Supported Features

The CT5760 WLC is an industry-leading platform designed for 802.11ac performance with maximum services, scalability, and high resiliency for mission-critical wireless networks. Through enhanced software programmable ASIC, it delivers a wide range of features highlighted in Table 2-1.

Table 2-1 Cisco 5760 WLC Features

Feature	Benefits
Scalability	• Supports up to 1000 APs and 12,000 wireless clients for business- critical wireless services. • Unparalleled scalable wireless solution, which comprises multiple controllers, can support up to 72,000 APs and 864,000 wireless clients.
High Performance	• Optimized for 802.11ac standard. • Six 10G Cisco SFP+ (Small Form-Factor Pluggable) uplinks. • Hardware assisted processing to provide up to 60 Gbps throughput with services such as a downloadable access control list (ACL), granular quality of service (QoS) queues, fairness algorithm, NetFlow v9 processing, and so on.
High Resiliency	• Converged Access deployment mode provides hierarchical network design that constraints failure to smaller domains. Thereby it provides higher resiliency. Wireless clients recover quickly from switch failures within the Catalyst 3850 and the 5760 Controller stack automatically through stateful switchover (AP SSO). • CT5760 in centralized deployment mode (also known as local mode) supports 1+1, N+1 resiliency, and AP SSO. • Multiple link aggregation (LAG) support to protect against link failures, while optimal network connectivity is maintained.
Cisco IOS® Software-based Controller	• Proven and security-hardened Cisco IOS® operating system. • Well-known Cisco IOS® software CLI allows customers to leverage current management tools for operations. • Cisco's rich NetFlow eco-system enables customers to report on, monitor, analyze traffic on, and troubleshoot the wireless network.
ClientLink 2.0	• Cisco ClientLink 2.0 technology improves downlink performance to all mobile devices including one, two, and three-spatial-stream devices on 802.11n and improves battery life on mobile devices such as smartphones and tablets.

Table 2-1 Cisco 5760 WLC Features

CleanAir	• Cisco CleanAir™ technology provides proactive, high-speed spectrum intelligence to combat performance problems due to wireless interference.
Radio Frequency (RF) Management	• Provides both real-time and historical information about RF interference that impacts network performance across controllers via system-wide Cisco CleanAir™ technology integration.
Comprehensive End-to-End Security	• Offers CAPWAP compliant Datagram Transport layer Security (DTLS) encryption to ensure encryption between access points and controllers or between controllers.
High Performance Video	• Optimized video delivery via single stream for both wired and wireless clients. • Supports Cisco VideoStream technology to optimize the delivery of business-critical multicast video applications across the WLAN.
End-to-end Voice	• Supports Unified Communications for improved collaboration through messages, presence, and conferences. • Supports all Cisco Unified Communications Wireless IP Phones for cost-effective, real-time voice services.
Advanced QoS	• Consistent configuration CLI for both wired and wireless QoS through Modular QoS CLI. • Granular QoS policies per access point (AP), service set identifier (SSID), radio, and client. • Fair bandwidth allocation across wireless clients on an AP. • Leverages Cisco's proven Cisco IOS® software and ASIC technology to provide line-rate performance.
Advanced ACL	• Simplifies and centralizes security policies through downloadable ACLs. • ACLs are processed in hardware to provide line-rate performance.
Flexible Netflow v9	• Network-wide visibility with Flexible Netflow for wireless clients.
Environmentally Responsible	• Organizations may choose to turn off AP radios to reduce power consumption during off peak hours. • Integrated WLC avoids the deployment of an additional device in the network.

Table 2-1 Cisco 5760 WLC Features

Mobility and Security	• Secure, reliable wireless connectivity and consistent end-user experience. • Increased network availability through proactive blocking of known threats.
IPv6	• Supports IPv6 addressing on interfaces with appropriate show commands for monitoring and troubleshooting. • IPv6 ACLs are processed in hardware to provide line-rate performance.

For a complete list of features and specifications, refer to the Cisco 5760 Series Wireless Controller page and Data Sheet.

