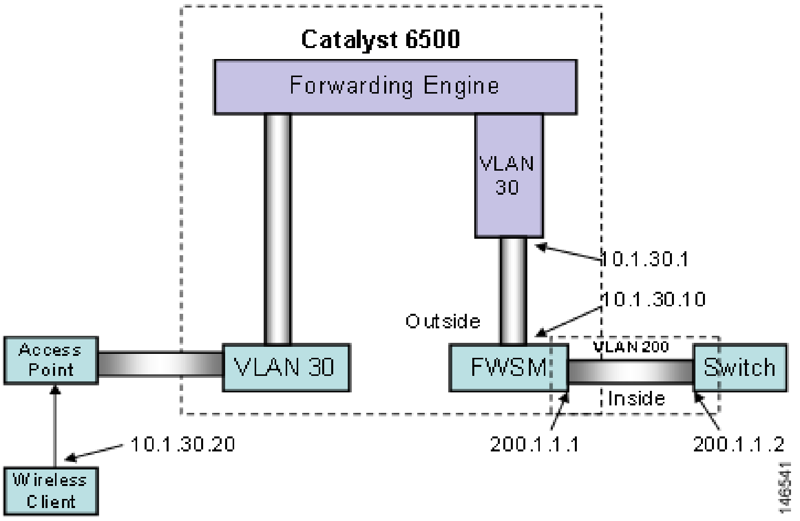
The *slow* and *fast path* processing is performed by network processors located on the FWSM. Slow path processing includes ACL route lookups, TCP intercept, session management, port address translation allocations, and more. Fast path processing facilitates support for multimedia protocols such as H.323, Real-Time Streaming Protocol (RTSP), Session Initiation Protocol (SIP), and so on, performing Network Address Translation (NAT), DNS guard, fragmentation and virtual reassembly, session identification, and more.

During normal packet processing, a packet passes over the Catalyst 6500 backplane into the services baseboard where it is presented to the firewall fast path processing. If the fast path does not handle the particular function, it passes the packet to the slow path process and then to the PC complex if the slow path process does not handle the packet.

Firewall and Cisco WiSM Implementation Configuration

The configuration of the Cisco WiSM described in earlier sections is used as the basis of the FWSM integration example that follows. Figure 40 shows the topology that is created as part of this configuration.

Figure 40 Topology



Configuration of the FWSM begins with a properly installed module. The FWSM can be installed in any of the line card slots in any of the current Catalyst 6500 chassis models. Correct installation of the module results in the following output from a **show module** command.

```
Sup720#sh mod
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  3   10  WiSM WLAN Service Module       WS-SVC-WISM-1-K9   SAD092504J8
  4   48  48-port 10/100 mb RJ45         WS-X6148-45AF      SAL08154UT3
  5    2  Supervisor Engine 720 (Active) WS-SUP720-3BXL       SAL0913827E
  6    6  Firewall Module                WS-SVC-FWM-1         SAD090100D9
```

From the CLI output, you can see that the FWSM is installed in slot 6 and has six ports. The six ports mentioned here are not actually external ports but rather logical connections that the module has to the backplane. In fact, these ports are actually the connections between the baseboard and the daughter card.

Before integrating the FWSM with the Cisco WiSM service module, configure the following prerequisites:

- Configure the management interface in the controller.
- Configure the AP-manager interfaces in the controller.
- Configure both the AP-manager and the management interface as part of the same VLAN network. Create an SVI on the MSFC as the default gateway for this VLAN.
- Assign the access points an IP address from a DHCP server. It can be either in the same network or across an L3 network using the **ip helper-address** CLI command.

The access points associate themselves with the controllers when an IP address has been assigned from the DHCP server. The **show ap summary** command lists these registered LWAPP devices.

The first configuration action assigns VLANs to the FWSM. These VLANs are essentially the firewall interfaces used by the FWSM to interface with the network. VLANs are configured using the VLAN command in the following example:

```
Cat6506(config)#vlan 30
Cat6506(config-vlan)#vlan 200
```

The first VLAN command causes the CLI to enter VLAN configuration mode, which is indicated by the *config-vlan* extension on the CLI prompt. The use of this command does not preclude the creation of the second VLAN at this configuration level.

After creating the VLANs, you must assign (or bind) them to the FWSM using the **firewall vlan-group** command.

```
Cat6506(config)#firewall vlan-group 1 30,200
```

Using this command configures a firewall VLAN group for the FWSM to manage. In this example, it assigns VLANS 30,200 to the VLAN group and assigns a firewall group number (1). This firewall group must now be attached to the FWSM as below:

```
Cat6506(config)#firewall module 6 vlan-group 1
```

The above command associates the firewall VLAN group you created with the earlier command (identified by firewall group 1) with the FWSM in slot 6.

Up to this point, the Catalyst 6500 CLI has issued commands. Use the FWSM CLI to perform subsequent configurations regarding the setting of policies on the FWSM. The administrator must establish a session with the FWSM using the following command:

```
Cat6506# session slot 6 processor 1
User Access Verification
Password:
Type help or '?' for a list of available commands.
FWSM>
```

The **session** command indicates the module with which you want to establish a session. The processor number at the end of the command should remain as 1. At this stage, you can set up the security policies on your FWSM.

When inside the firewall, configure the VLANs to be used by the firewall along with their IP addresses. The configuration statements are as follows:

```
FWSM> enable
Password:
FWSM# conf t
FWSM(config)# nameif vlan30 outside security0
FWSM(config)# nameif vlan200 inside security100
```

The first time you enter enable mode in the FWSM (identified by the FWSM# prompt), the enable password is not set. You must press **Enter** to enter enable mode. You should set the enable password to better restrict access to this operational mode.

