Configuring Ports and Interfaces

This chapter contains these sections:

• Information About Ports, page 4-1
• Information About Interfaces, page 4-3
• Configuring the Management Interface, page 4-4
• Configuring the AP-Manager Interface, page 4-8
• Configuring Virtual Interfaces, page 4-11
• Configuring Service-Port Interfaces, page 4-13
• Configuring Dynamic Interfaces, page 4-15
• Information About Dynamic AP Management, page 4-20
• Information About WLANs, page 4-20
• Configuring Ports, page 4-22
• Using the Cisco 5500 Series Controller USB Console Port, page 4-24
• Choosing Between Link Aggregation and Multiple AP-Manager Interfaces, page 4-26
• Configuring Link Aggregation, page 4-26
• Configuring Multiple AP-Manager Interfaces, page 4-32
• Configuration Example: Configuring AP-Manager on a Cisco 5500 Series Controller, page 4-37
• Configuring VLAN Select, page 4-39
• Configuring Interface Groups, page 4-40
• Multicast Optimization, page 4-42

Information About Ports

A port is a physical entity that is used for connections on the controller platform. Controllers have two types of ports: distribution system ports and a service port. Figure 4-1 shows the ports available on a 5500 series controller as an example.
Chapter 4  Configuring Ports and Interfaces

Information About Ports

This section contains the following topics:

- Information About Distribution System Ports, page 4-2
- Information About Service Ports, page 4-3
- Additional References, page 4-4

Information About Distribution System Ports

A distribution system port connects the controller to a neighbor switch and serves as the data path between these two devices.

Guidelines and Limitations

- Cisco 5508 Controllers have eight Gigabit Ethernet distribution system ports, through which the Controller can manage multiple access points. The 5508-12, 5508-25, 5508-50, 5508-100, and 5508-250 models allow a total of 12, 25, 50, 100, or 250 access points to join the controller. Cisco 5508 controllers have no restrictions on the number of access points per port. However, we recommend using link aggregation (LAG) or configuring dynamic AP-manager interfaces on each Gigabit Ethernet port to automatically balance the load. If more than 100 access points are connected to the Cisco 5500 Series Controller, make sure that more than one Gigabit Ethernet interface is connected to the upstream switch.
Note

The Gigabit Ethernet ports on the Cisco 5508 Controllers accept these SX/LC/T small form-factor plug-in (SFP) modules:
- 1000BASE-SX SFP modules, which provide a 1000-Mbps wired connection to a network through an 850nm (SX) fiber-optic link using an LC physical connector
- 1000BASE-LX SFP modules, which provide a 1000-Mbps wired connection to a network through a 1300nm (LX/LH) fiber-optic link using an LC physical connector
- 1000BASE-T SFP modules, which provide a 1000-Mbps wired connection to a network through a copper link using an RJ-45 physical connector

Each distribution system port is, by default, an 802.1Q VLAN trunk port. The VLAN trunking characteristics of the port are not configurable.

Information About Service Ports

Cisco 5500 Series Controllers also have a 10/100/1000 copper Ethernet service port. The service port is controlled by the service-port interface and is reserved for out-of-band management of the controller and system recovery and maintenance in the event of a network failure. It is also the only port that is active when the controller is in boot mode. The service port is not capable of carrying 802.1Q tags, so it must be connected to an access port on the neighbor switch. Use of the service port is optional.

Guidelines and Limitations

- The Cisco WiSM2 uses the service port for internal protocol communication between the controllers and the Supervisor 720.
- The service port is not autosensing. You must use the correct straight-through or crossover Ethernet cable to communicate with the service port.
- Do not configure wired clients in the same VLAN or subnet of the service port of the controller on the network. If you configure wired clients on the same subnet or VLAN as the service port, it is not possible to access the management interface of the controller.

Information About Interfaces

An interface is a logical entity on the controller. An interface has multiple parameters associated with it, including an IP address, default gateway (for the IP subnet), primary physical port, secondary physical port, VLAN identifier, and DHCP server.

These five types of interfaces are available on the controller. Four of these are static and are configured at setup time:
- Management interface (static and configured at setup time; mandatory)
- AP-manager interface (static and configured at setup time; mandatory)

Note

You are not required to configure an AP-manager interface on Cisco 5500 Series Controllers.

- Virtual interface (static and configured at setup time; mandatory)
Service-port interface (static and configured at setup time; optional)
Dynamic interface (user-defined)

Each interface is mapped to at least one primary port, and some interfaces (management and dynamic) can be mapped to an optional secondary (or backup) port. If the primary port for an interface fails, the interface automatically moves to the backup port. In addition, multiple interfaces can be mapped to a single controller port.

Guidelines and Limitations

Note
For Cisco 5500 Series Controllers in a non-link-aggregation (non-LAG) configuration, the management interface must be on a different VLAN than any dynamic AP-manager interface. Otherwise, the management interface cannot fail over to the port that the AP-manager is on.

Note
Cisco 5500 Series Controllers do not support fragmented pings on any interface.

Additional References

See the “Configuring Link Aggregation” section on page 4-26 if you want to configure the controller to dynamically map the interfaces to a single port channel rather than having to configure primary and secondary ports for each interface.

Configuring the Management Interface

This section contains the following topics:
- Information About the Management Interface, page 4-4
- Guidelines and Limitations, page 4-5
- Configuring the Management Interface (GUI), page 4-5
- Configuring the Management Interface (CLI), page 4-7

Information About the Management Interface

The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers. It is also used for communications between the controller and access points. The management interface has the only consistently “pingable” in-band interface IP address on the controller. You can access the controller’s GUI by entering the controller’s management interface IP address in Internet Explorer’s or Mozilla Firefox’s address field.

For CAPWAP, the controller requires one management interface to control all inter-controller communications and one AP-manager interface to control all controller-to-access point communications, regardless of the number of ports.
Guidelines and Limitations

- For CAPWAP, the controller requires one management interface to control all inter-controller communications and one AP-manager interface to control all controller-to-access point communications, regardless of the number of ports.
- If the service port is in use, the management interface must be on a different supernet from the service-port interface.
- Do not map a guest WLAN to the management interface. If the EoIP tunnel breaks, the client could obtain an IP and be placed on the management subnet.
- Do not configure wired clients in the same VLAN or subnet of the service port of the controller on the network. If you configure wired clients on the same subnet or VLAN as the service port, it is not possible to access the management interface of the controller.
- Typically, you define the management, AP-manager, virtual, and service-port interface parameters using the Startup Wizard. However, you can display and configure interface parameters through either the GUI or CLI after the controller is running.

Configuring the Management Interface

This section contains the following topics:

- Configuring the Management Interface (GUI), page 4-5
- Configuring the Management Interface (CLI), page 4-7

Configuring the Management Interface (GUI)

Step 1 Choose Controller > Interfaces to open the Interfaces page.

Figure 4-2 Interfaces Page

This page shows the current controller interface settings.

Step 2 Click management link. The Interfaces > Edit page appears.

Step 3 Set the management interface parameters:

Note The management interface uses the controller’s factory-set distribution system MAC address.

- Quarantine and quarantine VLAN ID, if applicable
Note: Select the Quarantine check box if you want to configure this VLAN as unhealthy or you want to configure network access control (NAC) out-of-band integration. Doing so causes the data traffic of any client that is assigned to this VLAN to pass through the controller. See Chapter 8, “Working with WLANs,” for more information about NAC out-of-band integration.

