CT5760 Controller Deployment Guide

Cisco Next Generation WLAN Controller
April 04, 2013

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

CONTENTS

Preface

Revised: January 24, 2014,

This section discusses the objectives, audience, conventions, and organization of the *CT5760 Controller Deployment Guide* and provides general information about Cisco IOS software documentation.

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription.

Objectives

This document introduces two new controllers within the Cisco Unified Access architecture and provides general guidelines for their deployment. The purpose of this document is to:

- Provide an overview of the new Cisco 5760 Next Generation Wireless LAN Controller and the Next Generation Catalyst 3850 Wired/Wireless Switch.

- Provide design recommendations and deployment considerations specific to the Centralized Access deployment.

Audience

This publication is intended primarily for users who configure and maintain routers, but are not necessarily familiar with tasks, the relationship between tasks, or the commands necessary to perform particular tasks to configure VoIP. In addition, this publication is intended for users with some familiarity with IP and telephony networks.

Cisco IOS Software Documentation

In addition to the information provided in this publication, you might need to refer to the Cisco IOS documentation set. The Cisco IOS software documentation is divided into nine modules and two master indexes. Each module consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Each configuration guide can be used in conjunction with its corresponding command reference.

Organization

This chapter describes the contents of each chapter in this document.

Table 1   Organization

Chapter	Title	Description
Chapter 1	Product Overview	Overview of controllers
Chapter 2	Supported Features	Overview of supported features
Chapter 3	Mobility Architecture	Overview of mobility components in the new mobility architecture
Chapter 4	Mobility Design and Configuration	Configuration of WLC5760, WLC5508, and Catalyst 3850 in hybrid mode
Chapter 5	Bring Your Own Device (BYOD) Security Configuration	Description of self-service additions of personal devices
Chapter 6	Secure WLAN configuration	Configuration on Catalyst 3850/WLC5508
Chapter 7	Radio Resource Management Configuration	Radio Resource Management (RRM) software
Chapter 8	CleanAir	CleanAir - spectrum intelligence solution
Chapter 9	High Availability	Overview of availability
Chapter 10	Interface Group	Overview of groups of interfaces
Chapter 11	Multicast Configuration	Overview of multicast configuration
Chapter 12	QoS Configuration	Introduction of Cisco IOS® software on the WLC5760 controller

Command Syntax Conventions

Table 2 describes the syntax used with the commands in this document.

Table 2   ***Command Syntax Guide***

Convention	Description
boldface	Commands and keywords.
italic	Command input that is supplied by you.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. You must select one.
^ or Ctrl	Represent the key labeled *Control*. For example, when you read **^***D* or *Ctrl-D*, you should hold down the Control key while you press the D key.
`screen font`	Examples of information displayed on the screen.
boldface screen font	Examples of information that you must enter.
< >	Nonprinting characters, such as passwords, appear in angled brackets.
[ ]	Default responses to system prompts appear in square brackets.

Product Overview

This section provides an overview of the two new controllers:

Unified Access CT5760 Wireless Controller

The CT5760 Wireless LAN Controller (WLC) is the first Cisco IOS® software-based controller built with Cisco's innovative UADP ASIC intended to be deployed as a centralized controller in the next generation unified wireless architecture. CT5760 controllers are specifically designed to function like the older unified model central wireless controllers. They also support the newer Mobility functionality with Next Generation Wireless Controllers 3850 switches in the wireless architecture.

CT5760 controllers are deployed behind a core switch/router. The core switch/router is the only gateway into the network for the controller. The uplink ports connected to the core switch are configured as EtherChannel trunk to ensure port redundancy.

This new controller is an extensible and high performance wireless controller, which can scale up to 1000 access points (AP) and 12,000 clients. The controller has 6x10 Gbps data ports.

As a component of the Cisco Unified Wireless Network, the 5760 series works in conjunction with Cisco Aironet Access Points, the Cisco Prime Infrastructure, and the Cisco Mobility Services Engine to support business-critical wireless data, voice, and video applications. See Figure 1-1 for the WLC5760 overview.

Figure 1-1   WLC5760 Overview
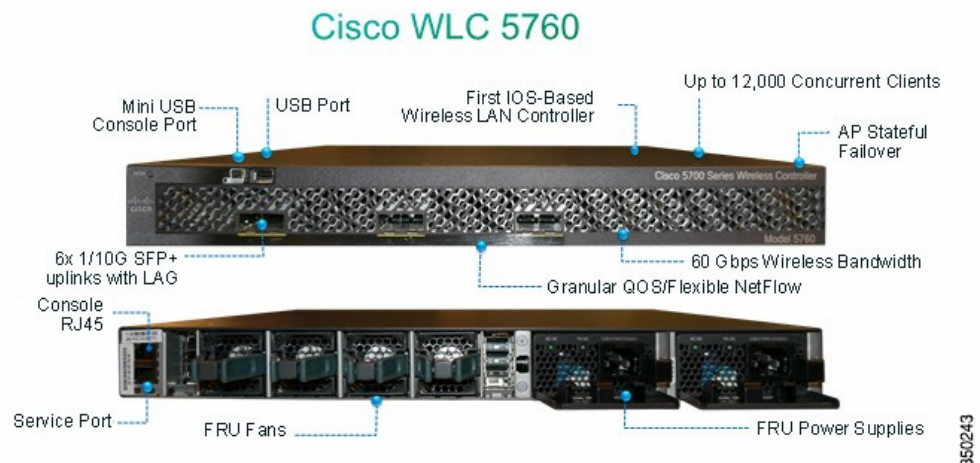
Unified Access Catalyst 3850 Switches

The Unified Access Catalyst 3850 switch is a flexible ASIC-based hardware that can support multiple protocols and has many advantages over the current hardware platform. The Catalyst 3850 switch has an integrated hardware-based wireless support with Control and Provisioning of Wireless Access Points (CAPWAP) and fragmentation. It also has 40 GB of uplink bandwidth when all ports function at line rate.

The Catalyst 3850 switch provides an open service platform. It has a 4-core CPU to leverage the operating system (OS) and to host various services. The Catalyst 3850 hardware is the next- generation switching hardware.

The UA Catalyst 3850 switch has unified wired and wireless architecture. The wireless operating system is Cisco IOS® software-based. UA Catalyst 3850 switch provides uniform wired and wireless policies. It can house 50 access points (802.11n) and support 2000 clients per stack. Figure 1-2 shows the platform overview for the Catalyst 3850.

Refer to the Catalyst 3850 Configuration Guides page for detailed information on configuration recommendation.