First, use the **nameif** command to define the VLAN interfaces. Each VLAN is identified with a name (in the above case, *inside* and *outside*) and assigned a security level. Security levels are assigned a value from 0 to 100, where 0 is the least secure and 100 is the most secure. These values are arbitrary and can be set to any value by the administrator. Next, assign the newly created interfaces an IP address as follows:

```
FWSM(config)#ip address outside 10.1.30.10 255.255.255.0
FWSM(config)#ip address inside 200.1.1.1 255.255.255.0
```

Some additional commands are optional but are useful in the ongoing administration of the FWSM. One of these commands is **enable pings**. By default, the FWSM does not respond to pings on any of its interfaces. If the outside or inside interface of the FWSM needs to be pinged, you must enable this on the FWSM. For example, you can enable ping replies on the inside interface (and optionally outside) of the FWSM as follows:

```
FWSM(config)#icmp permit any inside
FWSM(config)#icmp permit any outside
```

Create policies on the firewall using access control lists. In our example, we want to permit traffic from 200.1.1.0 (inside the firewall) to 10.1.30.0 (where the wireless client resides) in the following manner:

```
FWSM(config)#access-list 101 extended permit tcp 200.1.1.0 255.255.255.0 10.1.30.0
255.255.255.0
```

As in Cisco IOS software, an implicit "deny all" message can appear at the end of this access list. You must then apply the access list to the outside interface as follows:

```
FWSM(config)#access-group 101 in interface inside
```

Traffic flows from the wireless domain back to the inside in the following manner:

```
FWSM(config)#access-list 102 extended permit tcp 10.1.30.0 255.255.255.0 200.1.1.0
255.255.255.0
```

Now, create a VRF instance as follows. This is the first step towards configuring the VRF on the tunnel interface.

```
c6506(config)#ip vrf wism-fwsm
c6506(config-vrf)#rd 1:100
c6506(config-vrf)#route-target export 1:100
c6506(config-vrf)#route-target import 1:100
```

With this set of commands, a VRF instance called *wism-fwsm* is created. A route descriptor (RD) of 1:100 is added to each of the IPV4 prefixes in the forwarding table. These RDs associate the prefixes with this VRF instance.

Next, apply the VRF to the VLAN interface as follows:

```
c6506#conf t
```

Enter configuration commands, one per line, and end with **CNTL/Z**.

```
c6506(config)#interface vlan 30
c6506(config)#ip vrf forwarding wism-fwsm
% Interface Vlan30 IP address 10.1.30.1 removed due to disabling VRF wism-fwsm
```

When applying the VRF to the VLAN interface, the IP address is removed. Add the IP address back onto the interface before proceeding with the next step.

VLAN interface 201 must also be added into the same VRF so that the tunnel interface can see VLAN 201 in its route table and thus forward data onto the FWSM.

To finish the VRF configuration, install a static route in the VRF, and the global routing table points all traffic inbound from the wireless clients into the switch, to the firewall, and vice versa.

```
c6506#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
c6506(config)# ip route vrf wism-fwsm 200.1.1.0 255.255.255.0 10.1.30.10
```

The first configuration statement adds a static route into the VRF instance called *wism-fwsm.* It states that any data destined to network 200.1.1.0 is forwarded to the next hop address 10.1.30.10 (the VLAN interface on the FWSM). This static route is only applicable to any interface using that VRF.

The complete configuration on the 6500 is shown below:

Note If the switch is running Cisco IOS software release 12.2.(18)SXF11, 12.2.(33)SXH or later and you have configured auto-LAG, the output of the **show run** command will not show the Gigabit interfaces for the WiSM.

