Overview of Ports and Interfaces

Three concepts are key to understanding how controllers connect to a wireless network: ports, interfaces, and WLANs.

- Information About Ports, page 1
- Information About Distribution System Ports, page 2
- Information About Interfaces, page 4
- Information About Dynamic AP Management, page 5
- Information About WLANs, page 6

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 1: Ports on the Cisco 5508 Wireless Controllers

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Redundant port (RJ-45)</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Service port (RJ-45)</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>Console port (RJ-45)</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>USB ports 0 and 1 (Type A)</td>
<td>9</td>
</tr>
</tbody>
</table>
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.

Restrictions for Configuring Distribution System Ports

- 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

- GLC-SX-MM, a 1000BASE-SX connector should be in auto-negotiation mode to function as desired because all SFP modules using LC physical connectors must ideally be in auto-negotiation mode on Cisco 5508 Series Controllers to function properly. However, when Cisco ASR is connected using the fiber port, GLC-SX-MM does not come up between Cisco ASR and Cisco 5508 as Cisco ASR requires the connector to be in fixed mode to function properly.

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

Some controllers support link aggregation (LAG), which bundles all of the controller’s distribution system ports into a single 802.3ad port channel. Cisco 5500 Series Controllers support LAG, and LAG is enabled automatically on the controllers within the Cisco WiSM2.

- Cisco WLC configuration in access mode is not supported. We recommend that you configure Cisco WLC in trunk mode when you configure Cisco WLC ports on a switch.

- In Cisco Flex 7500 and 8500 Series Controllers:
  - If a port is unresponsive after a soaking period of 5 seconds, all the interfaces for which the port is the primary and the active port, fail over to the backup port, if a backup is configured and is operational. Similarly, if the unresponsive port is the backup port, then all the interfaces fail over to the primary port if it is operational.
  - After the unresponsive port is restored, there is a soaking period of 60 seconds after which if the port is still operational, then all the interfaces fall back to this port, which was the primary port. If the port was the backup port, then no change is done.
  - You must ensure that you configure the port before you connect a switch or distribution system in the Cisco Wireless LAN Controller 2500 series.

- If an IPv6 packet is destined to controller management IPv6 address and the client VLAN is different from the controller management VLAN, then the IPv6 packet is switched out of the WLC box. If the same IPv6 packet comes as a network packet to the WLC, management access is not denied.

**Information About Service Port**

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.

The service port of the Cisco Wireless Controller 7510 and 8510 models is a one Gigabit Ethernet port. To verify the speed of service port, you must connect the service port to a Gigabit Ethernet port on the switch.

**Note**
The service port is not auto-sensing. You must use the correct straight-through or crossover Ethernet cable to communicate with the service port.

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

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

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.

When LAG is disabled, 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.

In Cisco Wireless LAN Controller 5508 Series, the controller marks packets greater than 1500 bytes as long. However, the packets are not dropped. The workaround to this is to configure the MTU on a switch to less than 1500 bytes.

Interfaces that are quarantined are not displayed on the Controller > Interfaces page. For example, if there are 6 interfaces and one of them is quarantined, the quarantined interface is not displayed and the details of the other 5 interfaces are displayed on the GUI. You can get the total number of interfaces that is inclusive of quarantined interfaces through the count displayed on the top-right corner of the GUI.

Restrictions for Configuring Interfaces

- Each physical port on the wireless controller can have only one AP-manager configured with it. For the Cisco 5500 Series Controllers, the management interface with AP-management enabled cannot fail over to the backup port, which is primary for the AP-manager on the management or dynamic VLAN interface.
• Cisco 5500 Series Controllers do not support fragmented pings on any interface.

• When the port comes up in VMware ESXi with configuration for NIC teaming, the vWLC may lose connectivity. However, the virtual wireless LAN controller (vWLC) resumes connectivity after a while.

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.
Information About WLANs

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

Figure 2: Relationship between Ports, Interfaces, and WLANs

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.

---

**Note**

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.