Figure 1-2   New Catalyst 3850
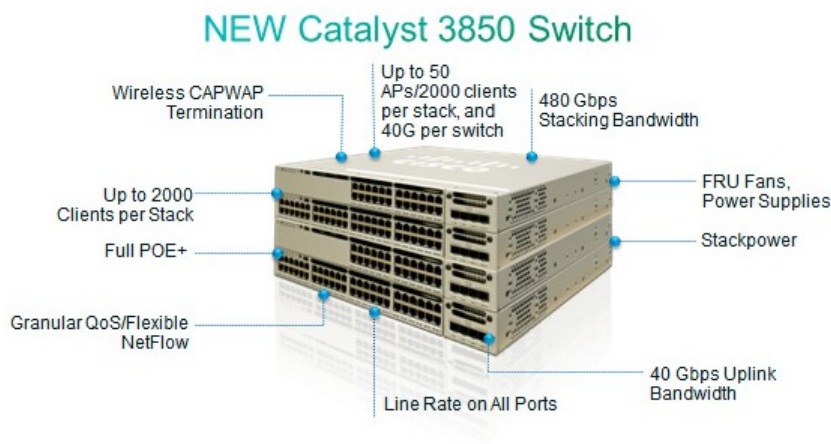
Supported Features

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
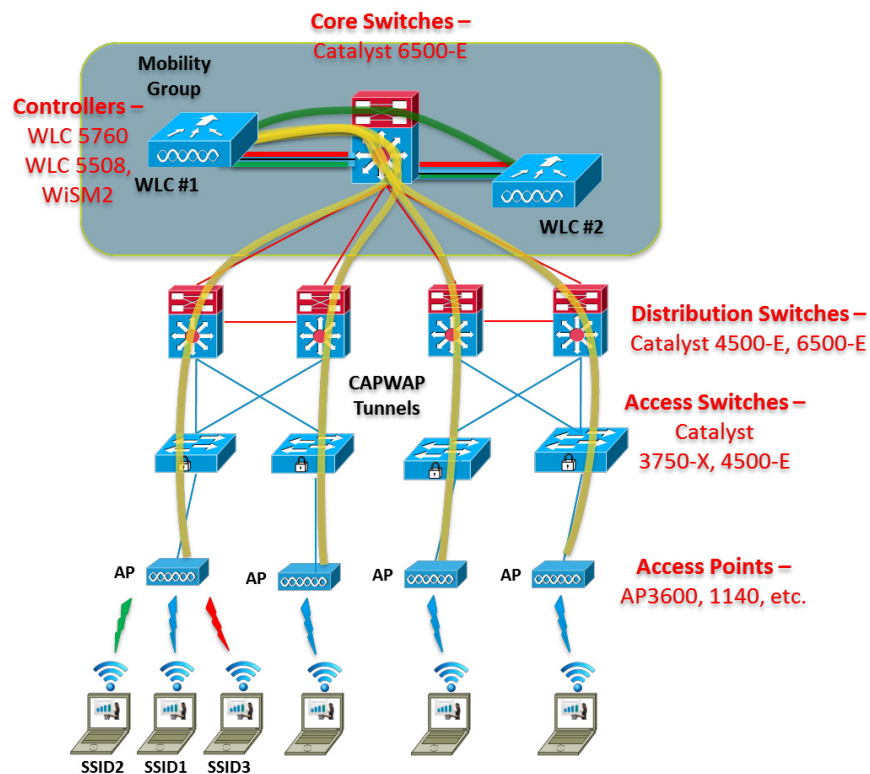
Converged Access Mode

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
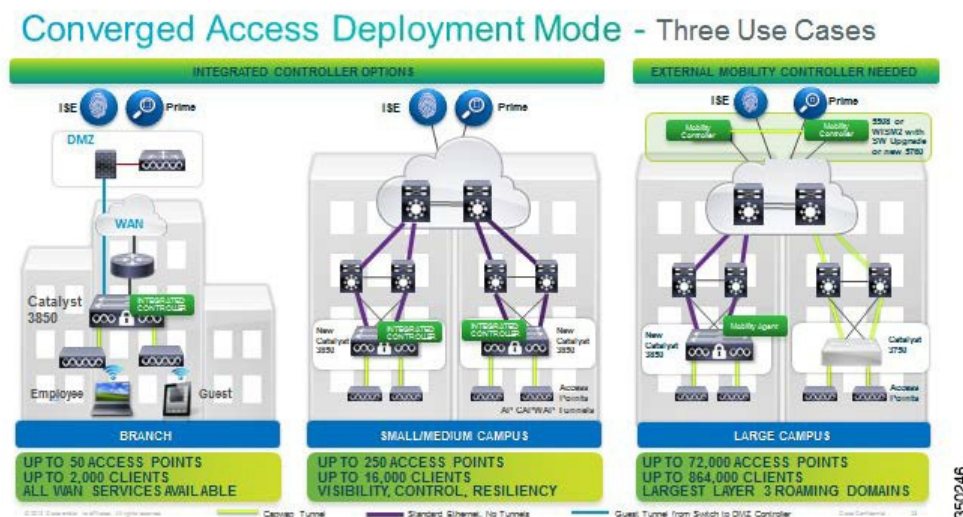
Converged Access Components

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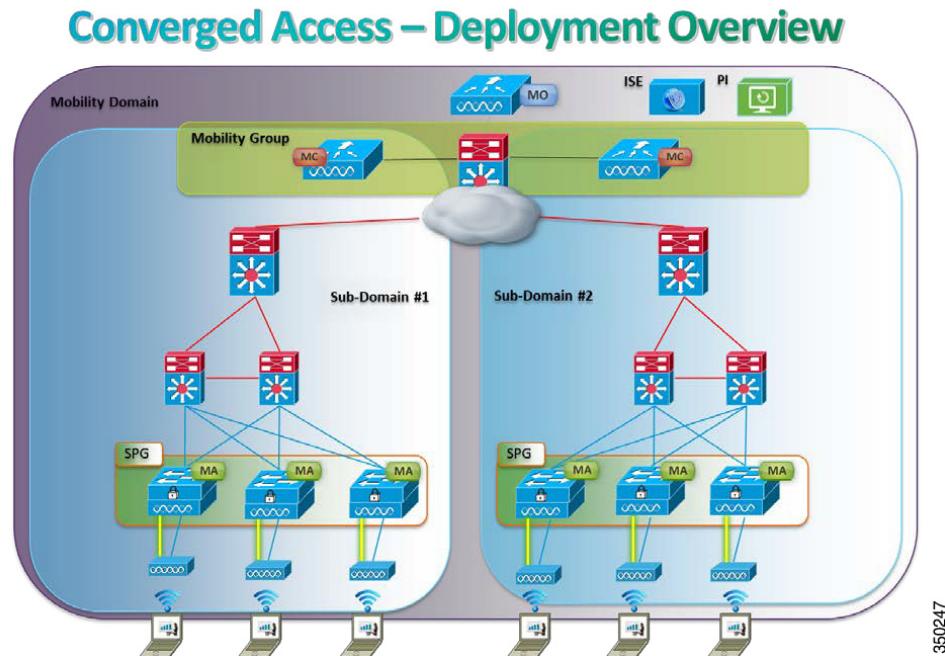
This deployment guide focuses on the configuration of the new CT5760 feature set with the Cisco IOS® software. For detailed information on the new Catalyst 3850 wired/wireless switch and its deployment scenarios, refer to the Catalyst 3850 Deployment/Configuration Guides page.