Note If the switch is running Cisco IOS software release 12.2.18SXF6 or later and you have configured auto-LAG, the output of the **show run** command will not show the port-channel interfaces that are created automatically with auto-LAG.

```
Sup720#show run
Building configuration...

Current configuration : 8069 bytes
!
upgrade fpd auto
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service counters max age 10
!
hostname cat6506
!
enable password cisco
!
no aaa new-model
clock timezone PDT -7
firewall multiple-vlan-interfaces
firewall module 6 vlan-group 1
firewall vlan-group 1  30,200
```

```
ip subnet-zero
!
!
ip dhcp excluded-address 192.168.10.1 192.168.10.2
!
```

```
ip dhcp pool wism-service-port
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
ip dhcp pool net
!
ip vrf wism-fwsm
 rd 1:100
 route-target export 1:100
 route-target import 1:100
!
no ip domain-lookup
ipv6 mfib hardware-switching replication-mode ingress
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
!
!
wism service-vlan 192
!
interface Port-channel1
 description wism-pod1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 mls qos trust dscp
 spanning-tree portfast
 no ip address
!
interface Port-channel2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 mls qos trust dscp
 spanning-tree portfast
 no ip address
!
interface Port-channel3
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 mls qos trust dscp
 spanning-tree portfast
 no ip address
!
interface GigabitEthernet3/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
 channel-group 1 mode on
!
interface GigabitEthernet3/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 mls qos trust dscp
 spanning-tree portfast
 no ip address
 channel-group 1 mode on
!
interface GigabitEthernet3/3
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 mls qos trust dscp
 spanning-tree portfast
 no ip address
 channel-group 1 mode on
!
interface GigabitEthernet3/4
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 mls qos trust dscp
 spanning-tree portfast
 no ip address
 channel-group 1 mode on
!
interface GigabitEthernet3/5
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 mls qos trust dscp
 spanning-tree portfast
 no ip address
 channel-group 2 mode on
!
interface GigabitEthernet3/6
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 mls qos trust dscp
 spanning-tree portfast
 no ip address
channel-group 2 mode on
!
interface GigabitEthernet3/7
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 mls qos trust dscp
 spanning-tree portfast
 no ip address
 channel-group 2 mode on
!
interface GigabitEthernet3/8
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 mls qos trust dscp
 spanning-tree portfast
 no ip address
 channel-group 2 mode on
!
interface FastEthernet4/1
 switchport
 no ip address
!
< snip >
!
interface FastEthernet4/13
 switchport
 switchport access vlan 40
 no ip address
!
interface FastEthernet4/14
 switchport
 switchport access vlan 40
 no ip address
!
< snip >
!
interface FastEthernet4/25
 description Host for the inside of FWSM 200.1.1.20
 switchport
 switchport access vlan 200
 no ip address
!
interface Vlan1
 ip address 10.1.1.2 255.255.255.0
!
interface Vlan30
 ip vrf forwarding wism-fwsm
 ip address 10.1.30.1 255.255.255.0
 ip helper-address 10.1.1.11
!
interface Vlan40
 ip address 40.1.1.1 255.255.0.0
 ip helper-address 10.1.1.11
!
interface Vlan192
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan200
 ip address 200.1.1.2 255.255.255.0
!
!
router eigrp 100
 network 10.0.0.0
 network 192.168.0.0
 no auto-summary
!
ip classless
ip route vrf wism-fwsm 200.1.1.0 255.255.255.0 10.1.30.10
!
no ip http server
!
!control-plane
!
dial-peer cor custom
!
line con 0
line vty 0 4
 password cisco
 no login
!
```

```
end

cat6506#
The complete configuration on the FWSM is shown below:

FWSM# show run
: Saved
:
FWSM Version 2.3(2)
nameif vlan30 outside security0
nameif vlan200 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname FWSM
ftp mode passive
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol rsh 514
fixup protocol sip 5060
no fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 102 extended permit tcp any host 10.1.30.254 eq www
access-list 101 extended permit tcp 200.1.1.0 255.255.255.0 any eq www
pager lines 24
logging buffer-size 4096
mtu outside 1500
mtu inside 1500
ip address outside 10.1.30.10 255.255.255.0
ip address inside 200.1.1.1 255.255.255.0
no failover
failover lan unit secondary
failover polltime unit 1 holdtime 15
failover polltime interface 15
failover interface-policy 50%
icmp permit any outside
icmp permit any inside
no pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 10.1.30.254 200.1.1.20 netmask 255.255.255.255
access-group 102 in interface outside
access-group 101 in interface inside
!
interface outside
!
interface inside
!
route outside 0.0.0.0 0.0.0.0 10.1.30.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
```

```
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
floodguard enable
fragment size 200 outside
fragment chain 24 outside
fragment size 200 inside
fragment chain 24 inside
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:fd9eac84597419d0969d1d906705d122
: end
[OK]
FWSM#
: end
```

The configuration is now complete. Data from the wireless clients is forwarded to the tunnel interface and then forwarded to the outside interface of the FWSM. The firewall now needs its security policies applied to determine what traffic can or cannot pass.

Integrating Cisco WiSM and VPN Service Module

This section includes the following topics:

- VPNSM Overview
- How the VPNSM Works
- VPNSM Configuration with the Cisco WiSM

VPNSM Overview

The VPN Services Module (VPNSM) was introduced as a high-performance VPN option to further extend the existing VPN portfolio of products from Cisco. The VPNSM is part of the Catalyst 6500 service module family, which comprises the Firewall Services Module (FWSM), Content Switching Module (CSM), Intrusion Detection System Module (IDSM), Network Analysis Module (NAM), and the Secure Socket Layer Module (SSL).

The VPNSM, like other service modules, is geared to provide high-performance services accelerated by hardware offering up to 1.9 Gbps of Triple Data Encryption Standard (3DES) data (at 500-byte packets) and 1.6 Gbps of 3DES traffic at a smaller packet size of 300 bytes.

The VPNSM offers the following features:

- Single slot in the Catalyst 6500 chassis
- Connections to both the 32 GB bus and the 256 GB crossbar
- High-speed VPN performance offering up to 1.9 Gbps of 3DES performance
- Catalyst 6500 integration, which allows a combination switch and VPN service
- Support for industry-recognized encryption algorithms, including DES and 3DES
- Multiple authentication schemes, including X.509 digital certificates, RADIUS, TACACS, PAP/CHAP, shared secrets, and simple certificate enrollment protocol

- Increased up time for IPSec tunnels
- Key management using Internet Key Exchange (IKE)
- Certificate Authority support
- Enhanced resilience by utilizing existing Catalyst 6500 routing protocols and resilience features such as HSRP, along with inbuilt resilience features such as Internet Key Exchange (IKE) keepalives
- Embedded web-based VPN Device Manager (VDM) for single device management
- Integration with VPN Solution Center (VPNSC) management solution for large enterprise or service provider management
- Built-in web-based device management using CiscoView Device Manager

How VPNSM Works

Unlike some of the other Catalyst 6500 services modules, the VPNSM does not rely on either the SPAN facility or VACL capture facility to process VPN traffic. The VPNSM must be placed in the path of traffic so that it can apply VPN processing to any traffic matching the configured ACL criteria; therefore, you should carefully consider design and implementation of the VPNSM.