- NAT address (only Cisco 2500 Series Controllers and Cisco 5500 Series Controllers are configured for dynamic AP management)

Note: Select the Enable NAT Address check box and enter the external NAT IP address if you want to be able to deploy your Cisco 2500 Series Controllers or Cisco 5500 Series Controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller’s intranet IP addresses to a corresponding external address. The controller’s dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

Note: The NAT parameters are supported for use only with one-to-one-mapping NAT, where each private client has a direct and fixed mapping to a global address. The NAT parameters do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

Note: If a Cisco 2500 Series Controllers or Cisco 5500 Series Controller is configured with an external NAT IP address under the management interface, the APs in local mode cannot associate with the controller. The workaround is to either ensure that the management interface has a globally valid IP address or ensure that external NAT IP address is valid internally for the local APs.

- VLAN identifier

Note: Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the management interface.

- Fixed IP address, IP netmask, and default gateway
- Dynamic AP management (for Cisco 5500 Series Controllers only)

Note: For Cisco 2500 Series Controllers or Cisco 5500 Series Controllers, the management interface acts like an AP-manager interface by default. If desired, you can disable the management interface as an AP-manager interface and create another dynamic interface as an AP manager.

- Physical port assignment (for all controllers except the Cisco 5500 Series Controller)
- Primary and secondary DHCP servers
### Configuring the Management Interface

**Step 4** Click **Save Configuration** to save your changes.

**Step 5** If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.

### Configuring the Management Interface (CLI)

**Step 1** Enter the `show interface detailed management` command to view the current management interface settings.

**Note** The management interface uses the controller’s factory-set distribution system MAC address.

**Step 2** Enter the `config wlan disable wlan-number` command to disable each WLAN that uses the management interface for distribution system communication.

**Step 3** Enter these commands to define the management interface:

- `config interface address management ip-addr ip-netmask gateway`
- `config interface quarantine vlan management vlan_id`

  **Note** Use the `config interface quarantine vlan management vlan_id` command to configure a quarantine VLAN on the management interface.

- `config interface vlan management {vlan-id | 0}`

  **Note** Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the management interface.

- `config interface ap-manager management {enable | disable}` (for Cisco 5500 Series Controllers only)

  **Note** Use the `config interface ap-manager management {enable | disable}` command to enable or disable dynamic AP management for the management interface. For Cisco 5500 Series Controllers, the management interface acts like an AP-manager interface by default. If desired, you can disable the management interface as an AP-manager interface and create another dynamic interface as an AP manager.

- `config interface port management physical-ds-port-number` (for all controllers except the 5500 series)

- `config interface dhcp management ip-address-of-primary-dhcp-server [ip-address-of-secondary-dhcp-server]`
**Configuring the AP-Manager Interface**

This section contains the following topics:
- Information About the AP-Manager Interface, page 4-8
- Guidelines and Limitations, page 4-9
- Configuring the AP-Manager Interface, page 4-9
- Additional References, page 4-11

**Information About the AP-Manager Interface**

A controller has one or more AP-manager interfaces, which are used for all Layer 3 communications between the controller and lightweight access points after the access points have joined the controller. The AP-manager IP address is used as the tunnel source for CAPWAP packets from the controller to the access point and as the destination for CAPWAP packets from the access point to the controller.
Guidelines and Limitations

- The Controller does not support transmitting the jumbo frames. To avoid having the controller transmit CAPWAP packets to the AP that will necessitate fragmentation and reassembly, reduce MTU/MSS on the client side.
- The AP-manager interface communicates through any distribution system port by listening across the Layer 3 network for access point CAPWAP or LWAPP join messages to associate and communicate with as many lightweight access points as possible.
- For Cisco 5500 Series Controllers, you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default, and the access points can join on this interface.
- With the 7.0.116.0 release onwards, the MAC address of the management interface and the AP-manager interface is the same as the base LAG MAC address.
- If only one distribution system port can be used, you should use distribution system port 1.
- If link aggregation (LAG) is enabled, there can be only one AP-manager interface. But when LAG is disabled, one or more AP-manager interfaces can be created, generally one per physical port.
- Port redundancy for the AP-manager interface is not supported. You cannot map the AP-manager interface to a backup port.
- Typically, you define the management, AP-manager, virtual, and service-port interface parameters using the Startup Wizard. However, you can display and configure interface parameters through either the GUI or CLI after the controller is running.

Configuring the AP-Manager Interface

This section contains the following topics:

- Configuring the AP-Manager Interface (GUI), page 4-9
- Configuring the AP-Manager Interface (CLI), page 4-10

Configuring the AP-Manager Interface (GUI)

Step 1 Choose Controller > Interfaces to open the Interfaces page.

Figure 4-3 Interfaces Page

This page shows the current controller interface settings.

Step 2 Click AP-Manager Interface. The Interface > Edit page appears.

Step 3 Set the AP-Manager Interface parameters:
Configuring the AP-Manager Interface

- Physical port assignment
- VLAN identifier

**Note** Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the AP-manager interface.

- Fixed IP address, IP netmask, and default gateway

**Note** The AP-manager interface’s IP address must be different from the management interface’s IP address and may or may not be on the same subnet as the management interface. However, we recommend that both interfaces be on the same subnet for optimum access point association.

- Primary and secondary DHCP servers
- Access control list (ACL) name, if required

**Note** To create ACLs, follow the instructions in Chapter 7, “Configuring Security Solutions.”

**Step 4** Click **Save Configuration** to save your changes.

**Step 5** If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.

Configuring the AP-Manager Interface (CLI)

**Step 1** Enter the ```show interface summary``` command to view the current interfaces.

**Note** If the system is operating in Layer 2 mode, the AP-manager interface is not listed.

**Step 2** Enter the ```show interface detailed ap-manager``` command to view the current AP-manager interface settings.

**Step 3** Enter the ```config wlan disable wlan-number``` command to disable each WLAN that uses the AP-manager interface for distribution system communication.

**Step 4** Enter these commands to define the AP-manager interface:

- ```config interface address ap-manager ip-addr ip-netmask gateway```  
- ```config interface vlan ap-manager {vlan-id | 0}```  