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*
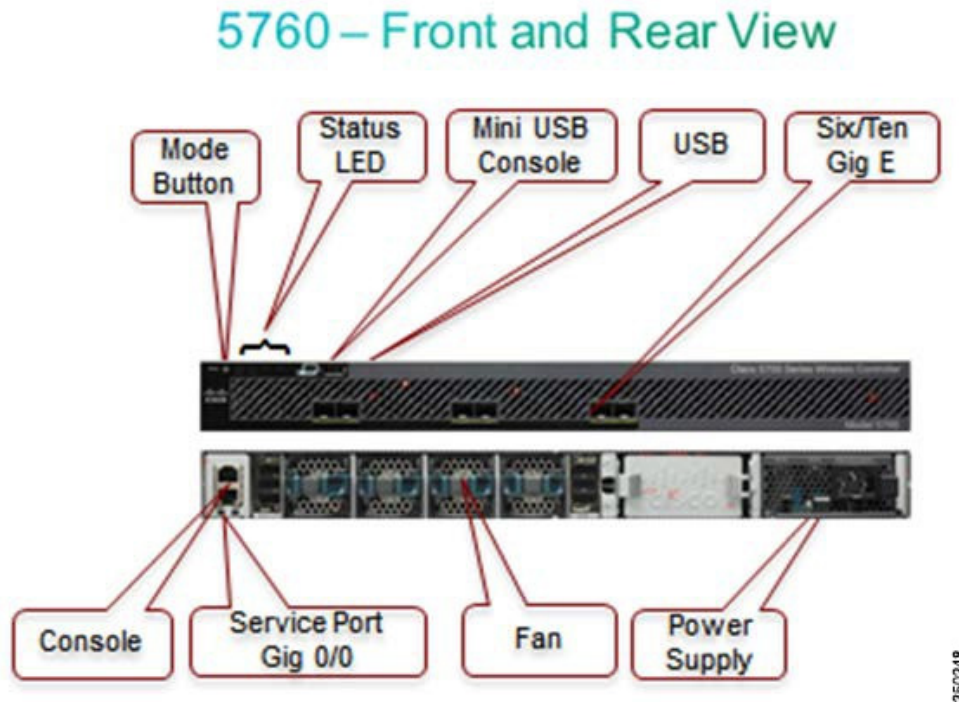
Management Port (Service Port) (RJ-45)

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
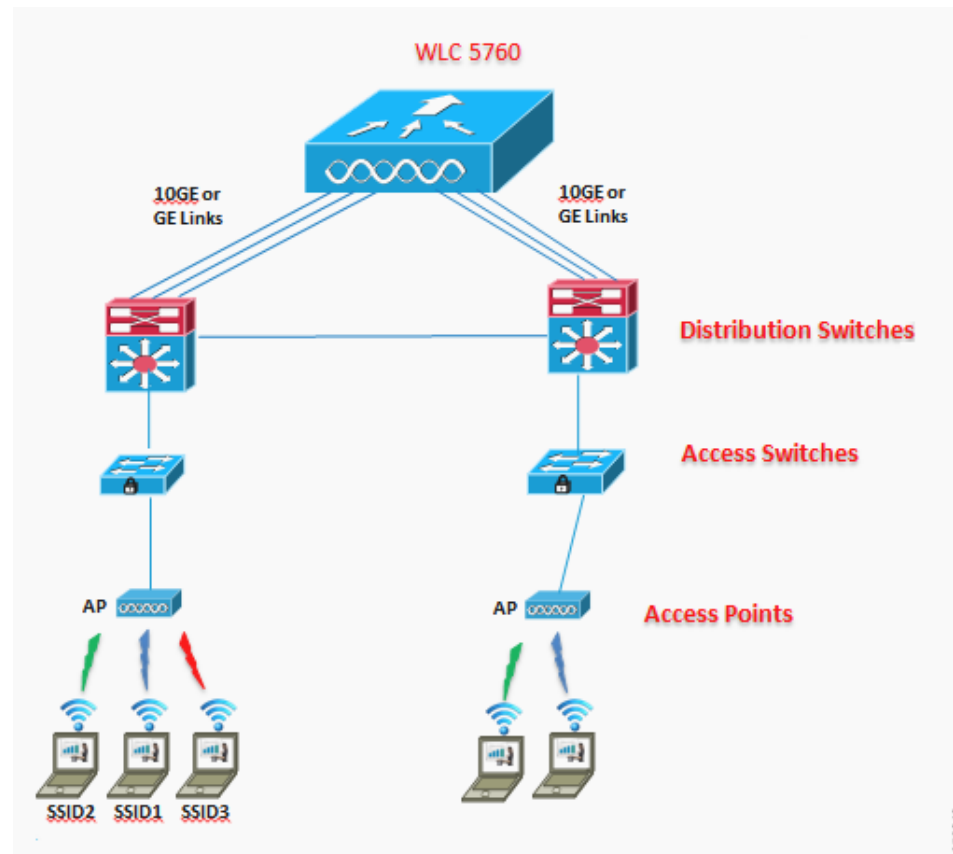
Configure the Controller and Neighbor Devices to Support LAG

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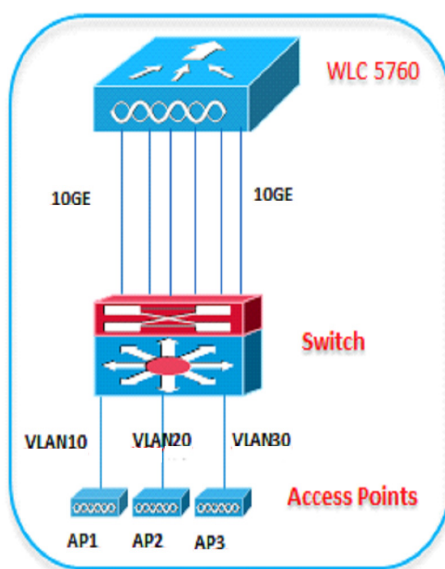
You can configure up to 5 AP-manager interfaces on the controller along with one wireless management interface.