Cisco Controllers Comparisons

This table shows the Cisco high-scale controllers comparison at a glance:

Table 2-2 Cisco Controllers Comparison

	85002	7500	5500	WiSM	5760
Deployment Type	Enterprise Large campus + SP Wi-Fi	Central site controller for large number of distributed, controller-less branches	Enterprise Campus and full-service branch	Enterprise campus	Large campus
Operational Modes	Local mode, FlexConnect Mesh	FlexConnect only	Local mode, FlexConnect Mesh	Local mode, FlexConnect Mesh	Centralized (local mode) or Converged Access mode
Maximum Scale	6000 APs 64,000 clients	6000 APs 64,000 clients	500 APs 7000 clients	1000 APs 15,000 clients	1000 APs 12,000 clients
AP Count Range	300-6k APs	300-6k APs	12-500 APs	100-1000 APs	1-1000 APs

Table 2-2 Cisco Controllers Comparison

Licenses	Right to Use (with EULA)	Right to Use (with EULA)	CISL based (unchanged)	CISL based (unchanged)	Right to Use (with EULA)
Connectivity	2x10G ports	2x10G ports	8x1G ports	Internal connections the Catalyst Backplanes	6x10G ports
Power	AC/DC dual redundant	AC dual redundant	AC (redundant PSU option)	AC/DC Catalyst chassis (redundant PSU option)	AC (redundant PSU option)
Maximum Number of FlexConnect Groups	2000	2000	100	100	N/A
Maximum Number of APs per FlexConnect Group	100	100	25	25	N/A
Maximum Number of Rogue APs Management	24,000	24,000	2000	4000	4000
Maximum Number of Rogue Clients Management	32,000	32,000	2500	5000	5000
Maximum Number of RFID	50,000	50,000	5000	10,000	10,000
Maximum APs per RRM Group	6000	6000	1000	2000	2000
Maximum AP Groups	6000	6000	500	500	1000
Maximum Interface Groups	512	512	64	64	64

Table 2-2 Cisco Controllers Comparison

Maximum Interfaces per Interface Group	64	64	64	64	64
Maximum VLANs Supported	4095	4095	512	512	4096
Maximum WLANs Supported	512	512	512	512	512
Supported Fast Secure Roaming (FSR)	64,000	64,000	14,000	30,000	24,000

New Operating System using Cisco IOS® Software CLI Commands

The CT5760 controllers use the same Cisco IOS® software CLI command used on the Cisco switches and routers. New wireless CLI commands have been added to the existing Cisco IOS® CLI. For a complete list of the wireless Cisco IOS® software CLI commands, refer to the Cisco 5700 Series Wireless LAN Controllers Command References document.

Licenses

Licenses are based on the Right-To-Use license model (per AP license price for the Catalyst 3850 and CT5760). AP licenses are enabled on the mobility controller. The mobility controller can be a Catalyst 3850 switch (or switches), CT5760, 5500, or WiSM2. There is not a separate license for mobility agent functionality (for example, CAPWAP termination on the switch). The same AP licenses can be used as before when the 5500/WiSM2 is used as mobility controller. AP licenses are transferable between Catalyst 3850 and CT5760, Catalyst 3850 and Catalyst 3850, and CT5760 and CT5760.

Please refer to the Cisco Right to Use Licensing FAQ for additional information.

Software Release Numbers

The first 5760 release is Cisco IOS XE 3.2.0SE.

Supported Platforms

Controllers

- Converged access mode: CT5760, CT5508, WS-SVC-WISM2, 3850
- Centralized mode: CT5760, WISM2, CT5508

APs

- 1040, 1140, 1260, 1600, 2600, 3500, 3600, 3700

Cisco Prime 2.0 (Future Release-May2013)

- Appliance and Virtual Instance

Mobility Services Engine (MSE)

- MSE 7.4 on 3300 and Virtual Instance

Identity Service Engine (ISE)