Physical modifications to the network may be required in order to place the VPNSM in the path of the necessary traffic. Also, unlike many of the other service modules, the VPNSM is configured directly from the Cisco IOS CLI. There is no need to access (or Telnet) into the module to configure it.

When a VPN module is installed into a Catalyst 6500/7600 chassis, it determines whether Catalyst 6500 interfaces and ports in that chassis belong to the inside network (local LAN) or the outside network (outside world). The determination of whether ports are inside or outside impacts the way VLANs are set up and how they interact with VPNSM. All ports that connect to the outside world (external networks) are referred to as *Catalyst outside ports*, and those within the local LAN network are referred to *Catalyst inside ports*. If an Ethernet 10/100 port (for example, port 5) on module 3 (port 3/5) was connected to an inside server, then that port is designated as a Catalyst inside port. If the same port were connected to the WAN router, then that port is designated as a Catalyst outside port.

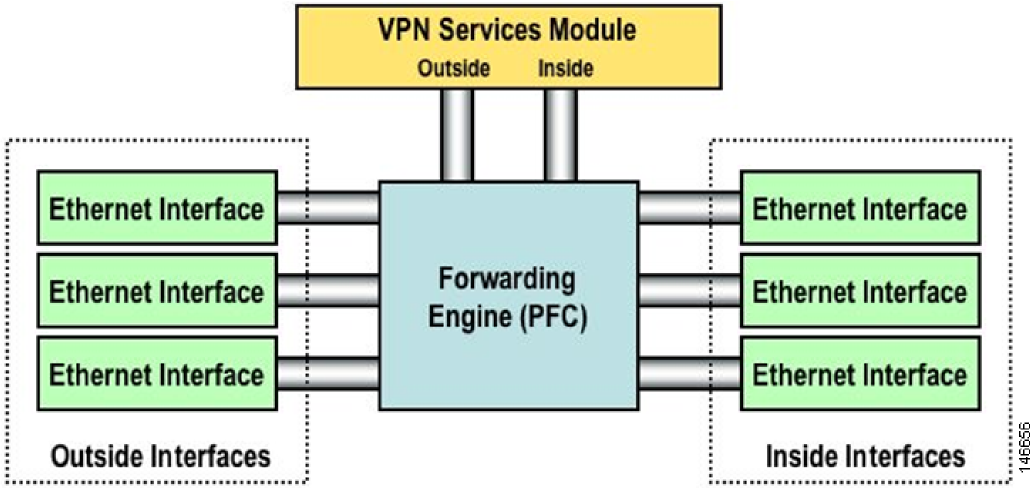
While the VPN module has no external (physical) ports, it has two logical ports that connect the VPN module to the backplane of the Catalyst 6500/7600. These two logical ports are configured as Gigabit Ethernet (GE) ports from the command line interface (CLI). The VPN ports can be seen from the following **show module** command from the supervisor CLI:

```
c6506# sh mod
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  2    2  IPSec VPN Accelerator                  WS-SVC-IPSEC-1     SAD0837063H
  3   10  WiSM WLAN Service Module=          WS-SVC-WiSM-1-K9   SAD092504J8
  4   48  48-port 10/100 mb RJ45                 WS-X6148-45AF      SAL08154UT3
  5    2  Supervisor Engine 720 (Active)         WS-SUP720-3BXL     SAL0913827E
  6    6  Firewall Module                        WS-SVC-FWM-1       SAD090100D9

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  2  0003.e470.05cc to 0003.e470.05cf   1.3   7.2(1)       8.5(0.46)RFW Ok
  3  0001.0002.0003 to 0001.0002.0012   0.1   12.2(14r)S5  12.2(PP_R31_ Ok
  4  0011.206d.7ef0 to 0011.206d.7f1f   1.0   5.4(2)       8.5(0.46)RFW Ok
  5  0013.7f0d.114c to 0013.7f0d.114f   4.3   8.1(3)       12.2(PP_R31_ Ok
  6  0012.8005.d418 to 0012.8005.d41f   3.0   7.2(1)       2.3(2)       Ok
```

```
Mod  Sub-Module                  Model              Serial       Hw     Status 
---- --------------------------- ------------------ ----------- ------- -------
  3  Centralized Forwarding Card FARFEL             SAD092608SU  0.2    Ok
  4  IEEE Voice Daughter Card    WS-F6K-FE48-AF     SAD082007YH  1.1    Ok
  5  Policy Feature Card 3       WS-F6K-PFC3BXL     SAL091597AS  1.6    Ok
  5  MSFC3 Daughterboard         WS-SUP720          SAL09158X9K  2.3    Ok

Mod  Online Diag Status 
---- -------------------
  2  Pass
  3  Pass
  4  Pass
  5  Pass
  6  Pass
```

The VPN designates one of these logical GE ports as the *VPN inside port* and the other logical GE port as the *VPN outside port*. The designation of which VPN port is the inside and outside port is fixed and cannot be changed. Port 1 is always treated as the VPNSM inside port, and Port 2 is always treated as the VPNSM outside port. The VPN inside port is used to transfer data to and from the Catalyst inside ports, and the VPN outside port is used to transfer data to and from the Catalyst outside ports, as shown in Figure 22.