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
```

CT5760 Centralized Configuration Example

Network Topology

The diagram in Figure 3-1 shows the network topology with only the Unified Access CT5760 controller in a centralized deployment.

Figure 3-1   *Network Topology Centralized Configuration*
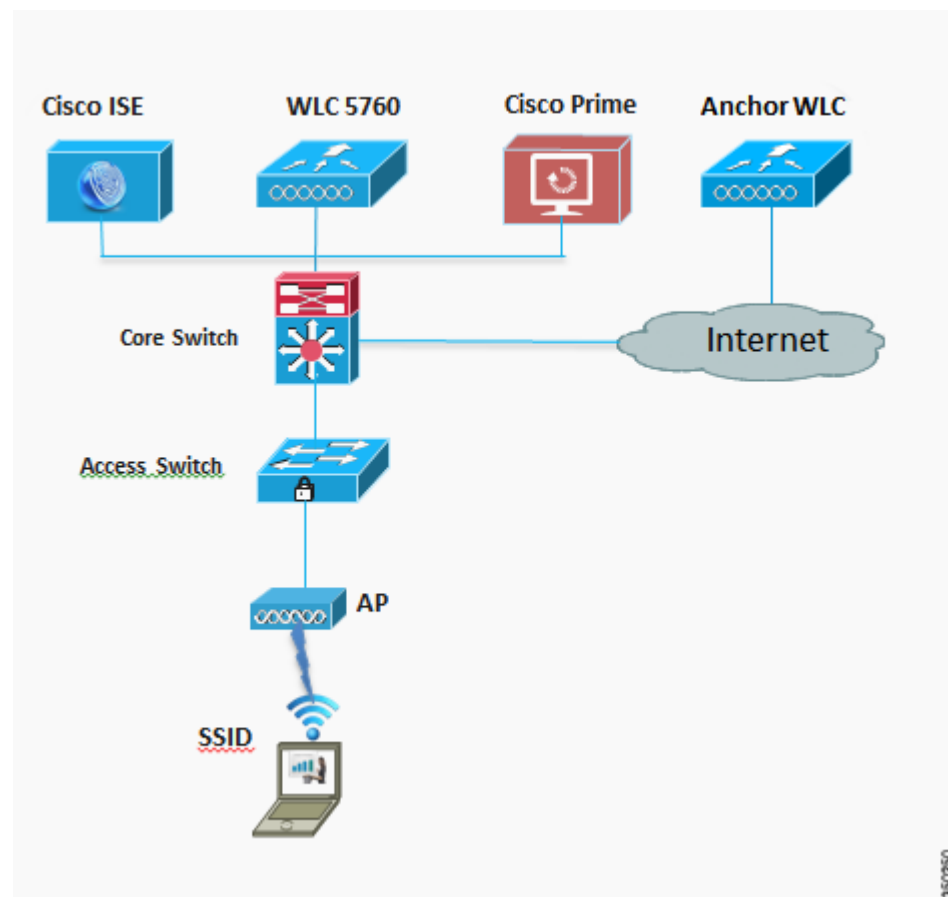
VLANs and IP Addresses

Table 3-1   VLANs and IP Address by Device

Device	VLAN	IP Address
DHCP Server	Gateway	10.10.100.1 / 10.10.200.1
Cisco Prime Infrastructure	200	10.10.200.30
Cisco ISE	200	10.10.200.60
Anchor WLC	300	192.168.1.5
Core Switch	200, 100	10.10.100.1 / 10.10.200.1
AP	200	DHCP
5760 WLC	200	10.10.200.5
Client VLAN	100	DHCP
Management VLAN	200	10.10.200.5
NTP Server	Gateway	10.10.200.1

CT5760 Controller Configuration Example using CLI

Before you start the controller configuration, ensure that there is complete connectivity between all of the switches in the configuration above.

Console Connection

Before you can configure the switch or controller for basic operations, you must connect it to a PC that uses a VT-100 terminal emulator (such as HyperTerminal, ProComm, or Putty).

The controller has both EIA/TIA-232 asynchronous (RJ-45) and USB 5-pin mini Type B, 2.0 compliant serial console ports. The default parameters for the console ports are 9600 baud, eight data bits, one stop bit, and no parity. The console ports do not support hardware flow control. Choose the serial baud rate of 9600; if you have issues, try a baud rate of 115200.Figure 3-2 shows an example of a Mac Secure CRT; use similar for PC/Windows Putty, and so on.

Figure 3-2   Mac Secure CRT Example
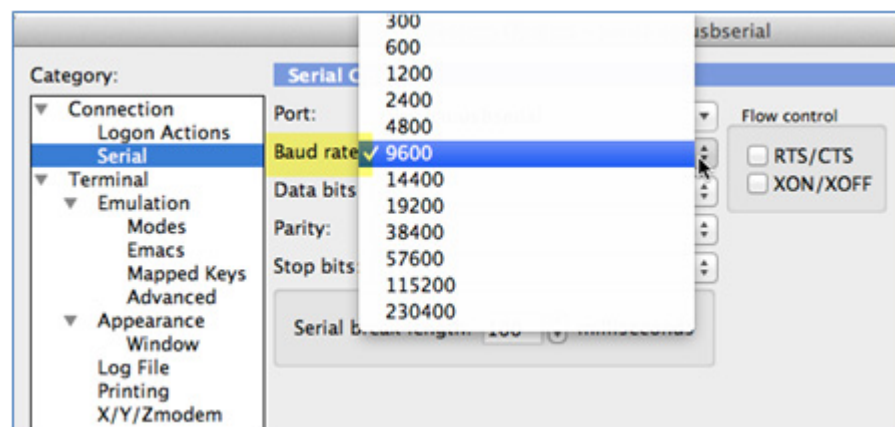
Startup Wizard

Before you launch the startup wizard, have your IP addresses and VLANs information available. Start without the wizard/initial configuration dialog (check the initial configuration).

```
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no
Would you like to terminate autoinstall? [yes]:
Controller>
Press RETURN to get started!


Start with the wizard/initial configuration dialog (check the initial config).
Enable secret warning
----------------------------------
In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the enable
secret
If you choose not to enter the initial configuration dialog, or if you exit setup
without setting the enable secret,
please set an enable secret using the following CLI in configuration mode-
enable secret 0 <cleartext password>
----------------------------------
Would you like to enter the initial configuration dialog? [yes/no]: yes


At any point you may enter a question mark '?' for help. Use ctrl-c to abort configuration
dialog at any prompt. Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity for management of the system,
extended setup will ask you to configure each interface on the system


Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:


Enter host name [Controller]: CT5760-Controller


The enable secret is a password used to protect access to privileged EXEC and
configuration modes. This password, after entered, becomes encrypted in the
configuration.
Enter enable secret: Cisco123


The enable password is used when you do not specify an enable secret password, with some
older software versions, and some boot images.
Enter enable password: Cisco123
The virtual terminal password is used to protect access to the router over a network
interface. Enter virtual terminal password: Cisco123
Configure a NTP server now? [yes]: yes
Enter ntp server address : 10.10.200.1
```

```
Enter a polling interval between 16 and 131072 secs which is power of 2:16
Do you want to configure wireless network? [no]: yes
Enter mobility group name: New-Mobility
Enter the country code[US]:US
Configure SNMP Network Management? [no]: no


Current interface summary


Any interface listed with OK? value "NO" does not have a valid configuration

  Interface          IP-Address       OK? Method Status        Protocol
  Vlan1              unassigned       NO  unset  up            down
  GigabitEthernet0/  unassigned       YES unset  up             up
  Te1/0/1            unassigned       YES unset  down          down
  Te1/0/2            unassigned       YES unset  down          down
  Te1/0/3            unassigned       YES unset  down          down
  Te1/0/4            unassigned       YES unset  down          down
  Te1/0/5            unassigned       YES unset  down          down
  Te1/0/6            unassigned       YES unset  down          down


Enter interface name used to connect to the management network from the above interface
summary: GigabitEthernet0/0[service port)


Configuring interface GigabitEthernet0/0: Configure IP on this interface? [no]: yes
IP address for this interface: 192.168.2.50
Subnet mask for this interface [255.255.0.0] : 255.255.255.0


Wireless management interface needs to be configured at startup
It needs to be mapped to an SVI that is not Vlan 1 (default)


Enter VLAN No for wireless management interface: 200
Enter IP address: 10.10.200.5
Enter IP address mask:: 255.255.255.0


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]:2
Press RETURN to get started!
```

Version

#show version

IOS XE 3.X (3.2.0SE at FCS) is the official version for 3850/5760 & should be the only version number used when referring to 3850/5760.

#show version running

Will show the WCM and IOSd versions

```
#show ap name apname config general
```

Will show AP version, which will be 15.X at FCS.

Date and Time Configuration

