Overview of Ports and Interfaces

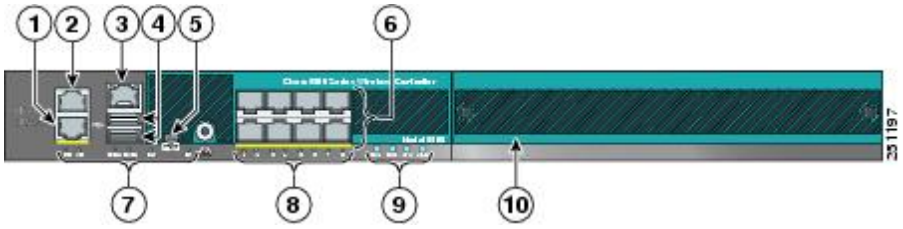
Three concepts are key to understanding how controllers connect to a wireless network: ports, interfaces, and WLANs.

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
- Service port

Figure 1: Ports on the Cisco 5508 Wireless Controllers



1	Redundant port (RJ-45)	6	SFP distribution system ports 1–8
2	Service port (RJ-45)	7	Management port LEDs
3	Console port (RJ-45)	8	SFP distribution port Link and Activity LEDs

4	USB ports 0 and 1 (Type A)	9	Power supply (PS1 and PS2), System (SYS), and Alarm (ALM) LEDs
5	Console port (Mini USB Type B) **Note** You can use only one console port (either RJ-45 or mini USB). When you connect to one console port, the other is disabled.	10	Expansion module slot

For more information about Cisco Unified Wireless Network Protocol and Port Matrix, see http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/113344-cuwn-ppm.html.

Note For a comparison of ports in different controllers, see https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html.

This section contains the following subsections:

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

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

  Note Some controllers support link aggregation (LAG), which bundles all of the controller's distribution system ports into a single 802.3ad port channel. Cisco 5508 WLCs support LAG, and LAG is enabled automatically on the controllers within the Cisco WiSM2.

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

- 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.

Service Port

The service port can be used management purposes, primarily for out-of-band management. However, AP management traffic is not possible across the service port. In most cases, the service port is used as a "last resort" means of accessing the controller GUI for management purposes. For example, in the case where the system distribution ports on the controller are down or their communication to the wired network is otherwise degraded.

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.

Service ports are not intended for high volume of traffic. We recommend that you use the management interface through the system distribution ports (dedicated or LAG).

Service ports can be used for SNMP polling in Release 8.2 or a later release.

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. We recommend that you place the service port in a VLAN or a subnet that is dedicated to out-of-band management.

Note For Cisco 5520 and 8540 Wireless Controllers, the disabling of administrative mode of the port does not physically disable the port. Only the packets are blocked due to which switchover does not happen.

For information about service ports in the applicable controllers, see the respecitve controller documentation:

- Cisco 3504 WLC Deployment Guide
- Cisco 5508 WLC Installation Guide
- Cisco WiSM2 Deployment Guide
- Cisco Flex 7510 WLC Deployment Guide
- Cisco 5520 WLC Deployment Guide
- Cisco 8510 WLC Installation Guide
- Cisco 8540 WLC Deployment Guide

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:

Note A interface that is static means that at least one must exist in the controller and cannot be deleted. However, you can choose to modify the parameters for these interfaces after the initial setup.

- 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 5508 and later controller models explicitly because this function can be enabled by default on the management interface itself.

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

Note 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.

The Cisco 5508 and later controller models mark packets greater than 1500 bytes as long. However, the packets are not dropped. The workaround for this is to configure the MTU on a switch to less than 1500 bytes.

Note 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.

This section contains the following subsections:

Restrictions on Configuring Interfaces

- Each physical port on the wireless controller can have only one AP-manager configured with it. For the Cisco 5508 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 5508 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 Cisco vWLC resumes connectivity after a while.
- IPv4 address needs to be configured on the interface prior to configuring the IPv6 address.