**Note** Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the AP-manager interface.

- ```config interface port ap-manager physical-ds-port-number```
• config interface dhcp ap-manager ip-address-of-primary-dhcp-server
  [ip-address-of-secondary-dhcp-server]
• config interface acl ap-manager access-control-list-name

Note  See Chapter 7, “Configuring Security Solutions,” for more information on ACLs.

Step 5  Enter the save config command to save your changes.
Step 6  Enter the show interface detailed ap-manager command to verify that your changes have been saved.

Additional References

See the “Configuring Multiple AP-Manager Interfaces” section on page 4-32 for information on creating and using multiple AP-manager interfaces.

Configuring Virtual Interfaces

This section contains the following topics:
• Information About Virtual Interfaces, page 4-11
• Guidelines and Limitations, page 4-11
• Configuring Virtual Interfaces, page 4-12

Information About Virtual Interfaces

A virtual interface is used to support mobility management, Dynamic Host Configuration Protocol (DHCP) relay, and embedded Layer 3 security such as guest web authentication and VPN termination. It also maintains the DNS gateway host name used by Layer 3 security and mobility managers to verify the source of certificates when Layer 3 web authorization is enabled.

Specifically, a virtual interface plays these two primary roles:
• Acts as the DHCP server placeholder for wireless clients that obtain their IP address from a DHCP server.
• Serves as the redirect address for the web authentication login page.


Guidelines and Limitations

• A virtual interface IP address is used only in communications between the controller and wireless clients. It never appears as the source or destination address of a packet that goes out a distribution system port and onto the switched network. For the system to operate correctly, a virtual interface
IP address must be set (it cannot be 0.0.0.0), and no other device on the network can have the same address as the virtual interface. A virtual interface must be configured with an unassigned and unused gateway IP address. A virtual interface IP address is not pingable and should not exist in any routing table in your network. In addition, a virtual interface cannot be mapped to a backup port.

- All controllers within a mobility group must be configured with the same virtual interface IP address. Otherwise, inter-controller roaming may appear to work, but the handoff does not complete, and the client loses connectivity for a period of time.

## Configuring Virtual Interfaces

This section contains the following topics:

- Configuring Virtual Interfaces (GUI), page 4-12
- Configuring Virtual Interfaces (CLI), page 4-13

### Configuring Virtual Interfaces (GUI)

**Step 1** Choose **Controller > Interfaces** to open the Interfaces page.

**Figure 4-4 Interfaces Page**

This page shows the current controller interface settings.

**Step 2** Click Virtual. The Interfaces > Edit page appears.

**Step 3** Enter the following parameters:

- Any fictitious, unassigned, and unused gateway IP address
- DNS gateway hostname

**Note** To ensure connectivity and web authentication, the DNS server should always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then the same DNS host name must be configured on the DNS server(s) used by the client.

**Step 4** Click **Save Configuration** to save your changes.

**Step 5** If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.
Configuring Virtual Interfaces (CLI)

Step 1  Enter the `show interface detailed virtual` command to view the current virtual interface settings.

Step 2  Enter the `config wlan disable wlan-number` command to disable each WLAN that uses the virtual interface for distribution system communication.

Step 3  Enter these commands to define the virtual interface:

- `config interface address virtual ip-address`
  
  **Note**  For `ip-address`, enter any fictitious, unassigned, and unused gateway IP address.

- `config interface hostname virtual dns-host-name`

Step 4  Enter the `reset system` command. At the confirmation prompt, enter `Y` to save your configuration changes to NVRAM. The controller reboots.

Step 5  Enter the `show interface detailed virtual` command to verify that your changes have been saved.

Configuring Service-Port Interfaces

This section contains the following topics:

- Information About Service-Port Interfaces, page 4-13
- Guidelines and Limitations, page 4-13
- Configuring Service-Port Interfaces, page 4-13

Information About Service-Port Interfaces

A service-port interface controls communications through and is statically mapped by the system to the service port. The service port can obtain an IP address using DHCP, or it can be assigned a static IP address, but a default gateway cannot be assigned to the service-port interface. Static routes can be defined through the controller for remote network access to the service port.

Guidelines and Limitations

- Only Cisco 5500 Series Controller and Cisco 7500 Series Controller have service-port interfaces.
- You must configure an IP address on the service-port interface of both Cisco WiSM controllers. Otherwise, the neighbor switch is unable to check the status of each controller.

Configuring Service-Port Interfaces

This section contains the following topics:

- Configuring Service-Port Interfaces (GUI), page 4-14
Configuring Service-Port Interfaces (GUI)

**Step 1** Choose Controller > Interfaces to open the Interfaces page.

**Figure 4-5 Interfaces Page**

This page shows the current controller interface settings.

**Step 2** Click the service-port link to open the Interfaces > Edit page.

**Step 3** Enter the Service-Port Interface parameters:

- **Note** The service-port interface uses the factory-set service-port MAC address of the controller.

- DHCP protocol (enabled)
- DHCP protocol (disabled) and IP address and IP netmask

**Step 4** Click Save Configuration to save your changes.

**Step 5** If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.

Configuring Service-Port Interfaces (CLI)

**Step 1** Enter the `show interface detailed service-port` command to view the current service-port interface settings.

- **Note** The service-port interface uses the controller’s factory-set service-port MAC address.

**Step 2** Enter these commands to define the service-port interface:

- To configure the DHCP server: `config interface dhcp service-port ip-address-of-primary-dhcp-server [ip-address-of-secondary-dhcp-server]
- To disable the DHCP server: config interface dhcp service-port none
- To configure the IP address: `config interface address service-port ip-addr ip-netmask`
Step 3 The service port is used for out-of-band management of the controller. If the management workstation is in a remote subnet, you may need to add a route on the controller in order to manage the controller from that remote workstation. To do so, enter this command:

```
config route add network-ip-addr ip-netmask gateway
```

Step 4 Enter the `save config` command to save your changes.

Step 5 Enter the `show interface detailed service-port` command to verify that your changes have been saved.

---

### Configuring Dynamic Interfaces

This section contains the following topics:

- Information About Dynamic Interfaces, page 4-15
- Guidelines and Limitations, page 4-15
- Configuring Dynamic Interfaces, page 4-16

### Information About Dynamic Interfaces

Dynamic interfaces, also known as VLAN interfaces, are created by users and designed to be analogous to VLANs for wireless LAN clients. A controller can support up to 512 dynamic interfaces (VLANs). Each dynamic interface is individually configured and allows separate communication streams to exist on any or all of a controller’s distribution system ports. Each dynamic interface controls VLANs and other communications between controllers and all other network devices, and each acts as a DHCP relay for wireless clients associated to WLANs mapped to the interface. You can assign dynamic interfaces to distribution system ports, WLANs, the Layer 2 management interface, and the Layer 3 AP-manager interface, and you can map the dynamic interface to a backup port.

You can configure zero, one, or multiple dynamic interfaces on a distribution system port. However, all dynamic interfaces must be on a different VLAN or IP subnet from all other interfaces configured on the port. If the port is untagged, all dynamic interfaces must be on a different IP subnet from any other interface configured on the port.

### Guidelines and Limitations

- If you are using DHCP proxy and/or a RADIUS source interface, ensure that the dynamic interface has a valid routable address. Duplicate or overlapping addresses across controller interfaces are not supported.
- We recommend using tagged VLANs for dynamic interfaces.
- You must not configure a dynamic interface in the same sub-network as a server that should be reachable by the controller CPU, like a RADIUS server, as it might cause asymmetric routing issues.
- For SNMP requests that come from a subnet that is configured as a dynamic interface, the controller responds but the response does not reach the device that initiated the conversation.
- Wired clients cannot access management interface of the Cisco WLC 2500 series using the IP address of the AP Manager interface – when dynamic AP management is enabled on dynamic VLAN.
Configuring Dynamic Interfaces

This section contains the following topics:

- Configuring Dynamic Interfaces (GUI), page 4-16
- Configuring Dynamic Interfaces (CLI), page 4-18

Configuring Dynamic Interfaces (GUI)

**Step 1** Choose **Controller > Interfaces** to open the Interfaces page.

**Figure 4-6 Interfaces > New Page**

**Step 2** Perform one of the following:

- To create a new dynamic interface, click **New**. The Interfaces > New page appears. Go to **Step 3**.
- To modify the settings of an existing dynamic interface, click the name of the interface. The Interfaces > Edit page for that interface appears. Go to **Step 5**.
- To delete an existing dynamic interface, hover your cursor over the blue drop-down arrow for the desired interface and choose **Remove**.

**Step 3** Enter an interface name and a VLAN identifier, as shown in **Figure 4-6**.

**Step 4** Click **Apply** to commit your changes. The Interfaces > Edit page appears.

**Step 5** Configure the following parameters:

- Guest LAN, if applicable
- Quarantine and quarantine VLAN ID, if applicable

**Note** Select the **Quarantine** check box if you want to configure this VLAN as unhealthy or you want to configure network access control (NAC) out-of-band integration. Doing so causes the data traffic of any client that is assigned to this VLAN to pass through the controller. See Chapter 8, “Working with WLANs,” for more information about NAC out-of-band integration.

- Physical port assignment (for all controllers except the 5500 series)
- NAT address (only for Cisco 5500 Series Controllers configured for dynamic AP management)
Select the **Enable NAT Address** check box and enter the external NAT IP address if you want to be able to deploy your Cisco 5500 Series Controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller’s intranet IP addresses to a corresponding external address. The controller’s dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

The NAT parameters are supported for use only with one-to-one-mapping NAT, where each private client has a direct and fixed mapping to a global address. The NAT parameters do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

- Dynamic AP management

When you enable this feature, this dynamic interface is configured as an AP-manager interface (only one AP-manager interface is allowed per physical port). A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

Set the APs in a VLAN that is different than the dynamic interface configured on the controller. If the APs are in the same VLAN as the dynamic interface, the APs are not registered on the controller and the “LWAPP discovery rejected” and “Layer 3 discovery request not received on management VLAN” errors are logged on the controller.

- VLAN identifier
- Fixed IP address, IP netmask, and default gateway
- Primary and secondary DHCP servers
- Access control list (ACL) name, if required

See Chapter 7, “Configuring Security Solutions,” for more information on ACLs.

To ensure proper operation, you must set the Port Number and Primary DHCP Server parameters.

**Step 6**  
Click **Save Configuration** to save your changes.

**Step 7**  
Repeat this procedure for each dynamic interface that you want to create or edit.
Chapter 4 Configuring Ports and Interfaces

Configuring Dynamic Interfaces

When you apply a flow policer or an aggregate policer at the ingress of a Dynamic Interface VLAN for the Upstream (wireless to wired) traffic, it is not possible to police because the VLAN based policy has no effect and no policing occurs. When the traffic comes out of the WiSM LAG (L2) and hits the Switch Virtual Interface (SVI) (L3), the QoS policy applied is a VLAN-based policy that has no effect on the policing.

To enable an ingress L3 VLAN-based policy on the SVI, you must enable a VLAN-based QoS equivalent to the `mls qos-vlan-based` command on the WiSM LAG. All the previous 12.2(33)SXI releases, which support Auto LAG for WiSM only, such as 12.2(33)SXI, 12.2(33)SXI1, 12.2(33)SXI2a, 12.2(33)SXI3, and so on, do not have this WiSM CLI. Therefore, the VLAN-based QoS policy applied at the ingress of the SVI for wireless to wired traffic never polices any traffic coming out of the WiSM LAG that hits the SVI. The commands that are equivalent to the `mls qos-vlan-based` command are as follows:

Standalone: `wism module module_no controller controller_no qos-vlan-based`

Virtual Switching System: `wism switch switch_no module module_no controller controller_no qos-vlan-based`

Configuring Dynamic Interfaces (CLI)

Step 1
Enter the `show interface summary` command to view the current dynamic interfaces.

Step 2
View the details of a specific dynamic interface by entering this command:

`show interface detailed operator_defined_interface_name`.

Note
Interface names that contain spaces must be enclosed in double quotes. For example: `config interface create "vlan 25"`.

Step 3
Enter the `config wlan disable wlan_id` command to disable each WLAN that uses the dynamic interface for distribution system communication.

Step 4
Enter these commands to configure dynamic interfaces:

- `config interface create operator_defined_interface_name {vlan_id | x}`
- `config interface address operator_defined_interface_name ip_addr ip_netmask [gateway]`
- `config interface vlan operator_defined_interface_name {vlan_id | 0}`
- `config interface port operator_defined_interface_name physical_ds_port_number`
- `config interface ap-manager operator_defined_interface_name {enable | disable}`

Note
Use the `config interface ap-manager operator_defined_interface_name {enable | disable}` command to enable or disable dynamic AP management. When you enable this feature, this dynamic interface is configured as an AP-manager interface (only one AP-manager interface is allowed per physical port). A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

- `config interface dhcp operator_defined_interface_name ip_address_of_primary_dhcp_server [ip_address_of_secondary_dhcp_server]`
• `config interface quarantine vlan interface_name vlan_id`

  **Note**  Use the `config interface quarantine vlan interface_name vlan_id` command to configure a quarantine VLAN on any interface.

• `config interface acl operator_defined_interface_name access_control_list_name`

  **Note**  See Chapter 7, “Configuring Security Solutions,” for more information on ACLs.

**Step 5**  Enter these commands if you want to be able to deploy your Cisco 5500 Series Controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT):

  • `config interface nat-address dynamic-interface operator_defined_interface_name { enable | disable }
  • `config interface nat-address dynamic-interface operator_defined_interface_name set public_IP_address`

  NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller’s intranet IP addresses to a corresponding external address. The controller’s dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

  **Note**  These NAT commands can be used only on Cisco 5500 Series Controllers and only if the dynamic interface is configured for dynamic AP management.

  **Note**  These commands are supported for use only with one-to-one-mapping NAT, whereby each private client has a direct and fixed mapping to a global address. These commands do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

**Step 6**  Enter the `config wlan enable wlan_id` command to reenable each WLAN that uses the dynamic interface for distribution system communication.

**Step 7**  Enter the `save config` command to save your changes.

**Step 8**  Enter the `show interface detailed operator_defined_interface_name` command and `show interface summary` command to verify that your changes have been saved.

  **Note**  If desired, you can enter the `config interface delete operator_defined_interface_name` command to delete a dynamic interface.
Information About Dynamic AP Management

A dynamic interface is created as a WLAN interface by default. However, any dynamic interface can be configured as an AP-manager interface, with one AP-manager interface allowed per physical port. A dynamic interface with the Dynamic AP Management option enabled is used as the tunnel source for packets from the controller to the access point and as the destination for CAPWAP packets from the access point to the controller. The dynamic interfaces for AP management must have a unique IP address and are usually configured on the same subnet as the management interface.

**Note**

If link aggregation (LAG) is enabled, there can be only one AP-manager interface.

We recommend having a separate dynamic AP-manager interface per controller port. See the “Configuring Multiple AP-Manager Interfaces” section on page 4-32 for instructions on configuring multiple dynamic AP-manager interfaces.

Information About WLANs

A WLAN associates a service set identifier (SSID) to an interface. It is configured with security, quality of service (QoS), radio policies, and other wireless network parameters. Up to 512 access point WLANs can be configured per controller.

Figure 4-7 shows the relationship between ports, interfaces, and WLANs.