```
clock set hh:mm:ss day month year
```

Enable the CT5760 Controller Web GUI

Supported Browser Version

Below is a list of supported browser versions:

- Chrome – Ver. 26.x
- Mozilla – Ver. 20.x
- IE – Ver. 8.x, 9.x, and 10.x

Enabling WEB GUI on both the 5760 and 3850 Platforms

Both the Cat3850 and CT5760 currently ship with the first release labeled as 3.2.01. If you have an existing CAT3850/CT5760 and want to use GUI to Configure/Monitor your wireless network, please follow the steps below:

1. Console to the 3850/5760 platform. Save your current config and upgrade to 3.2.2 release available on cisco.com. Upgrade procedure can be found in the link below:

    Note During the upgrade, firmware will be upgraded and therefore it will take few more additional minutes than the regular upgrade. Please do not turn off the unit during the upgrade.

    http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/system_management/appendix/swiosfs.html#wp1311040

2. After upgrading to 3.2.2 version, the web GUI functionality will be enabled. By default, https is enabled. You can access the web GUI through https but if you want to enable http access, you can do so by issuing the following command using IOS CLI: `Controller(config)#ip http server`

3. Using IOS CLI, you will need to create a username and password to access the GUI. You can configure a local username by issuing the following command: `Controller(config)#username admin privilege 15 password Cisco123`. Or you can configure it to use credentials using an authentication server. Make sure the user has privilege 15 access level.

4. In order to access the GUI, you can configure the out of band management port (GigE 0/0) or use existing reachable configured interfaces through the network.

5. Now you will be able to access the Web GUI interface. Open a browser and type your controller/switch IP address. Example: https://10.10.10.5/ . Please refer to the access example below.

    Note If you have an out of the box or brand new 5760 or 3850, please console to the box and go through the Startup Wizard as outlined in this deployment guide in earlier sections.

GUI Access for CT5760/3850 Example

Complete these steps:

Step 1   GUI access–Open a browser and type your controller IP address. By default https is enabled.

For example:

https://10.10.10.5

username: admin

Password: Cisco123

Note   You can setup username/password using the following CLI command: `Controller(config)#username admin privilege 15 password Cisco123`. This is an example and not the default username and password.
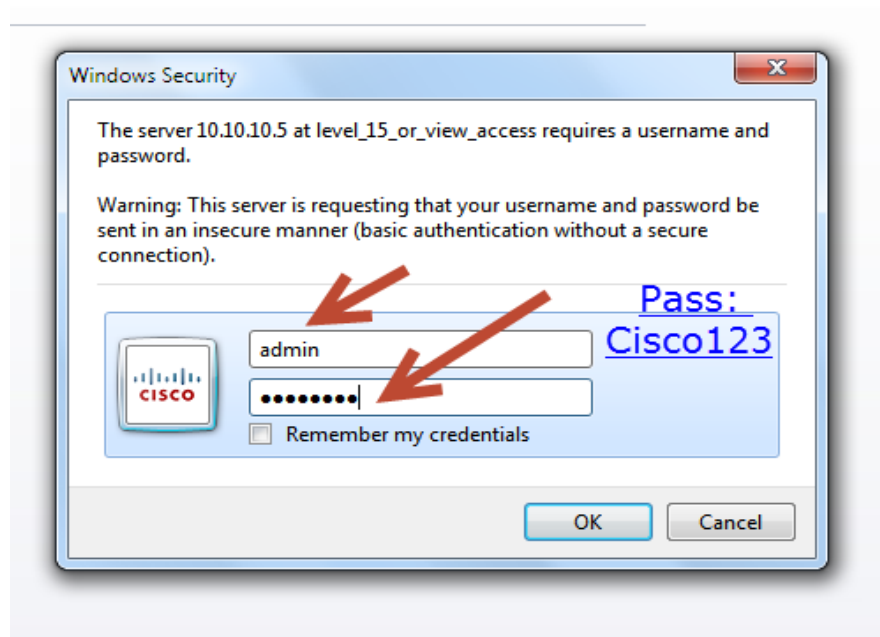
Once you login, you will be directed to the following page:

Cisco Systems

Accessing Cisco AIR-CT5760 "Controller"

Telnet - to the router.

Show interfaces - display the status of the interfaces.
Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

Show tech-support - display information commonly needed by tech support.
Extended Ping - Send extended ping commands.

Wireless Web GUI - Configure wireless on the Controller through the Web GUI interface.

Help resources

1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.

Step 2   Click **Wireless WEB GUI**, this will take you to the home page shown below:
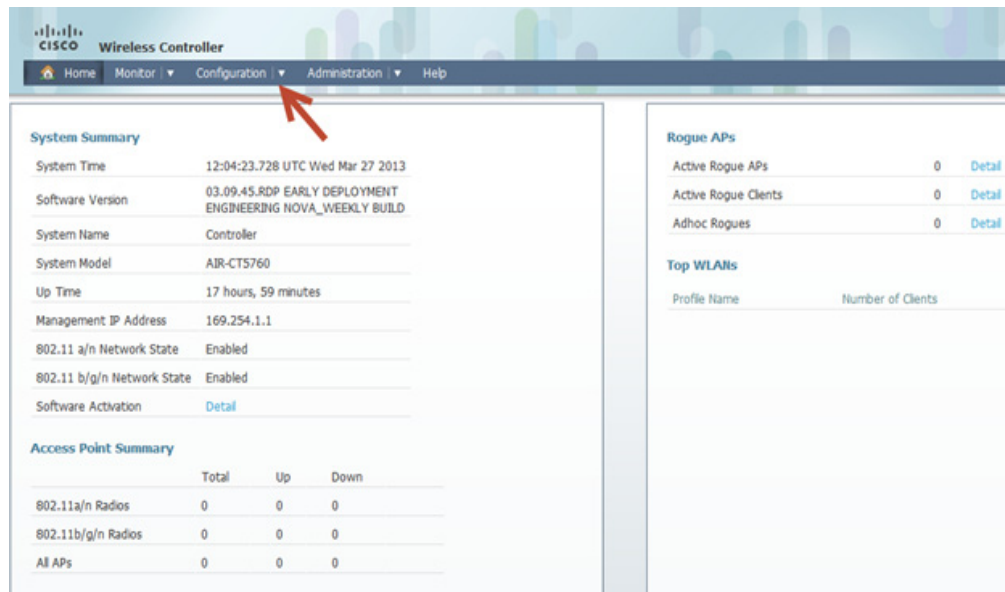
Note   For additional GUI configuration examples, please see Cisco Unified Access CT5760 Controllers, Catalyst 3850 Switches IOS XE Software release 3.2.2 Web GUI Deployment Guide

Basic Configuration

This section shows the configuration options from the console of the CT5760 for the following:

- Management and client interfaces
- DHCP configuration

Add Management and Client Interface

```
interface Vlan200
description "Management VLAN"
ip address 10.10.200.5 255.255.255.0
no shut

interface Vlan100
description "Client VLAN"
no shut


default-gateway 10.10.200.1
```

Wireless Management Interface Configuration on CT5760

Wireless management interface has been configured as part of the Startup Wizard section above. If you have not configured it through the Startup Wizard, you need to configure it by issuing the following command:

```
Controller# wireless management interface Vlan200
```

This will enable the AP to join the controller.

DHCP Snooping and Trust Configuration on CT5760

```
ip dhcp snooping vlan 100, 200
ip dhcp snooping wireless bootp-broadcast enable
ip dhcp snooping

interface TenGigabitEthernet1/0/1
description Connection to Core Switch
switchport trunk allowed vlan 100, 200
switchport mode trunk
ip dhcp relay information trusted ip dhcp snooping trust

interface Vlan100
description Client Vlan
ip dhcp relay information trusted
```

DHCP snooping is required for the following functionality:

1. "ip dhcp required" is enabled for the wlan. In this case, client won't go to run state unless DHCP snooping is enabled.

2. Dynamic ARP Inspection ("ip arp inspection" CLI) requires DHCP snooping database.

3. If 3rd party WGBs are used. In this case, destination MAC address in DHCP packets is modified.

4. To ensure that broadcast OFFER/ACK from server is converted unicast. If "ip dhcp snooping wireless bootp-broadcast enable" is configured, the broadcast OFFER/ACK from server is forwarded without modification.

5. To ensure that broadcast OFFER/ACK uses the right vlan in case of AAA over-ride. In general, not using DHCP snooping implies that DHCP packets are forwarded in hardware.

WLAN Configuration

Configure a WLAN and assign a client VLAN. Use WPA/PSK for security, and the passkey is **cisco123**.

```
wlan corporate 1 corporate band-select
client vlan 100
no security wpa akm dot1x
security wpa akm psk set-key ascii 0 cisco123
no shutdown
```

Enter this command to allow management over wireless.