Dynamic AP Management

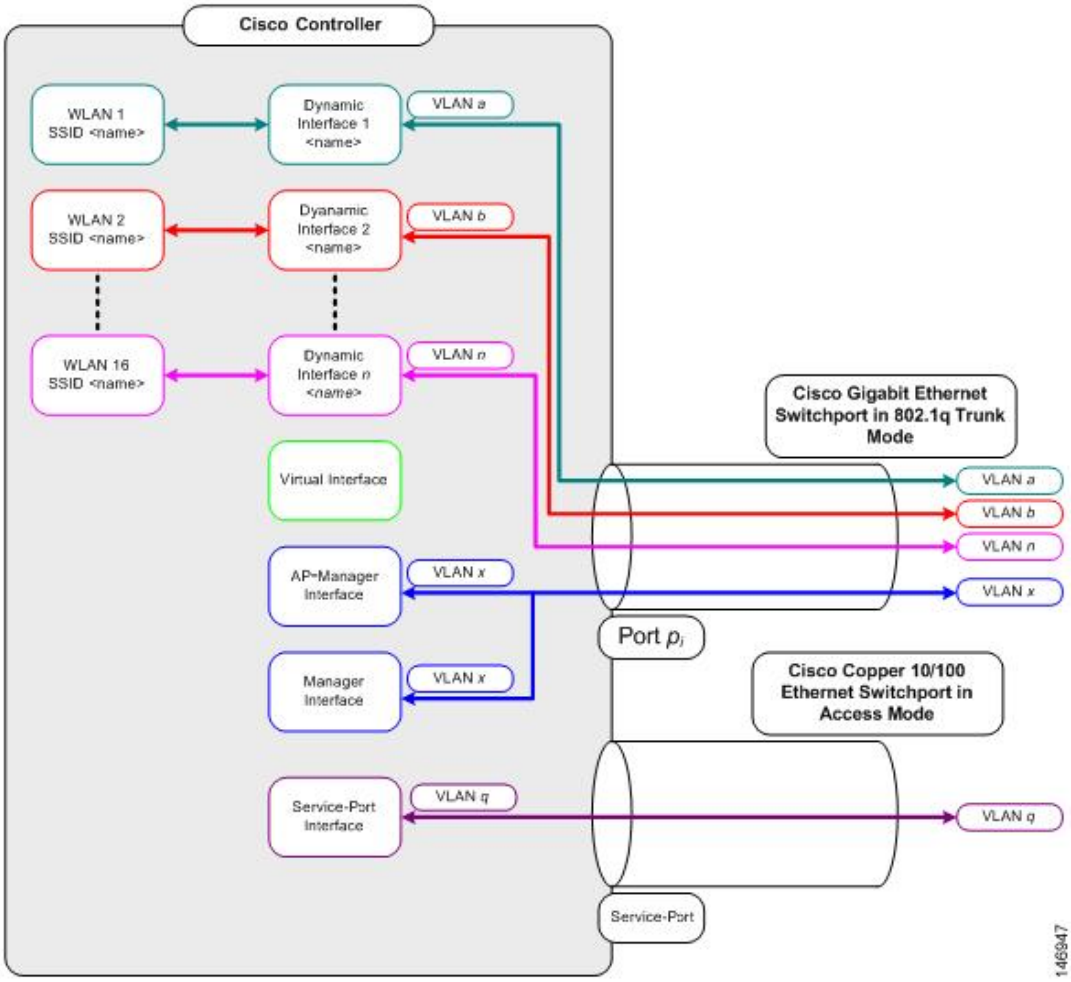
A dynamic interface is created as a WLAN interface by default. However, any dynamic interface can be configured as an AP-manager interface, with one AP-manager interface allowed per physical port. A dynamic interface with the Dynamic AP Management option enabled is used as the tunnel source for packets from the controller to the access point and as the destination for CAPWAP packets from the access point to the controller.

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

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.