- ISE 1.1.1 on 3315, 3355, 3395 and Virtual Instance

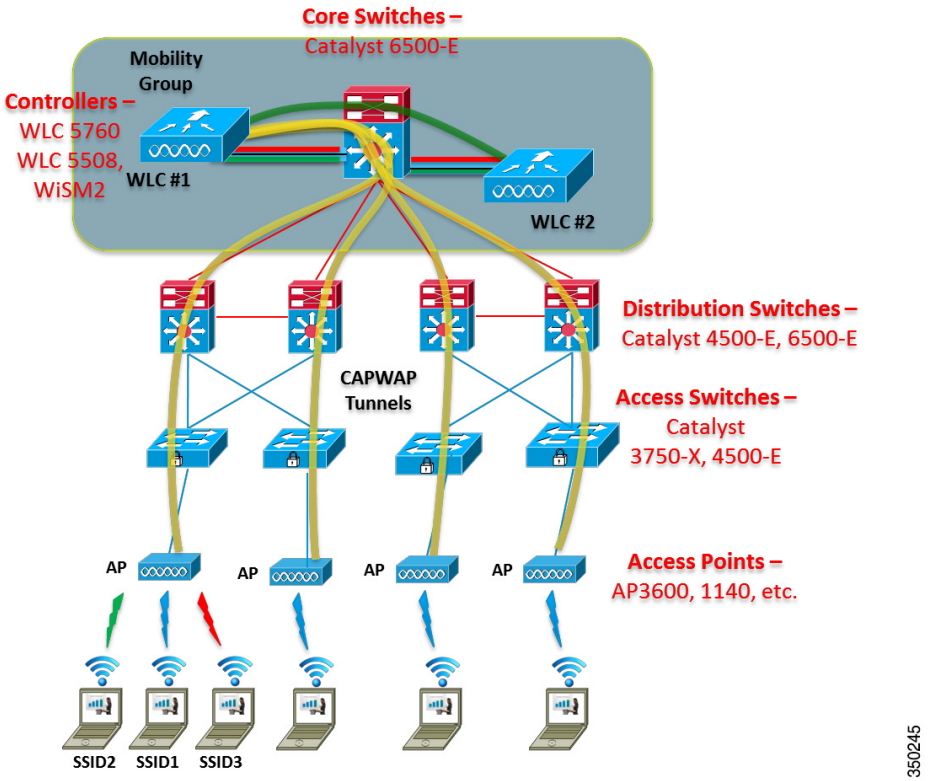
Unified Access Deployment Modes

With the introduction of the CT5760 and Catalyst 3850, there are two deployment modes within the Cisco Unified Access Architecture - Centralized and Converged Access.

Centralized Mode

The centralized mode (also known as local mode on legacy controllers) is the same deployment model currently used today in the Cisco Unified Wireless Network (CUWN) solution set for wireless as well as wired connectivity. The current CUWN provides centralized tunneling of user traffic to the controller (data plane and control plane) and system-wide coordination for channel and power assignment, rogue detection, security attacks, interference, roaming, and so on.

Figure 2-1 Centralized Mode

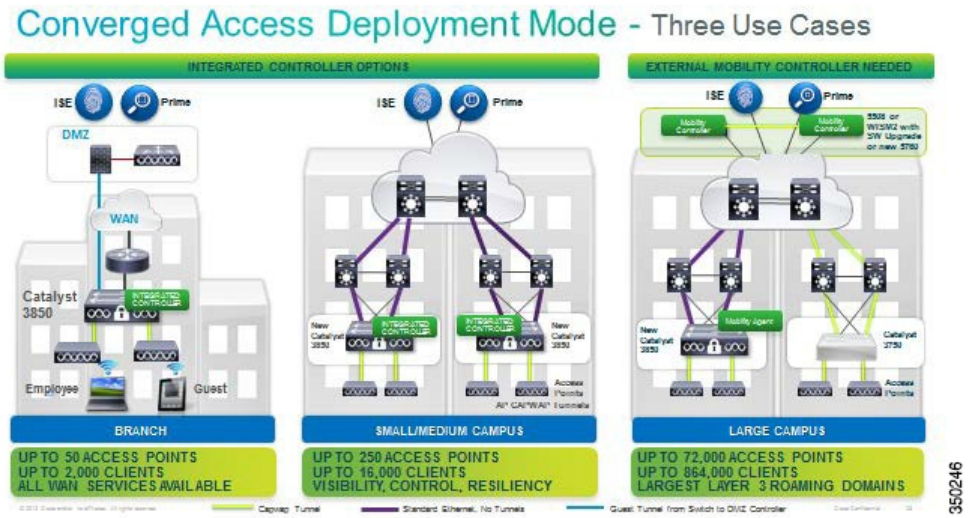


Converged Access Mode

Converged mode is an evolution of the current wireless deployments and offers an additional deployment mode for mobility. With the converged access model, there are a few design differences to note:

- The Catalyst 3850 can act as a mobility agent for terminating CAPWAP tunnels for locally connected APs.
- The Catalyst 3850 can act as a Mobility Controller (MC) for other mobility agent switches in small deployments.
- MC handles roaming across a switch peer group (SPG) (L2 / L3).
- Mobility agents within an SPG are fully meshed (auto-created at SPG formation).

Figure 2-2 Converged Access Deployment Mode

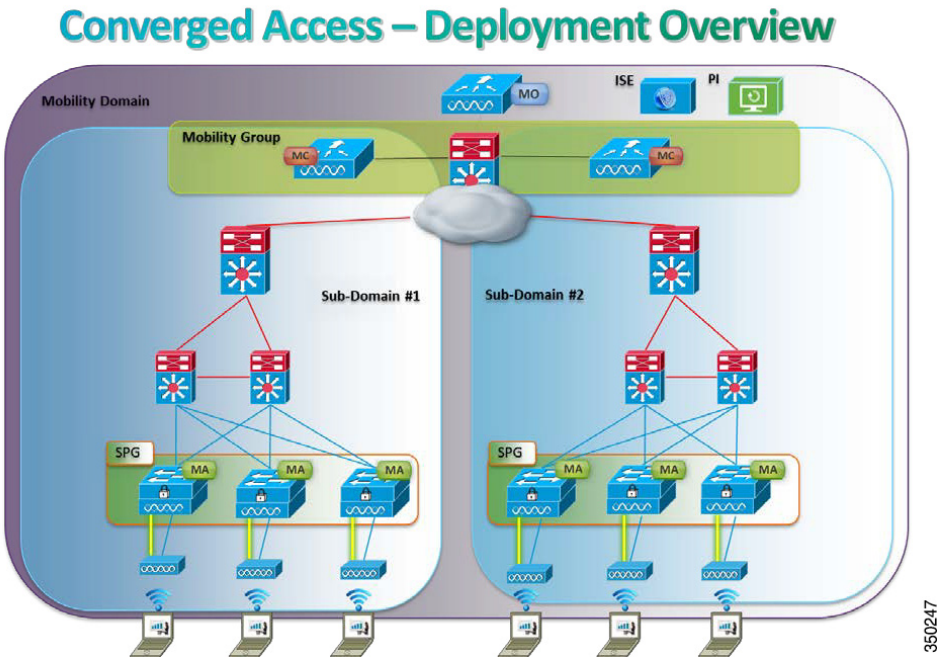


Converged Access Components

A few components are highlighted in order to understand the Converged Access model. These components are shown in Figure 2-3.

1. **Physical Entities:**
   - Mobility Agent – Terminates CAPWAP tunnel from AP and handles the local client database.
   - Mobility Controller – Manages mobility within and across sub-domains, RRM, CleanAir and roaming.
   - Mobility Oracle – Superset of mobility controller, allows for scalable mobility management within a domain.
2. **Logical Entities:**
   - Mobility Groups – The grouping of mobility controllers to enable fast and secure roaming.
   - Switch Peer Group – Localizes traffic for roams within its distribution block.

Figure 2-3 Converged Access - Deployment Overview



This deployment guide focuses on the configuration of the new CT5760 feature set with the Cisco IOS® software. For detailed information on the new Catalyst 3850 wired/wireless switch and its deployment scenarios, refer to the Catalyst 3850 Deployment/Configuration Guides page.