```
wireless mgmt-via-wireless <cr>
```

AP Joins

Connect an AP to any port configured with Vlan 200 on the L2 switch. Wait until it joins and enter command:

show ap summary

show ap summary

```
Number of APs: 1
Global AP User Name: Not configured
Global AP Dot1x User Name: Not configured
AP Name / AP Model / Ethernet MAC / Radio MAC / State
--------------------------------------------------------------------------------
AP44d3.ca42.321a / 3602I / 44d3.ca42.321a / 64d9.8942.4090 / Registered
```

Connect a wireless client to the corporate SSID with the WPA key 'cisco123'. On the controller, you might see the following successful authorization for new client association.

Show wireless client summary from controller to confirm wireless clients.

Security Configuration

This section shows the configuration options from the console of the CT5760:

- Enable Authentication, Authorization, and Accounting (AAA)
- Configure ISE as RADIUS server (10.10.200.60)
- Shared secret - **secret**

Form CT5760 console (telnet/serial) - Configure AAA

```
aaa new-model
!
aaa group server radius Cisco
server 10.10.200.60
!
aaa authentication login no_auth none
aaa authentication dot1x default group radius
```

```
aaa authentication dot1x Cisco_dot1x group Cisco
aaa authorization network default group Cisco
aaa accounting network default start-stop group Cisco
dot1x system-auth-control
!
aaa server radius dynamic-author
auth-type any
!
radius-server attribute 6 on-for-login-auth
radius-server dead-criteria time 10 tries 3
radius-server deadtime 3
radius-server vsa send accounting
radius-server vsa send authentication
!
radius server Cisco
address ipv4 10.10.200.60 auth-port 1812 acct-port 1813
key secret
```

This command creates the WLAN with 802.1x security.

```
wlan corporate1x 2 corporate1x
accounting-list Cisco
client vlan 100
security dot1x authentication-list Cisco
session-timeout 600
no shutdown
```

Connect wireless client to corporate-1x with the following credentials:

Username = cisco ; Password = Cisco123

```
Controller#show wireless client summary
```

Wireless WebAuth and Guest Anchor Solutions

The following sections show a WebAuthentication (WebAuth) configuration and Guest Anchor examples on the CT5760.

Note   For a complete webauth configuration, please download the webauth bundle from the following URL: http://software.cisco.com/download/release.html?mdfid=284397235&softwareid=282791507& release=3.2.2&relind=AVAILABLE&rellifecycle=&reltype=latest .The readme file has all the GUI and CLI configuration for webauth.

Configure Parameter-Map Section in Global Configuration

The **parameter map** connection configuration mode commands allow you to define a connection- type parameter map. After you create the connection parameter map, you can configure TCP, IP, and other settings for the map.

! First section is to define our global values and the internal Virtual Address.

! This should be common across all WCM nodes.

```
PARAMETER-MAP TYPE WEBAUTH GLOBAL?
VIRTUAL-IP IPV4 192.0.2.1
PARAMETER-MAP TYPE WEBAUTH WEBPARALOCAL?
TYPE WEBAUTH?
BANNER TEXT ^C WEBAUTHX^C
REDIRECT ON-SUCCESS HTTP://9.12.128.50/WEBAUTH/LOGINSUCCESS.HTML
REDIRECT PORTAL IPV4 9.12.128.50
```

Configure Customized WebAuth Tar Packages

Transfer each file to flash:

```
copy tftp://10.1.10.100/WebAuth/webauth/ webauth_consent.htmlflash:webauth_consent.html
copy tftp://10.1.10.100/WebAuth/ webauth_success.html flash: webauth_success.html
copy tftp://10.1.10.100/WebAuth/ webauth_failure.html flash: webauth_failure.html
copy tftp://10.1.10.100/WebAuth/ webauth_expired.html flash: webauth_expired.html
```

Note In case the customized page contains images, they won't be displayed unless certain requirements are met, which are:

- The filename of the images must start with "web_auth_". For example: web_auth_logo.png.

- The image source in the HTML file must be edited to look like: `<img src="http://[wireless management ip]/flash:[name of the file]">`

Configure Parameter Map with Custom Pages

```
parameter-map type webauth webparalocal
type webauth
custom-page login device flash:webauth_consent.html
custom-page success device flash:webauth_success.html
custom-page failure device flash: webauth_failure.html
custom-page login expired device flash:webauth_expired.html
```

Configure Parameter Map with Type Consent and Email Options

```
parameter-map type webauth webparalocal
type consent
consent email
custom-page login device flash:webauth_consent.html
custom-page success device flash:webauth_success.html
custom-page failure device flash:webauth_failure.html
custom-page login expired device flash:webauth_expired.html
```

Configure Local WebAuth Authentication

```
username guest password guest123
aaa new model
dot1x system-auth-control
aaa authentication login EXT_AUTH local
aaa authorization network EXT_AUTH local
aaa authorization network default local
or
aaa authentication login default local
aaa authorization network default local
```

Configure External Radius for WebAuth

```
aaa new model
dot1x system-auth-control
aaa server radius dynamic-author ?
client 10.10.200.60 server-key cisco ?server-key cisco ?
auth-type any

radius server cisco
address ipv4 10.10.200.60 auth-port 1812 acct-port 1813
key cisco

aaa group server radius cisco server name cisco
aaa authentication login EXT_AUTHgroup cisco
or
aaa authentication login default group cisco
```

Configure WLAN with WebAuth

```
wlan Guest-WbAuth 3 Guest-WbAuth
client vlan 100
mobility anchor 192.168.5.1
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list EXT_AUTH
security web-auth parameter-map webparalocal
no shutdown
```

Configure HTTP Server in Global Configuration

!--- These are needed to enable Web Services in the Cisco IOS® software.

```
ip http server
ip http secure-server
ip http active-session-modules none
```

Other Configurations to be Checked or Enabled

!--- These are some global housekeeping Cisco IOS® software commands:

```
ip device tracking
ip dhcp snooping
```

SNMP Configuration

From the CT5760 console, configure the SNMP strings.

snmp---server community public ro

snmp---server community private rw

IPv6 Configuration

IPv6 is supported on the data path. Wireless clients will be able to get an IPv6 address.

Enable IPv6 Snooping - CT5760

There are slight differences in configurations on a CT5760 when configuring IPv6. To enable IPv6 on a CT5760, the following step must be completed.

```
ipv6 nd raguard attach-policy testgaurd
Trusted-port
Device-role router
interface TenGigabitEthernet1/0/1
description Uplink to Core Switch
switchport trunk native vlan 200
switchport mode trunk
ipv6 nd raguard attach-policy testgaurd
ip dhcp snooping trust
```

Enable IPv6 on Interface - CT5760

Based on interfaces that need IPv6 configurations and the type of address needed, respective configurations are enabled as follows. IPv6 configurations are enabled on VLAN200.