Figure 41 Catalyst and VPN Inside and Outside Ports



Normally, the Catalyst outside ports are connected either directly to the LAN/WAN or to a WAN device that connects to an external network. The VPN outside port is grouped with the Catalyst outside ports so the VPN processing of packets comes into the VPNSM. You need to place the VPN outside port and the Catalyst outside ports in the same VLAN to accomplish this. This VLAN is normally set as a Layer 2 VLAN, and no associated VLAN interface is set on the MSFC. However, to interoperate with the Cisco WiSM, the VLAN interface that is associated with the VPN outside interface is set up as a Layer 3 interface.

An *interface VLAN* is created on the MSFC. This port is placed in the same VLAN as the VPN inside port. This interface VLAN has the security configuration assigned to it. For instance, any crypto maps that are configured are usually applied to this VLAN interface. Do not add any other ports to this VLAN. Cisco recommends that any Catalyst inside ports use the PFC to L3 switch data to the VPNSM.

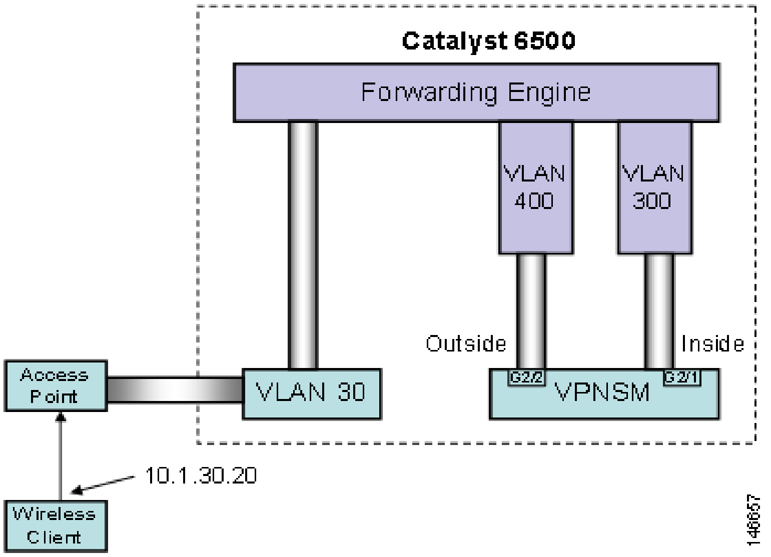
VPNSM Configuration with the Cisco WiSM

To integrate Cisco WiSM with the VPNSM, we use the following process: VRFs on the ingress tunnel interface push ingress VPN packets to the outside VPNSM interface as the next hop. The VRF may need to be primed with a static route that has the destination VPN peer address as its next hop. Other traffic not destined for the VPNSM is forwarded as required.

This configuration assumes that the Cisco WiSM setup described earlier in this paper is working and that the wireless client can successfully authenticate and register with the network.

The integration of the VPNSM with the wireless setup is based on the diagram in Figure 23.

Figure 42 Topology of the VPNSM with the Cisco WiSM



First, we need to explore the basic VPN configuration statements that allows a VPN client to connect with the VPNSM. Those key configuration statements are listed below:

```
c6506(config)#crypto isakmp policy 1
c6506(config-isakmp)#encr 3des
c6506(config-isakmp)#hash md5
c6506(config-isakmp)#auth pre-share
c6506(config-isakmp)#group 2
c6506(config-isakmp)#exit
```

This set of statements defines a crypto policy, which is used to define the crypto environment that connects the VPN client with the VPNSM. This policy defines the use of the 3DES algorithm for encrypting traffic. The MD5 hash algorithm is used to protect passwords; and *group 2* refers to the use of Diffie-Hellman Group 2 (1024 bit) key generation.

The following statement defines the ISAKMP key that the VPN client uses to establish a VPN session with the VPNSM:

```
c6506(config)#crypto isakmp key cisco1 address 0.0.0.0 0.0.0.0
```

The key is defined as *cisco1*. The address component of the statement sets classification criteria for the address of the incoming VPN client address. The use of 0.0.0.0 is a catch-all and provides a match for all incoming connections.

The following statements are ISAKMP tuning values used to set the interval between keepalives and the amount of idle time allowed in the ISAKMP setup before the session is closed:

```
c6506(config)#crypto isakmp keepalive 10
c6506(config)#crypto isakmp xauth timeout 45
```

The following set of statements defines the attributes using the group access information name of vpnsm-with-remclient. The attributes include the key and the address pool used when assigning an IP address to the client.

```
c6506(config)#crypto isakmp client configuration group wism-vpnsm
c6506(config-isakmp-group)#key cisco1
c6506(config-isakmp-group)#domain cisco.com
c6506(config-isakmp-group)#pool pool-1
c6506(config-isakmp-group)#crypto dynamic-map dynmap 1
c6506(config-crypto-map)#exit
```

After the initial VPN tunnel has been set up, the following **transform set** defines a set of crypto attributes for data transmission. It defines the usable encryption algorithm options to be negotiated between the VPNSM and the VPN client for this VPN session.

```
c6506(config)#crypto ipsec transform-set transform-1 esp-3des esp-sha-hmac
```

The following **crypto map** indicates the transform set to use. The use of reverse route is to instruct the switch to install a route into the local routing table that points back to the client on successful VPN setup.

```
c6506(config)#crypto dynamic-map dynmap 1
c6506(config-crypto-map)#set transform-set transform-1
c6506(config-crypto-map)#reverse-route
c6506(config-crypto-map)#exit
c6506(config)#crypto map client-map client authentic list vpnusers
c6506(config)#crypto map client-map isakmp authorization list vpnsm-with-remclient
c6506(config)#crypto map client-map client configuration address respond
c6506(config)#crypto map client-map 1 ipsec-isakmp dynamic dynmap
```

The final collection of **crypto map** statements pull many of the configured elements above into a composite crypto map that is bounded to the port from which the remote client peers.