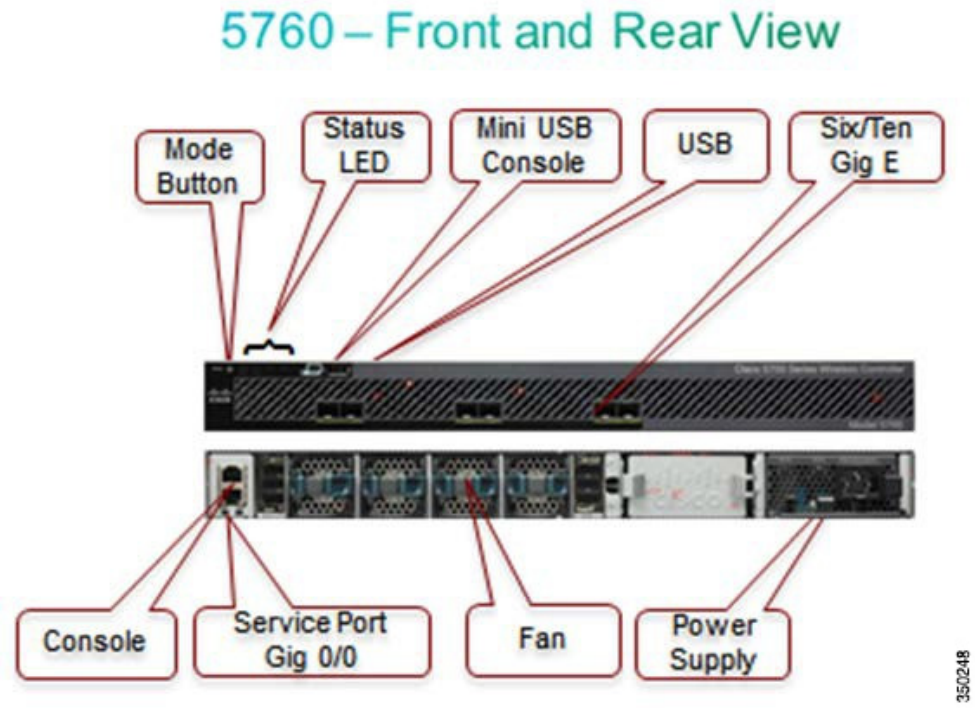
Deployment Basics: Ports, Interfaces, WLAN

This section covers information about the CT5760 ports, interfaces, and WLANs.

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. The ports available on the CT5760 controller are shown in Figure 2-4

Figure 2-4 CT5760 Controller - Front and Rear View



Management Port (Service Port) (RJ-45)

The Cisco 5760 Series Controllers have a 10/100/1000 copper Ethernet Management port (GE 0/0). The management port is reserved for out-of-band management of the controller, system recovery, and maintenance in the event of a network failure.

Console Ports (RJ-45) and Mini USB Type B port

The CT5760 WLC has two console ports: the RJ45 and Mini USB Type B port.

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.

USB Ports 0 (Type A):

The USB console port on the Cisco 5760 Series Controllers connects directly to the USB connector of a PC using a USB Type A-to-5-pin mini Type B cable.

SFP Distribution System Ports 1-6:

The Cisco 5760 Controllers have six 10 Gigabit Ethernet (GE) distribution system ports, through which the controller can manage multiple APs. Cisco 5760 controllers support a maximum of 1000 APs and have no restrictions on the number of APs per port. However, Cisco recommends using link aggregation (LAG) or EtherChannel to balance the load automatically. LAG is covered in another section in this document. The part numbers for the supported SFPs on the 10GE ports are listed in Table 2-3.