```
vlan configuration 100 200
ipv6 nd suppress
ipv6 snooping

interface Vlan100
description Client VLAN
ip address 10.10.100.5 255.255.255.0
ip helper-address 10.10.100.1 2001:DB8:0:10::1/64
```

```
ipv6 address FEC0:20:21::1/64
ipv6 enable
```

Mobility Architecture

Here are the mobility components in the new mobility architecture:

Mobility Agent

A mobility agent manages AP connectivity, CAPWAP tunnel terminations from APs and builds a database of client stations (endpoints) that are served locally as well as roamed from an Anchor WLC. Mobility agent can be either a Catalyst 3850 or a CT5760 mobility controller with an internal mobility agent running on it.

Mobility Controller:

A mobility controller provides mobility management tasks including inter-SPG roaming, RRM, and guest access. Mobility roaming, where a wireless client moves from one physical location to another without losing connectivity and services at any time, can be managed by a single mobility controller if roaming is limited to a mobility sub-domain. Roaming beyond a mobility sub-domain can be managed by multiple mobility controllers in a mobility group. The mobility controller is responsible for caching the Pairwise Master Key (PMK) of all clients on all the mobility controllers, enabling fast roaming of the clients within its sub-domain and mobility group. All the mobility agents in the sub-domain form CAPWAP mobility tunnels to the mobility controller and report local and roamed client states to the mobility controller. The mobility controller builds a database of client stations across all the mobility agents.

Mobility Oracle

Mobility oracle further enhances mobility scalability and performance by coordinating roaming activities among multiple mobility groups, which removes the need for N2 communications between mobility controllers in different mobility groups to improve efficiency and performance.

Mobility Group

The mobility group is a logical group of mobility controllers to enable fast roaming of clients within the mobility controllers of a mobility group.

Mobility Sub-domain

Multiple SPGs can be grouped together and collectively managed as a mobility sub-domain. One mobility controller is required for each mobility sub-domain.

Switch Peer Group

The Converged Access deployment defines an SPG as a logical group of mobility agents within one mobility controller (or mobility sub-domain). The main advantage of configuring SPGs is to constrain the roaming traffic to switches that form the SPG. When the mobility agents are configured in one SPG on the mobility controller, the software automatically forms full mesh CAPWAP tunnels between the mobility agent switches. These CAPWAP tunnels can be formed in a multi-layer network design (where the mobility agent switches are L2 adjacent on a VLAN spanned across) or a routed access design (where the mobility agent switches are L3 adjacent).

The SPGs should be designed as a group of mobility agent switches to where the users frequently roam.

Note   Roams within an SPG are local to the SPG, and need not involve the mobility controller. Roams across a SPG require traffic to traverse the mobility controller.

Figure 4-1   *Mobility Domain*
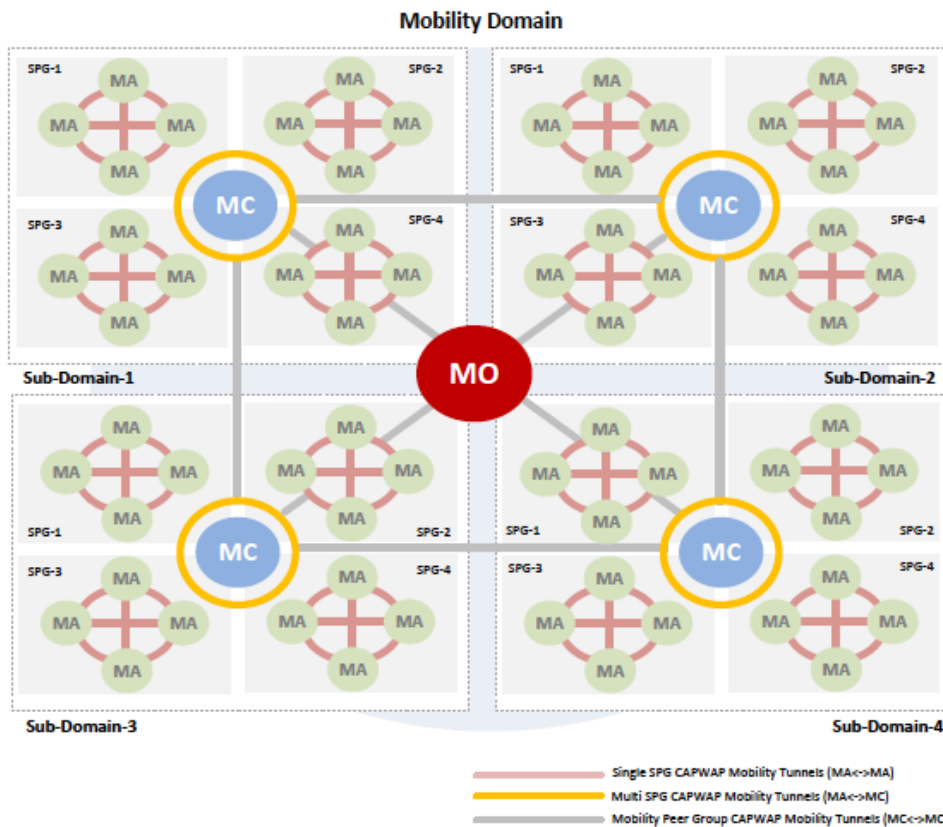
Figure 4-2   Mobility Design and Configuration: WLC5760 in Centralized Mode
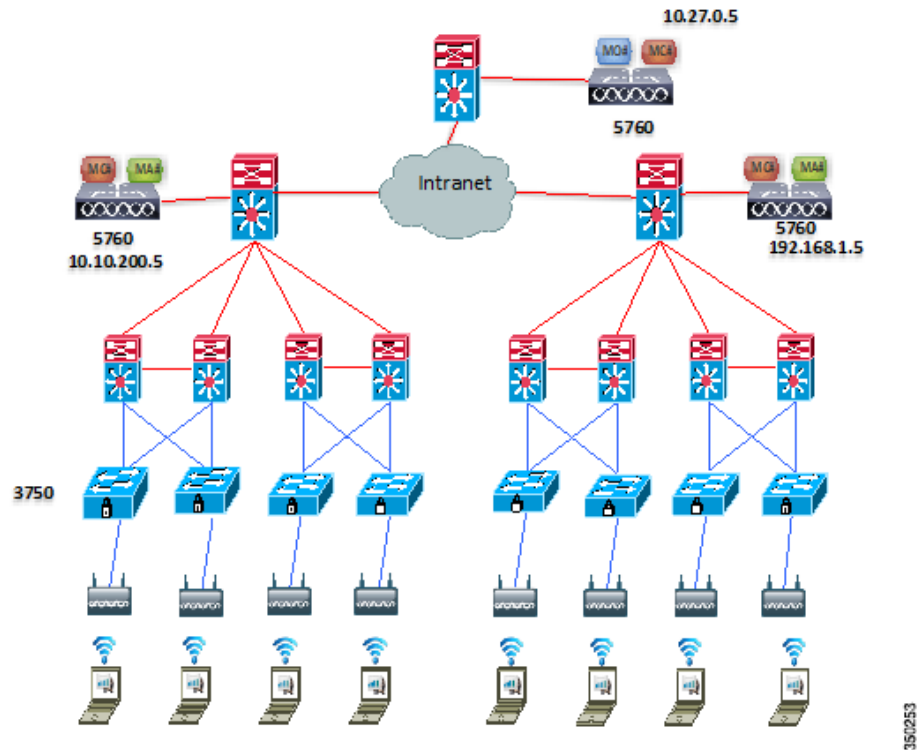
Mobility Configuration on WLC5760-Mobility Controller

```
wireless mobility controller
wireless mobility group member ip 10.27.0.5 public-ip 10.27.0.5
wireless mobility group member ip 192.168.1.5 public-ip 192.168.1.5
wireless mobility dscp 46
wireless management interface Vlan21
```

Mobility Configuration on WLC5760-Mobility Controller-Mobility Oracle

```
wireless mobility group member ip 10.10.200.5 public-ip 10.10.200.5
wireless mobility group member ip 192.168.1.5 public-ip 192.168.1.5
wireless mobility oracle
wireless management interface Vlan27
```

Mobility Configuration on WLC5508-Mobility Controller