Next, the interface with which the VPN client peers must be defined. In the above example, VLAN 300 has been created for this purpose. It is set up as a Layer 3 interface with an IP address assigned to it. It uses the **crypto map** command to identify which crypto policy is being used. The crypto policy indicates which crypto features are available to set up and manage data through the VPN tunnel.

The following local pool command defines a set of IP addresses that are assigned to each authenticated incoming user. In the example above, an address pool named *remote-pool* has been set up to serve addresses from a 172.16 network. Addresses 10.10 through 10.254 are available for this pool.

```
c6506(config)#ip local pool pool-1 172.16.10.10 172.16.10.254
```

The following set of statements authenticates incoming VPN connections to the VPNSM. They reference some of the group definitions stated earlier in this configuration section.

```
c6506(config)#aaa new-model
c6506(config)#aaa authen login def local
c6506(config)#aaa authen login vpnusers local none
c6506(config)#aaa author network vpnusers local
```

Now configure the VPNSM logical interfaces as follows:

```
c6506(config)#interface g2/1
c6506(config-if)#no ip address
c6506(config-if)#switchport
c6506(config-if)#switchport trunk encap dot1q
```

```
c6506(config-if)#switchport trunk allowed vlan 300
c6506(config-if)#switchport mode trunk

c6506(config-if)#int g2/2
c6506(config-if)#no ip address
c6506(config-if)#switchport
c6506(config-if)#switchport trunk encap dot1q
c6506(config-if)#switchport trunk allowed vlan 400
c6506(config-if)#switchport mode trunk
```

In the above example, the VPNSM has been installed in slot 2. Port is always deemed the inside VPN port, and Port 2 is the outside VPN port. This nomenclature is fixed (internal to the VPNSM) and cannot be changed. Both ports are set up as 802.1q trunk ports and have no IP address associated with them.

The main configuration option specifies which VLANs the user wants to allow across each of the ports. The inside port VLAN must match the VLAN interface which has the crypto maps applied to it. The permitted VLANs on the VPNSM outside port must match the VLAN on which the outside switch port is located.

```
c6506(config)#int vlan 300
c6506(config-if)#ip add 22.1.1.2 255.255.255.0
c6506(config-if)#crypto map client-map
c6506(config-if)#crypto engine slot 2

c6506(config)#interface Vlan400
c6506(config-if)#ip address 22.1.1.3 255.255.255.0
c6506(config-if)#
00:57:14: %CRYPTO: Wrong config: MAC addresses are the same between VLAN 300 and VLAN 400.
c6506(config-if)#mac-add 0000.cccc.dddd
c6506(config-if)#crypto connect vlan 300
c6506(config-if)#crypto engine slot 2
```

When you configure the VPNSM for normal operation, each VLAN that contains ports receiving traffic from the wireless world needs to have the crypto connect command applied to it.

In the configuration example above, VLAN interface 400 is the interface facing the outside. The **crypto connect vlan** command ties this port to the VPN inside port. The VLAN specified as part of the crypto connect command is the VLAN interface where the crypto map is applied (containing the crypto policy for incoming sessions). The first time a crypto connect vlan command is applied in the configuration, a hardware crypto engine that sits on the VPNSM is activated.

VLAN 400 also needs to operate in Layer 3 mode; therefore, you need an IP address to route packets from the tunnel interface to the outside interface. However, the VPNSM continues to operate at Layer 2, so the IP address must be in the same subnet as the inside interface. Using VRF, you can assign two IP addresses in the same subnet to two different VLAN interfaces.

In addition, a different MAC address for this interface is needed. When defining a VLAN interface, the MAC is assigned by the supervisor to be part of the static pool on the box, and all the virtual interfaces get the same MAC address by default. Generally, when interfaces are in different subnets, this is not a problem. However, with VLAN interfaces that are connected to the VPNSM, at least one interface between VLAN interface 300 and 300 must be manually configured with a MAC address.

The following VRF configuration is necessary for the tunnel interface and for the interface VLAN outside:

```
c6506(config)#ip vrf wism-vpnsm
c6506(config-vrf)#rd 2:100
c6506(config-vrf)#route-target export 2:100
c6506(config-vrf)#route-target import 2:100
```

With this set of commands, we have created a VRF instance called *wism-vpnsm*. A route descriptor (RD) of 2:100 is added to each of the IPV4 prefixes in the forwarding table to associate them with this VRF instance.

```
Next, the VRF needs to be applied to the tunnel interface and to the outside VLAN
interface that is associated with the outside VPNSM interface. This is done as follows:
c6506#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
c6506(config)#interface vlan 30
c6506(config-if)#ip vrf forwarding wism-vpnsm
c6506(config-if)#ip address 10.1.30.1 255.255.255.0
c6506(config-if)#interface vlan400
c6506(config-if)#ip vrf forwarding wism-vpnsm
% Interface Vlan400 IP address 22.1.1.3 removed due to enabling VRF wism-vpnsm
c6506(config-if)#ip address 22.1.1.3 255.255.255.0
```

When the VRF is applied to the interface, the IP address is removed. The IP address needs to be reapplied onto the interface before you proceed to the next step.