Table 2-3 Part Numbers for Supported SFPs on the 10GE

SFP+/SFP (only Cisco SFPs supported)	• SFP-10G-ER, • SFP-10G-LR, • SFP-10G-SR, • SFP-10G-LRM, • SFP-H10GB-CU1M • SFP-H10GB-CU3M • SFP-H10GB-CU5M • GLC-BX-D, • GLC-BX-U, • GLC-SX-MM, • GLC-SX-MMD, • GLC-T, • GLC-LH-SM, • GLC-ZX-SM, • CWDM-SFP, • DWDM-SFP, • SFP-GE-L, • SFP-GE-S, • GLC-LH-SMD, • GLC-EX-SMD, • GLC-GE-100FX

Information about Interfaces

An interface is a logical entity on the controller. The next-generation controllers contain multiple interfaces, but these interfaces should be configured:

1. Wireless management interface (can be configured at setup time; mandatory)

   The wireless management interface is used for AP to controller discovery, mobility and Radio Resource Management (RRM). This interface is also used for in-band management: Telnet/SSH CLI, SNMP, and WebGUI.

2. VLANs, which are considered dynamic interfaces, where WLAN traffic is mapped to them.

Information about WLANs

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

WLANs are directly mapped to VLANs, which are mapped to physical interfaces.

Note Cisco recommends 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.

AP Join Controller Discovery Process

In a CAPWAP environment, a lightweight AP discovers a controller by using CAPWAP discovery mechanisms and then sends the controller a CAPWAP join request. The controller sends the AP a CAPWAP join response, allowing the AP to join the controller. When the AP joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

APs must be discovered by a controller before they can become an active part of the network. The lightweight APs support the following controller discovery process:

- Layer 3 CAPWAP discovery: This feature can be enabled on different subnets from the AP and uses IP addresses and UDP packets rather the MAC addresses used by Layer 2 discovery.
- Locally stored controller IP address discovery: If the AP was previously associated to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the AP's nonvolatile memory. This process of storing controller IP addresses on an AP for later deployment is known as priming the AP.
- DHCP server discovery: This feature uses DHCP option 43 to provide controller IP addresses to the APs. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, refer to the Configuring DHCP Option 43 for Lightweight Access Points document.
- DNS discovery: The AP can discover controllers through your DNS. In order for the AP to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the AP domain name. When an AP receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain or CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the AP sends discovery requests to the controllers.

Link Aggregation/Load Balancing/Port Redundancy

The Cisco 5760 WLC has no restrictions on the number of APs per port, but Cisco recommends using LAG or EtherChannel on each 10GE port to automatically balance the load.

LAG functionality is achieved for a CT5760 controller through configuration of EtherChannels in the Cisco IOS® software. Through EtherChannels, the controller dynamically manages port redundancy and load balances APs transparently to the user.

Information about Link Aggregation

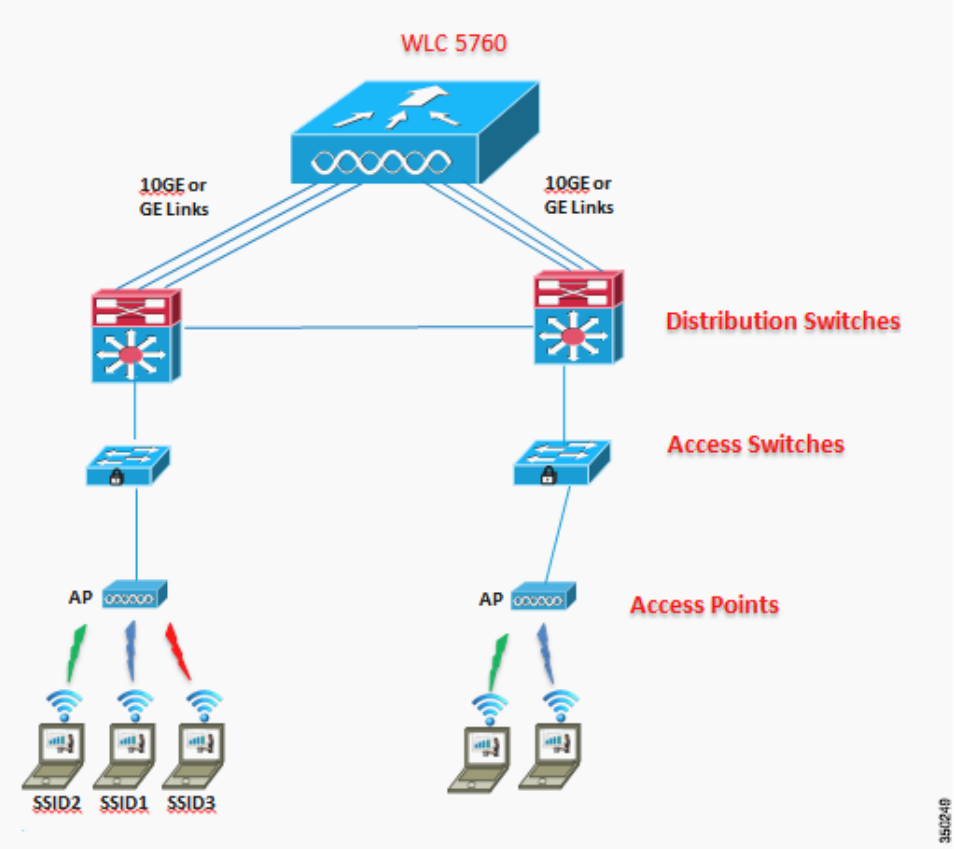
Link Aggregation (LAG) or Etherchannel can be configured on the 5760 Controller. It bundles all of the controller's distribution system ports into a single port channel. The Cisco 5760 Controller supports Cisco Port Aggregation Protocol (PAgP) and industry-standard IEEE 802.3ad Link Aggregation Control Protocol (LACP). When LAG is enabled, the system dynamically manages port redundancy and load balances APs transparently to the user.