As shown in Figure 4-7, each controller port connection is an 802.1Q trunk and should be configured as such on the neighbor switch. On Cisco switches, the native VLAN of an 802.1Q trunk is an untagged VLAN. If you configure an interface to use the native VLAN on a neighboring Cisco switch, make sure you configure the interface on the controller to be untagged.

**Note**

A zero value for the VLAN identifier (on the Controller > Interfaces page) means that the interface is untagged.

The default (untagged) native VLAN on Cisco switches is VLAN 1. When controller interfaces are configured as tagged (meaning that the VLAN identifier is set to a nonzero value), the VLAN must be allowed on the 802.1Q trunk configuration on the neighbor switch and not be the native untagged VLAN.

We recommend that tagged VLANs be used on the controller. You should also allow only relevant VLANs on the neighbor switch’s 802.1Q trunk connections to controller ports. All other VLANs should be disallowed or pruned in the switch port trunk configuration. This practice is extremely important for optimal performance of the controller.
We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that controllers properly route VLAN traffic.

### Configuring Ports

This section contains the following topics:

- Information About Configuring Ports, page 4-22
- Configuring Ports (GUI), page 4-22

### Information About Configuring Ports

The ports of the controller are preconfigured with factory-default settings designed to make the ports of the controller operational without additional configuration. However, you can view the status of the ports of the controller and edit their configuration parameters at any time.

### Configuring Ports (GUI)

#### Step 1

Choose **Controller > Ports** to open the Ports page.

**Figure 4-8 Ports Page**

This page shows the current configuration for each of the controller’s ports.

If you want to change the settings of any port, click the number for that specific port. The Port > Configure page appears.

**Note**

If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.
Chapter 4  Configuring Ports and Interfaces

Configuring Ports

Note

The number of parameters available on the Port > Configure page depends on your controller type.

The following show the current status of the port:

- Port Number—Number of the current port.
- Admin Status—Current state of the port. Values: Enable or Disable
- Physical Mode—Configuration of the port physical interface. The mode varies by the controller type. Values: Auto, 100 Mbps Full Duplex, 100 Mbps Half Duplex, 10 Mbps Full Duplex, or 10 Mbps Half Duplex

Note

In Cisco Wireless LAN Controller Module (NM-AIR-WLC6-K9), Cisco 5500 Series Controller, and Cisco Flex 7500 Series Controllers, the physical mode is always set to auto.

- Physical Status—The data rate being used by the port. The available data rates vary based on controller type. The following options are available:
  - 5500 series—1000 Mbps full duplex
  - WiSM—1000 Mbps full duplex
  - Controller network module—100 Mbps full duplex
  - Catalyst 3750G Integrated Wireless LAN Controller Switch—1000 Mbps full duplex
- Link Status—Port’s link status. Values: Link Up or Link Down
- Link Trap—Whether the port is set to send a trap when the link status changes. Values: Enable or Disable
- Power over Ethernet (PoE)—If the connecting device is equipped to receive power through the Ethernet cable and if so, provides ~48 VDC. Values: Enable or Disable

Note

Some older Cisco access points do not draw PoE even if it is enabled on the controller port. In such cases, contact the Cisco Technical Assistance Center (TAC).

Note

The controller in the Catalyst 3750G Integrated Wireless LAN Controller Switch supports PoE on all ports.

Step 2

The following is a list of the port’s configurable parameters.

- Admin Status—Enables or disables the flow of traffic through the port. Options: Enable or Disable
  Default: Enable.

Note

Administratively disabling the port on a controller does not affect the port’s link status. The link can be brought down only by other Cisco devices. On other Cisco products, however, administratively disabling a port brings the link down.
Using the Cisco 5500 Series Controller USB Console Port

The USB console port on the Cisco 5500 Series Controllers connects directly to the USB connector of a PC using a USB Type A-to-5-pin mini Type B cable.

**Note** The 4-pin mini Type B connector is easily confused with the 5-pin mini Type B connector. They are not compatible. Only the 5-pin mini Type B connector can be used.

For operation with Microsoft Windows, the Cisco Windows USB console driver must be installed on any PC connected to the console port. With this driver, you can plug and unplug the USB cable into and from the console port without affecting Windows HyperTerminal operations.
**Note** Only one console port can be active at a time. When a cable is plugged into the USB console port, the RJ-45 port becomes inactive. Conversely, when the USB cable is removed from the USB port, the RJ-45 port becomes active.

**USB Console OS Compatibility**

These operating systems are compatible with the USB console:

- Microsoft Windows 2000, XP, Vista (Cisco Windows USB console driver required)
- Apple Mac OS X 10.5.2 (no driver required)
- Linux (no driver required)

**Installing the Cisco Windows USB Console Driver**

**Step 1** Download the USB_Console.inf driver file as follows:

a. Click this URL to go to the Software Center:
   

b. Click **Wireless LAN Controllers**.

c. Click **Standalone Controllers**.

d. Click **Cisco 5500 Series Wireless LAN Controllers**.

e. Click **Cisco 5508 Wireless LAN Controller**.

f. Choose the USB driver file.

g. Save the file to your hard drive.

**Step 2** Connect the Type A connector to a USB port on your PC.

**Step 3** Connect the mini Type B connector to the USB console port on the controller.

**Step 4** When prompted for a driver, browse to the USB_Console.inf file on your PC. Follow the prompts to install the USB driver.

**Note** Some systems might also require an additional system file. You can download the Usbser.sys file from this URL:

http://support.microsoft.com/kb/918365

**Changing the Cisco USB Systems Management Console COM Port to an Unused Port**

The USB driver is mapped to COM port 6. Some terminal emulation programs do not recognize a port higher than COM 4. If necessary, change the Cisco USB systems management console COM port to an unused port of COM 4 or lower.
Choosing Between Link Aggregation and Multiple AP-Manager Interfaces

Cisco 5500 Series Controllers have no restrictions on the number of access points per port, but we recommend using link aggregation (LAG) or multiple AP-manager interfaces on each Gigabit Ethernet port to automatically balance the load.

The following factors should help you decide which method to use if your controller is set for Layer 3 operation:

- With LAG, all of the controller ports need to connect to the same neighbor switch. If the neighbor switch goes down, the controller loses connectivity.
- With multiple AP-manager interfaces, you can connect your ports to different neighbor devices. If one of the neighbor switches goes down, the controller still has connectivity. However, using multiple AP-manager interfaces presents certain challenges (as discussed in the “Configuring Multiple AP-Manager Interfaces” section) when port redundancy is a concern.

Follow the instructions on the page indicated for the method you want to use:

- Configuring Link Aggregation, page 4-26
- Configuring Multiple AP-Manager Interfaces, page 4-32

Configuring Link Aggregation

This section contains the following topics:

- Information About Link Aggregation, page 4-27
- Guidelines and Limitations, page 4-27
- Enabling Link Aggregation, page 4-30
- Verifying Link Aggregation Settings (CLI), page 4-31
- Configuring Neighbor Devices to Support Link Aggregation, page 4-31
Information About Link Aggregation

Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. It bundles all of the controller’s distribution system ports into a single 802.3ad port channel, thereby reducing the number of IP addresses needed to configure the ports on your controller. When LAG is enabled, the system dynamically manages port redundancy and load balances access points transparently to the user.

Figure 4-9 shows LAG.

**Figure 4-9  Link Aggregation**

LAG simplifies controller configuration because you no longer need to configure primary and secondary ports for each interface. If any of the controller ports fail, traffic is automatically migrated to one of the other ports. As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send and receive data.

*Note*
LAG is supported across switches.

Guidelines and Limitations

- You can bundle all eight ports on a Cisco 5508 Controller into a single link.
- Cisco 5500 Series Controllers support LAG in software release 6.0 or later releases, Catalyst 3750G Integrated Wireless LAN Controller Switch. With LAG enabled, the logical port on the Catalyst 3750G Integrated Wireless LAN Controller Switch and on each Cisco WiSM controller supports up to 150 access points.
- Terminating on two different modules within a single Catalyst 6500 series switch provides redundancy and ensures that connectivity between the switch and the controller is maintained when one module fails. Figure 4-10 shows this use of redundant modules. A Cisco 4402-50 Controller is
connected to two different Gigabit modules (slots 2 and 3) within the Catalyst 6500 Series Switch. The controller’s port 1 is connected to Gigabit interface 3/1, and the controller’s port 2 is connected to Gigabit interface 2/1 on the Catalyst 6500 series switch. Both switch ports are assigned to the same channel group.

When a Cisco 5500 Series Controller LAG port is connected to a Catalyst 3750G or a 6500 or 7600 channel group employing load balancing, note the following:

- LAG requires the EtherChannel to be configured for the on mode on both the controller and the Catalyst switch.

- Once the EtherChannel is configured as on at both ends of the link, it does not matter if the Catalyst switch is configured for either Link Aggregation Control Protocol (LACP) or Cisco proprietary Port Aggregation Protocol (PAgP) because no channel negotiation is done between the controller and the switch. Additionally, LACP and PAgP are not supported on the controller.

- The load-balancing method configured on the Catalyst switch must be a load-balancing method that terminates all IP datagram fragments on a single controller port. Not following this recommendation may result in problems with access point association.

- The recommended load-balancing method for Catalyst switches is **src-dst-ip** (enter the `port-channel load-balance src-dst-ip` command).

- The Catalyst 6500 series switches running in PFC3 or PFC3CXL mode implement enhanced EtherChannel load balancing. The enhanced EtherChannel load balancing adds the VLAN number to the hash function, which is incompatible with LAG. From Release 12.2(33)SXH and later releases, Catalyst 6500 IOS software offers the `exclude vlan` keyword to the `port-channel load-balance` command to implement `src-dst-ip` load distribution. See the *Cisco IOS Interface and Hardware Component Command Reference* for more information.

- Enter the `show platform hardware pfc mode` command on the Catalyst 6500 switch to confirm the PFC operating mode.

The following example shows a Catalyst 6500 series switch in PFC3B mode when you enter the global configuration `port-channel load-balance src-dst-ip` command for proper LAG functionality:

```
# show platform hardware pfc mode PFC operating mode
PFC operating mode : PFC3B
# show EtherChannel load-balance
EtherChannel Load-Balancing Configuration:
  src-dst-ip
```

The following example shows Catalyst 6500 series switch in PFC3C mode when you enter the `exclude vlan` keyword in the `port-channel load-balance src-dst-ip exclude vlan` command:

```
# show platform hardware pfc mode
PFC operating mode : PFC3C
# show EtherChannel load-balance
EtherChannel Load-Balancing Configuration:
  src-ip enhanced
  # mpls label-ip
```

- If the recommended load-balancing method cannot be configured on the Catalyst switch, then configure the LAG connection as a single member link or disable LAG on the controller.
You cannot configure the controller’s ports into separate LAG groups. Only one LAG group is supported per controller. Therefore, you can connect a controller in LAG mode to only one neighbor device.

**Note** The two internal Gigabit ports on the controller within the Catalyst 3750G Integrated Wireless LAN Controller Switch are always assigned to the same LAG group.

- When you enable LAG or make any changes to the LAG configuration, you must immediately reboot the controller.
- When you enable LAG, you can configure only one AP-manager interface because only one logical port is needed. LAG removes the requirement for supporting multiple AP-manager interfaces.
- When you enable LAG, all dynamic AP-manager interfaces and untagged interfaces are deleted, and all WLANs are disabled and mapped to the management interface. Also, the management, static AP-manager, and VLAN-tagged dynamic interfaces are moved to the LAG port.
- Multiple untagged interfaces to the same port are not allowed.
- When you enable LAG, you cannot create interfaces with a primary port other than 29.
- When you enable LAG, all ports participate in LAG by default. You must configure LAG for all of the connected ports in the neighbor switch.
- When you enable LAG, if any single link goes down, traffic migrates to the other links.
- When you enable LAG, only one functional physical port is needed for the controller to pass client traffic.
- When you enable LAG, access points remain connected to the switch, and data service for users continues uninterrupted.
- When you enable LAG, you eliminate the need to configure primary and secondary ports for each interface.
When you enable LAG, the controller sends packets out on the same port on which it received them. If a CAPWAP packet from an access point enters the controller on physical port 1, the controller removes the CAPWAP wrapper, processes the packet, and forwards it to the network on physical port 1. This may not be the case if you disable LAG.

When you disable LAG, the management, static AP-manager, and dynamic interfaces are moved to port 1.

When you disable LAG, you must configure primary and secondary ports for all interfaces.

When you disable LAG, you must assign an AP-manager interface to each port on the controller. Otherwise, access points are unable to join.

Cisco 5500 Series Controllers support a single static link aggregation bundle.

LAG is typically configured using the Startup Wizard, but you can enable or disable it at any time through either the GUI or CLI.

**Note**
LAG is enabled by default and is the only option on the Catalyst 3750G Integrated Wireless LAN Controller Switch.

### Enabling Link Aggregation

This section contains the following topics:

- Enabling Link Aggregation (GUI), page 4-30
- Enabling Link Aggregation (CLI), page 4-31

### Enabling Link Aggregation (GUI)

**Step 1**  Choose **Controller > General** to open the General page.

**Figure 4-11  General Page**
Step 2  Set the LAG Mode on Next Reboot parameter to **Enabled**.

**Note**  Choose **Disabled** if you want to disable LAG. LAG is disabled by default on the Cisco 5500 but enabled by default on the Catalyst 3750G Integrated Wireless LAN Controller Switch.

Step 3  Click **Apply** to commit your changes.

Step 4  Click **Save Configuration** to save your changes.

Step 5  Reboot the controller.

Step 6  Assign the WLAN to the appropriate VLAN.

---

### Enabling Link Aggregation (CLI)

**Step 1**  Enter the `config lag enable` command to enable LAG.

**Note**  Enter the `config lag disable` command if you want to disable LAG.

**Step 2**  Enter the `save config` command to save your settings.

**Step 3**  Reboot the controller.

---

### Verifying Link Aggregation Settings (CLI)

To verify your LAG settings, enter this command:

```
show lag summary
```

Information similar to the following appears:

```
LAG Enabled
```

---

### Configuring Neighbor Devices to Support Link Aggregation

The controller’s neighbor devices must also be properly configured to support LAG.

- Each neighbor port to which the controller is connected should be configured as follows:

  ```
  interface GigabitEthernet <interface id>
  switchport
  channel-group <id> mode on
  no shutdown
  ```

- The port channel on the neighbor switch should be configured as follows:

  ```
  interface port-channel <id>
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk native vlan <native vlan id>
  switchport trunk allowed vlan <allowed vlans>
  switchport mode trunk
  no shutdown
  ```
Configuring Multiple AP-Manager Interfaces

This section contains the following topics:

- Information About Multiple AP-Manager Interfaces, page 4-32
- Guidelines and Limitations, page 4-33
- Creating Multiple AP-Manager Interfaces, page 4-35

Information About Multiple AP-Manager Interfaces

When you create two or more AP-manager interfaces, each one is mapped to a different port (see Figure 4-12). The ports should be configured in sequential order so that AP-manager interface 2 is on port 2, AP-manager interface 3 is on port 3, and AP-manager interface 4 is on port 4.

Before an access point joins a controller, it sends out a discovery request. From the discovery response that it receives, the access point can tell the number of AP-manager interfaces on the controller and the number of access points on each AP-manager interface. The access point generally joins the AP-manager with the least number of access points. In this way, the access point load is dynamically distributed across the multiple AP-manager interfaces.

Note

Access points may not be distributed completely evenly across all of the AP-manager interfaces, but a certain level of load balancing occurs.

Figure 4-12  Three AP-Manager Interfaces
This configuration has the advantage of load balancing all 100 access points evenly across all four AP-manager interfaces. If one of the AP-manager interfaces fails, all of the access points connected to the controller would be evenly distributed among the three available AP-manager interfaces. For example, if AP-manager interface 2 fails, the remaining AP-manager interfaces (1, 3, and 4) would each manage approximately 33 access points.

Guidelines and Limitations

- Only Cisco 2500 and 5500 Series Controllers support the use of multiple AP-manager interfaces.
- AP-manager interfaces do not need to be on the same VLAN or IP subnet, and they may or may not be on the same VLAN or IP subnet as the management interface. However, we recommend that you configure all AP-manager interfaces on the same VLAN or IP subnet.
- You must assign an AP-manager interface to each port on the controller.
- Before implementing multiple AP-manager interfaces, you should consider how they would impact your controller’s port redundancy.

Examples:
- The Cisco 4404-100 Controller supports up to 100 access points and has four ports. To support the maximum number of access points, you would need to create three (or more) AP-manager interfaces (see Figure 4-14). If the port of one of the AP-manager interfaces fails, the controller clears the access points’ state, and the access points must reboot to reestablish communication with the controller using the normal controller join process. The controller no longer includes the failed AP-manager interface in the CAPWAP or LWAPP discovery responses. The access points then rejoin the controller and are load balanced among the available AP-manager interfaces.
Figure 4-13  Two AP-Manager Interfaces

Figure 4-14  Four AP-Manager Interfaces
Creating Multiple AP-Manager Interfaces

This section contains the following topics:

- Creating Multiple AP-Manager Interfaces (GUI), page 4-35
- Creating Multiple AP-Manager Interfaces (CLI), page 4-37

Creating Multiple AP-Manager Interfaces (GUI)

**Step 1** Choose **Controller > Interfaces** to open the Interfaces page.

**Step 2** Click **New**. The Interfaces > New page appears.

**Figure 4-15 Interfaces > New Page**

**Step 3** Enter an AP-manager interface name and a VLAN identifier.

**Step 4** Click **Apply** to commit your changes. The Interfaces > Edit page appears.
Step 5 Enter the appropriate interface parameters.

**Note** Do not define a backup port for an AP-manager interface. Port redundancy is not supported for AP-manager interfaces. If the AP-manager interface fails, all of the access points connected to the controller through that interface are evenly distributed among the other configured AP-manager interfaces.

Step 6 To make this interface an AP-manager interface, select the **Enable Dynamic AP Management** check box.

**Note** Only one AP-manager interface is allowed per physical port. A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

Step 7 Click **Save Configuration** to save your settings.

Step 8 Repeat this procedure for each additional AP-manager interface that you want to create.
Creating Multiple AP-Manager Interfaces (CLI)

**Step 1**
Enter these commands to create a new interface:

- `config interface create operator_defined_interface_name {vlan_id \ x}`
- `config interface address operator_defined_interface_name ip_addr ip_netmask [gateway]`
- `config interface vlan operator_defined_interface_name {vlan_id \ 0}`
- `config interface port operator_defined_interface_name physical_ds_port_number`
- `config interface dhcp operator_defined_interface_name ip_address_of_primary_dhcp_server [ip_address_of_secondary_dhcp_server]`
- `config interface quarantine vlan interface_name vlan_id`

**Note** Use this command to configure a quarantine VLAN on any interface.

- `config interface acl operator_defined_interface_name access_control_list_name`

**Note** See Chapter 7, “Configuring Security Solutions,” for more information on ACLs.

**Step 2**
To make this interface an AP-manager interface, enter this command:

`config interface ap-manager operator_defined_interface_name {enable \ disable}`

**Note** Only one AP-manager interface is allowed per physical port. A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

**Step 3**
To save your changes, enter this command:

`save config`

**Step 4**
Repeat this procedure for each additional AP-manager interface that you want to create.

Configuration Example: Configuring AP-Manager on a Cisco 5500 Series Controller

For a Cisco 5500 Series Controller, we recommend having eight dynamic AP-manager interfaces and associating them to the controller’s eight Gigabit ports. If you are using the management interface, which acts like an AP-manager interface by default, you need to create only seven more dynamic AP-manager interfaces and associate them to the remaining seven Gigabit ports. For example, **Figure 4-17** shows a dynamic interface that is enabled as a dynamic AP-manager interface and associated to port number 2, and **Figure 4-18** shows a Cisco 5500 Series Controller with LAG disabled, the management interface used as one dynamic AP-manager interface, and seven additional dynamic AP-manager interfaces, each mapped to a different Gigabit port.
Configuration Example: Configuring AP-Manager on a Cisco 5500 Series Controller

Figure 4-17  Dynamic Interface Example with Dynamic AP Management

Figure 4-18  Cisco 5500 Series Controller Interface Configuration Example
Configuring VLAN Select

This section contains the following topics:

- Information About VLAN Select, page 4-39
- Guidelines and Limitations, page 4-39

Information About VLAN Select

Whenever a wireless client connects to a wireless network (WLAN), the client is placed in a VLAN that is associated with the WLAN. In a large venue such as an auditorium, a stadium, or a conference where there may be numerous wireless clients, having only a single WLAN to accommodate many clients might be a challenge.

The VLAN select feature enables you to use a single WLAN that can support multiple VLANs. Clients can get assigned to one of the configured VLANs. This feature enables you to map a WLAN to a single or multiple interface VLANs using interface groups. Wireless clients that associate to the WLAN get an IP address from a pool of subnets identified by the interfaces. The IP address is derived by an algorithm based on the MAC address of the wireless client. This feature also extends the current AP group architecture where AP groups can override an interface or interface group to which the WLAN is mapped to, with multiple interfaces using the interface groups. This feature also provides the solution to auto anchor restrictions where a wireless guest user on a foreign location can get an IP address from multiple subnets based on their foreign locations or foreign controllers from the same anchor controller.

When a client roams from one controller to another, the foreign controller sends the VLAN information as part of the mobility announce message. Based on the VLAN information received, the anchor decides whether the tunnel should be created between the anchor controller and the foreign controller. If the same VLAN is available on the foreign controller, the client context is completely deleted from the anchor and the foreign controller becomes the new anchor controller for the client.