The WLAN traffic coming from the VLAN interface is destined to the IP address of the VPN server (22.1.1.2 in this example, which is the IP address on the inside VLAN of the VPNSM). The router checks its VRF *wism-vpnsm* routing table and sees that this destination IP address is directly connected to the outside interface (VLAN 400). If IPsec is the only traffic you receive from the tunnel interface, then no static route statement in the VRF domain is needed. All packets are routed out of interface VLAN 400 because it is in the same subnet as the destination. However, if you have something besides encrypted traffic, you need to use a vrf static route in the VRF domain to forward the packets where appropriate.

For the reverse path of traffic destined to the wireless client, the reverse route injection feature configured with *crypto dynamic-map* ensures that a host route for the VPN client gets installed in the default VRF routing table, pointing to the inside interface of the VPN module.

Some final configuration statements must be applied to complete the configuration. A static ARP entry must be added into the VRF MAC table for the inside VLAN interface and also for the VLAN outside interface. Because ARP is not supported through the VPN blade, the supervisor needs the IP/MAC mapping to forward the packets.

```
c6506(config)#arp vrf wism-vpnsm 22.1.1.2 0005.dc56.9400 ARPA
c6506(config)#arp 22.1.1.3 0000.cccc.dddd ARPA
```

Also, a username and password needs to be defined for when the VPN client connects to the VPN services module. For this example, simply use the *cisco* username and password as follows:

```
c6506(config)#username cisco password 0 cisco
```

The final configuration for the 6500 is the following:

Note If the switch is running Cisco IOS software release 12.2.(18)SXF11, 12.2.(33)SXH or later and you have configured auto-LAG, the output of the **show run** command will not show the Gigabit interfaces for the WiSM.

```
c6506#show run
Building configuration...

Current configuration : 10194 bytes
!
upgrade fpd auto
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
service counters max age 10
!
hostname cat6506
!
boot system flash disk0:s72033-adventerprisek9_wan_dbg-mz.PP_R31_INTEG_051018
enable password cisco
!
username cisco password 0 cisco
username test password 0 cisco
aaa new-model
aaa authentication login default local
aaa authentication login vpnusers local none
aaa authorization network vpnusers local
!
aaa session-id common
clock timezone PDT -7
firewall multiple-vlan-interfaces
firewall module 6 vlan-group 1
firewall vlan-group 1  30,200
ip subnet-zero
!
!
ip dhcp excluded-address 10.0.2.1 10.0.2.20
ip dhcp excluded-address 172.16.23.1 172.16.23.20
ip dhcp excluded-address 192.168.10.1 192.168.10.2
!
ip dhcp pool 172
   network 172.16.23.0 255.255.255.0
   default-router 172.16.23.1
   domain-name cisco.com
!
ip dhcp pool wism-service-port
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
ip dhcp pool net
!
ip dhcp pool scream
   network 10.101.101.0 255.255.255.0
   domain-name cisco.com
   dns-server 192.168.1.1
   default-router 10.101.101.1
!
ip dhcp snooping vlan 221
ip dhcp snooping
ip vrf contractor_access
 rd 11:1
!
ip vrf wism-fwsm
 rd 1:100
 route-target export 1:100
 route-target import 1:100
!
ip vrf wism-vpnsm
 rd 2:100
 route-target export 2:200
 route-target import 2:200
!
no ip domain-lookup
ipv6 mfib hardware-switching replication-mode ingress
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
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco1 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
crypto isakmp xauth timeout 45

!
crypto isakmp client configuration group wism-vpnsm
 key cisco1
 domain cisco.com
 pool pool-1
!
!
crypto ipsec transform-set transform-1 esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
 reverse-route
!
!
crypto map client-map client authentication list vpnusers
crypto map client-map isakmp authorization list vpnusers
crypto map client-map client configuration address respond
crypto map client-map 1 ipsec-isakmp dynamic dynmap
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
!
power redundancy-mode combined
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
port-channel per-module load-balance
wism service-vlan 192
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
interface Port-channel1
 description wism-pod1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 no ip address
!
interface Port-channel2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 no ip address
!
```

```
interface Port-channel3
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 no ip address
!
interface GigabitEthernet2/1
 description VPNSM inisde port
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 300
 switchport mode trunk
 mtu 4500
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet2/2
 description VPNSM outside port
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 400
 switchport mode trunk
 mtu 4500
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet3/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 no ip address
 channel-group 1 mode on
!
interface GigabitEthernet3/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 no ip address
 channel-group 1 mode on
!
interface GigabitEthernet3/3
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 no ip address
 channel-group 1 mode on
!
interface GigabitEthernet3/4
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 no ip address
 channel-group 1 mode on
!
interface GigabitEthernet3/5
```

```
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 no ip address
 channel-group 2 mode on
!
interface GigabitEthernet3/6
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 no ip address
 channel-group 2 mode on
!
interface GigabitEthernet3/7
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 no ip address
 channel-group 2 mode on
!
interface GigabitEthernet3/8
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 no ip address
 channel-group 2 mode on
!
< snip >
interface Vlan1
 ip address 10.1.1.2 255.255.255.0
!
!
interface Vlan30
 ip vrf forwarding wism-vpnsm
 ip address 10.1.30.1 255.255.255.0
 ip helper-address 10.1.1.11
!
interface Vlan40
 ip address 40.1.1.1 255.255.0.0
 ip helper-address 10.1.1.11
!
interface Vlan192
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan300
 ip address 22.1.1.2 255.255.255.0
 no mop enabled
 crypto map client-map
 crypto engine slot 2
!
interface Vlan400
 description to Outside VPNSM
 mac-address 0000.cccc.dddd
 ip vrf forwarding wism-vpnsm
 ip address 22.1.1.3 255.255.255.0
 crypto engine slot 2
 crypto connect vlan 300
!
router eigrp 100
 network 10.0.0.0
network 192.168.0.0
 no auto-summary
!
ip local pool pool-1 172.16.12.100 172.16.12.254
ip classless
ip route 10.1.30.0 255.255.255.0 22.1.1.3
ip route 172.16.10.0 255.255.255.0 22.1.1.3
ip route vrf wism-vpnsm 0.0.0.0 0.0.0.0 22.1.1.2
!
no ip http server
!
arp vrf wism-vpnsm 22.1.1.2 0005.dc56.9400 ARPA
arp 22.1.1.3 0000.cccc.dddd ARPA
!
!
radius-server source-ports 1645-1646
!
control-plane
!
dial-peer cor custom
!
!
line con 0
line vty 0 4
 password cisco
!
!
no cns aaa enable
end
```