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, APs remain connected to the network, and wireless clients continue to send and receive data.

Multiple LAGs

Multiple LAG groups can be configured to support configurations requiring connectivity to multiple switches for redundancy. APs are load balanced across multiple LAG groups by configuring an AP manager for each LAG group.

Figure 2-5 Multiple LAGs



Configure the Controller and Neighbor Devices to Support LAG

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

- Each neighbor port to which the controller is connected should be configured with these commands:

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

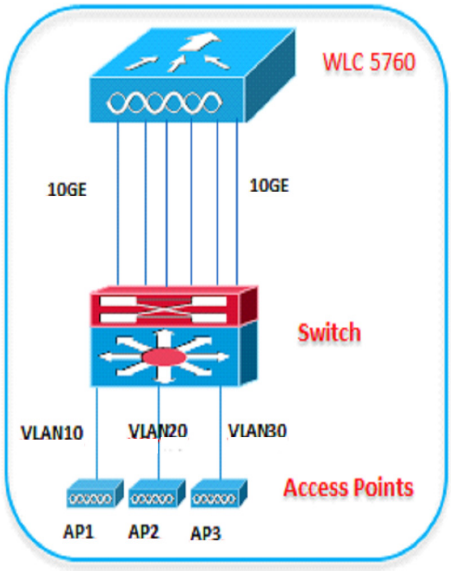
- The port channel on the neighbor switch should be configured with these commands:

```
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
```

With the introduction of Cisco IOS® software on the WLC5760, LAG configuration is similar to the neighboring switch configuration.

Load Balancing with AP Manager Configuration Example

Note Load balancing that uses multiple AP manager interfaces is supported on the CT5760 WLAN controller similar to the AireOs controller. However, Cisco recommends using LAG for redundancy and load balancing. Please check the example below for AP Manager configuration example:



You can configure up to 5 AP-manager interfaces on the controller along with one wireless management interface.

5760 Config Example

```
WLC5760(config)#wireless management interface vlan 10
WLC5760(config)#wireless ap-manager interface vlan 20
WLC5760(config)#wireless ap-manager interface vlan 30
```

5760 Interfaces Config:

```
WLC5760(config)#interface tenGigabitEthernet 1/0/1
WLC5760(config-if)#switchport mode trunk
WLC5760(config-if)#switchport trunk allowed vlan 10

WLC5760(config)#interface tenGigabitEthernet 1/0/2
WLC5760(config-if)#switchport mode trunk
WLC5760(config-if)#switchport trunk allowed vlan 20

WLC5760(config)#interface tenGigabitEthernet 1/0/3
WLC5760(config-if)#switchport mode trunk
WLC5760(config-if)#switchport trunk allowed vlan 30
```