If an interface (int-1) in a subnet is untagged in one controller (Vlan ID 0) and the interface (int-2) in the same subnet is tagged to another controller (Vlan ID 1), then with the VLAN select, client joining the first controller over this interface may not undergo an L2 roam while it moves to the second controller. Hence, for L2 roaming to happen between two controllers with VLAN select, all the interfaces in the same subnet should be either tagged or untagged.

As part of the VLAN select feature, the mobility announce message carries an additional vendor payload that contains the list of VLAN interfaces in an interface group mapped to a foreign controller’s WLAN. This VLAN list enables the anchor to differentiate from a local to local or local to foreign handoff.

Note

VLAN pooling applies to wireless clients and centrally switched WLANs.

Guidelines and Limitations

- Release 7.0.116.0 and prior releases of the controller software enabled you to associate one VLAN with a WLAN. Each VLAN required a single IP subnet. As a result, a WLAN required a large subnet to accommodate more clients. The VLAN select feature enables you to use a single WLAN that can support multiple VLANs.

- The following lightweight access points are supported: Cisco Aironet 1130, 1040, 1140, 1240, 1250, 1260, 3500, 3600, 1522/1524 Access Points, and 800 Series access points.
• The following controllers are supported: Cisco Flex 7500, Cisco 5508, WiSM-2, 2500 Series Controllers.

### Configuring Interface Groups

This section contains the following topics:

- Information About Interface Groups, page 4-40
- Guidelines and Limitations, page 4-40
- Configuring Interface Groups, page 4-41

### Information About Interface Groups

Interface groups are logical groups of interfaces. Interface groups facilitate user configuration where the same interface group can be configured on multiple WLANs or while overriding a WLAN interface per AP group. An interface group can exclusively contain either quarantine or nonquarantine interfaces. An interface can be part of multiple interface groups.

A WLAN can be associated with an interface or interface group. The interface group name and the interface name cannot be the same.

This feature also enables you to associate a client to specific subnets based on the foreign controller that they are connected to. The anchor controller WLAN can be configured to maintain a mapping between foreign controller MAC and a specific interface or interface group (Foreign maps) as needed. If this mapping is not configured, clients on that foreign controller gets VLANs associated from interface group configured on WLAN.

You can also configure AAA override for interface groups. This feature extends the current access point group and AAA override architecture where access point groups and AAA override can be configured to override the interface group WLAN that the interface is mapped to. This is done with multiple interfaces using interface groups.

This feature enables network administrators to configure guest anchor restrictions where a wireless guest user at a foreign location can obtain an IP address from multiple subnets on the foreign location and controllers from within the same anchor controller.

### Guidelines and Limitations

Table 4-1 lists the platform support for interface and interface groups:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Interface Groups</th>
<th>Interfaces per Interface Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>WiSM2, Cisco 5508 Series Controller, Cisco Flex 7500 Series Controller, Cisco 2500 Series Controller.</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>NM6 series</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>
Configuring Interface Groups

This section contains the following topics:

- Creating Interface Groups (GUI), page 4-41
- Creating Interface Groups (CLI), page 4-41
- Adding Interfaces to Interface Groups (GUI), page 4-41
- Adding Interfaces to Interface Groups (CLI), page 4-42
- Adding an Interface Group to a WLAN (GUI), page 4-42
- Adding an Interface Group to a WLAN (CLI), page 4-42
- Viewing VLANs in Interface Groups (CLI), page 4-42

Creating Interface Groups (GUI)

Step 1
Choose Controller > Interface Groups from the left navigation pane.
The Interface Groups page appears with the list of interface groups already created.

Note
To remove an interface group, hover your mouse pointer over the blue drop-down icon and choose Remove.

Step 2
Click Add Group to add a new group.
The Add New Interface Group page appears.

Step 3
Enter the details of the interface group:

- **Interface Group Name**—Specify the name of the interface group.
- **Description**—Add a brief description of the interface group.

Step 4
Click Add.

Creating Interface Groups (CLI)

- `config interface group {create| delete} interface_group_name`—Creates or deletes an interface group
- `config interface group description interface_group_name "description"`—Adds a description to the interface group

Adding Interfaces to Interface Groups (GUI)

Step 1
Choose Controller > Interface Groups.
The Interface Groups page appears with a list of all interface groups.

Step 2
Click the name of the interface group to which you want to add interfaces.
The Interface Groups > Edit page appears.
Step 3  Choose the interface name that you want to add to this interface group from the Interface Name drop-down list.

Step 4  Click Add Interface to add the interface to the Interface group.

Step 5  Repeat Steps 2 and 3 if you want to add multiple interfaces to this interface group.

**Note**  To remove an interface from the interface group, hover your mouse pointer over the blue drop-down arrow and choose Remove.

### Adding Interfaces to Interface Groups (CLI)

To add interfaces to interface groups, use the `config interface group interface add interface_group interface_name` command.

### Viewing VLANs in Interface Groups (CLI)

To view a list of VLANs in the interface groups, use the `show interface group detailed interface-group-name` command.

### Adding an Interface Group to a WLAN (GUI)

**Step 1**  Choose the WLAN tab.

The WLANs page appears listing the available WLANs.

**Step 2**  Click the WLAN ID of the WLAN to which you want to add the interface group.

**Step 3**  In the General tab, choose the interface group from the Interface/Interface Group (G) drop-down list.

**Step 4**  Click Apply.

### Adding an Interface Group to a WLAN (CLI)

To add an interface group to a WLAN, use the command `config wlan interface wlan_id interface_group_name`.

### Multicast Optimization

This section contains the following topics:

- Information About Multicast Optimization, page 4-43
- Configuring Multicast VLAN, page 4-43
Information About Multicast Optimization

Prior to the 7.0.116.0 release, multicast was based on the grouping of the multicast address and the VLAN as one entity, MGID. With VLAN select and VLAN pooling, there is a possibility that you might increase duplicate packets. With the VLAN select feature, every client listens to the multicast stream on a different VLAN. As a result, the controller creates different MGIDs for each multicast address and VLAN. Therefore, the upstream router sends one copy for each VLAN, which results, in the worst case, in as many copies as there are VLANs in the pool. Since the WLAN is still the same for all clients, multiple copies of the multicast packet are sent over the air. To suppress the duplication of a multicast stream on the wireless medium and between the controller and access points, you can use the multicast optimization feature.

Multicast optimization enables you to create a multicast VLAN which you can use for multicast traffic. You can configure one of the VLANs of the WLAN as a multicast VLAN where multicast groups are registered. Clients are allowed to listen to a multicast stream on the multicast VLAN. The MGID is generated using multicast VLAN and multicast IP addresses. If multiple clients on the VLAN pool of the same WLAN are listening to a single multicast IP address, a single MGID is generated. The controller makes sure that all multicast streams from the clients on this VLAN pool always go out on the multicast VLAN to ensure that the upstream router has one entry for all the VLANs of the VLAN pool. Only one multicast stream hits the VLAN pool even if the clients are on different VLANs. Therefore, the multicast packets that are sent out over the air is just one stream.

Configuring Multicast VLAN

This section contains the following topics:
- Configuring Multicast VLAN (GUI), page 4-43
- Configuring Multicast VLAN (CLI), page 4-43

Configuring Multicast VLAN (GUI)

- **Step 1** Choose the WLANs tab.
  The WLANs tab appears.
- **Step 2** Click on the WLAN ID of the WLAN that you want to choose for a multicast VLAN.
  The WLANs > Edit page appears.
- **Step 3** Enable the multicast VLAN feature by selecting the Multicast VLAN feature check box.
  The Multicast Interface drop-down list appears.
- **Step 4** Choose the VLAN from the Multicast Interface drop-down list.
- **Step 5** Click Apply.

Configuring Multicast VLAN (CLI)

Use the `config wlan multicast interface wlan_id enable interface_name` command to configure the multicast VLAN feature.