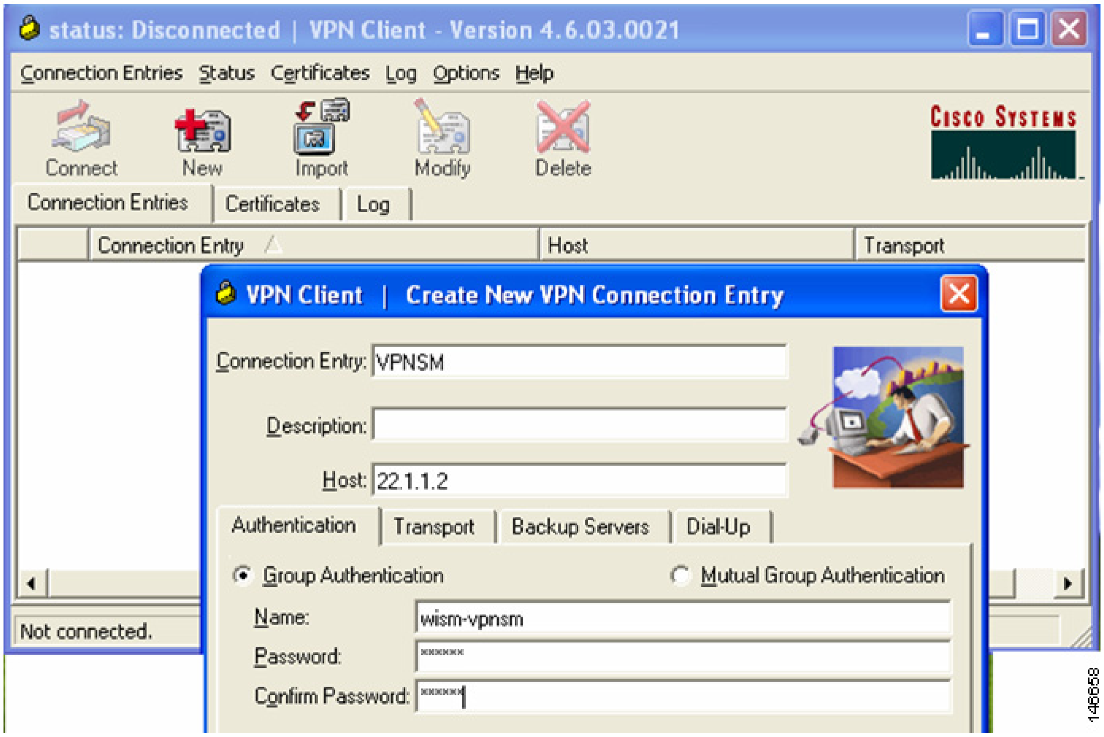
Configuring the VPN Client

After the switch side of the VPN configuration is done, the VPN client must be configured as follows.

Step 1 Start the VPN client.

Step 2 Create a new profile to use when dialing into the VPNSM. On the initial VPN client window, click **New** to create a profile. The Create New VPN Connection Entry window appears (see Figure 43).

Figure 43 Create New VPN Connection Entry



status: Disconnected | VPN Client - Version 4.6.03.0021

VPN Client | Create New VPN Connection Entry

Connection Entry: VPNSM

Description:

Host: 22.1.1.2

● Group Authentication ○ Mutual Group Authentication

Name: wism-vpnsm

Password: ******

Confirm Password: ******

Step 3 Add a name for the connection entry.

Step 4 Enter the IP address of the remote end VPN device. In the Catalyst 6500 configuration above, it is set as 22.1.1.2 and is actually the address for VLAN interface 300.

Step 5 Enter the VPN client group name and the associated password as shown in Figure 24. Obtain both of these values from the Catalyst 6500 configuration above. In the example, the group access information values are *wism-vpnsm* as the group name and *cisco1* as the password. The password must be entered twice to verify correct entry.

Step 6 Click **Save**.

The profile is now defined, and you can initiate a VPN connection with the VPNSM.

To initiate the connection, choose the connection entry just defined from the main window and click **Connect**.

When the VPN process is initiated, the EZ-VPN client establishes a connection with the VPNSM and initially negotiates a security association. During this phase, a common set of crypto values are agreed upon by both ends. The client is then challenged to enter a username and password to validate access rights.

After successfully logging in, the client sees a lock icon in the Windows system tray located in the bottom right-hand corner of the desktop.