```
config mobility new-architecture enable
```

```
config mobility mobility-oracle10.27.0.5
config mobility group member add 10.10.200.5
config mobility group member add 10.27.0.5
config mobility dtls-mode enable
config mobility dscp 46
```

Mobility Design and Configuration: WLC5760 (mobility controller) and Catalyst 3850 (mobility agent) in Converged Access Mode

Figure 4-3   Mobility Design and Configuration in Converged Access Mode
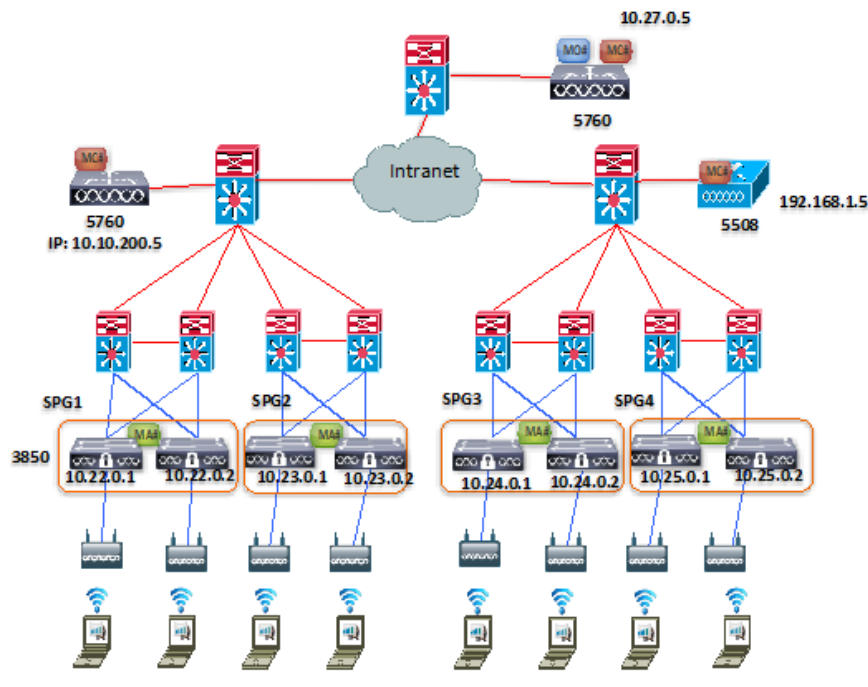
Mobility Configuration on WLC5760-Mobility Controller-Mobility Agent

```
wireless mobility controller
wireless mobility controller peer-group SPG1
wireless mobility controller peer-group SPG1 member ip 10.22.0.1 public-ip 10.22.0.1
wireless mobility controller peer-group SPG1 member ip 10.22.0.2 public-ip 10.22.0.2
wireless mobility controller peer-group SPG2
wireless mobility controller peer-group SPG2 member ip 10.23.0.1 public-ip 10.23.0.1
wireless mobility controller peer-group SPG2 member ip 10.23.0.2 public-ip 10.23.0.2
wireless mobility group member ip 10.27.0.5 public-ip 10.27.0.5
wireless mobility group member ip 192.168.1.5 public-ip 192.168.1.5
```

```
wireless mobility dscp 46
wireless mobility oracle ip 10.27.0.5 wireless management interface Vlan21
```

Mobility Configuration on WLC5760-Mobility Controller-Mobility Oracle

```
wireless mobility group member ip 10.10.200.5 public-ip 10.10.200.5
wireless mobility group member ip 192.168.1.5 public-ip 192.168.1.5
wireless mobility oracle
wireless management interface Vlan27
```

Mobility Configuration on WLC5508-Mobility Controller-Mobility Agent

```
config mobility new-architecture enable
config mobility mobility-oracle10.27.0.5
config mobility group member add 10.10.200.5
config mobility group member add 10.27.0.5
config mobility switchPeerGroup create SPG3
config mobility switchPeerGroup member add 10.24.0.1 SPG3
config mobility switchPeerGroup member add 10.24.0.2 SPG3
config mobility switchPeerGroup create SPG4
config mobility switchPeerGroup member add 10.25.0.1 SPG4
config mobility switchPeerGroup member add 10.25.0.2 SPG4
config mobility dtls-mode enable
config mobility dscp 46
```

Mobility Configuration on Catalyst 3850-Mobility Agent 1

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan22
```

Mobility Configuration on Catalyst 3850-Mobility Agent 2

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan22
```

Mobility Configuration on Catalyst 3850-Mobility Agent 3

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan23
```

Mobility Configuration on Catalyst 3850-Mobility Agent 4

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan23
```

Mobility Configuration on Catalyst 3850-Mobility Agent 5

```
wireless mobility controller ip 192.168.1.5 public-ip 192.168.1.5
wireless management interface Vlan24
```

Mobility Configuration on Catalyst 3850-Mobility Agent 6

```
wireless mobility controller ip 192.168.1.5 public-ip 192.168.1.5
wireless management interface Vlan24
```

Mobility Configuration on Catalyst 3850-Mobility Agent 7

```
wireless mobility controller ip 192.168.1.5 public-ip 192.168.1.5
wireless management interface Vlan25
```

Mobility Configuration on Catalyst 3850-Mobility Agent 8

```
wireless mobility controller ip 192.168.1.5 public-ip 192.168.1.5
wireless management interface Vlan25
```

Mobility Design and Configuration

Mobility Design and Configuration: WLC5760, WLC5508, and Catalyst 3850 in Hybrid Mode

The following section outlines the Mobility configuration for Hybrid deployment where you have a 3850 switch acting as a Mobility Agent and 3750 switch acting as regular L2 switch.

Figure 5-1 *Mobility Design and Configuration: WLC5760, WLC5508, and Catalyst 3850 in Hybrid Mode*

Mobility Configuration on WLC5760-Mobility Controller-Mobility Agent

```
wireless mobility controller
wireless mobility controller peer-group SPG1
wireless mobility controller peer-group SPG1 member ip 10.22.0.1 public-ip 10.22.0.1
wireless mobility controller peer-group SPG1 member ip 10.22.0.2 public-ip 10.22.0.2
wireless mobility controller peer-group SPG2
wireless mobility controller peer-group SPG2 member ip 10.23.0.1 public-ip 10.23.0.1
wireless mobility group member ip 10.27.0.5 public-ip 10.27.0.5
wireless mobility group member ip 192.168.1.5 public-ip 192.168.1.5
wireless mobility dscp 46
wireless mobility oracle ip 10.27.0.5
wireless management interface Vlan21
```

Mobility Configuration on WLC5760-Mobility Controller-Mobility Oracle

```
wireless mobility group member ip 10.10.200.5 public-ip 10.10.200.5
wireless mobility group member ip 192.168.1.5 public-ip 192.168.1.5
wireless mobility oracle
wireless management interface Vlan27
```

Mobility Configuration on WLC5508-Mobility Controller-Mobility Agent

```
config mobility new-architecture enable
config mobility mobility-oracle10.27.0.5
config mobility group member add 10.10.200.5
config mobility group member add 10.27.0.5
config mobility switchPeerGroup create SPG3
config mobility switchPeerGroup member add 10.24.0.1 SPG3
config mobility switchPeerGroup member add 10.24.0.2 SPG3
config mobility dtls-mode enable
config mobility dscp 46
```

Mobility Configuration on Catalyst 3850-Mobility Agent 1

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan22
```

Mobility Configuration on Catalyst 3850-Mobility Agent 2

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan22
```

Mobility Configuration on Catalyst 3850-Mobility Agent 3

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan23
```

Mobility Configuration on Catalyst 3850-Mobility Agent 4

```
wireless mobility controller ip 192.168.1.5 public-ip 192.168.1.5
wireless management interface Vlan24
```

Mobility Configuration on Catalyst 3850-Mobility Agent 5

```
wireless mobility controller ip 192.168.1.5 public-ip 192.168.1.5
wireless management interface Vlan24
```
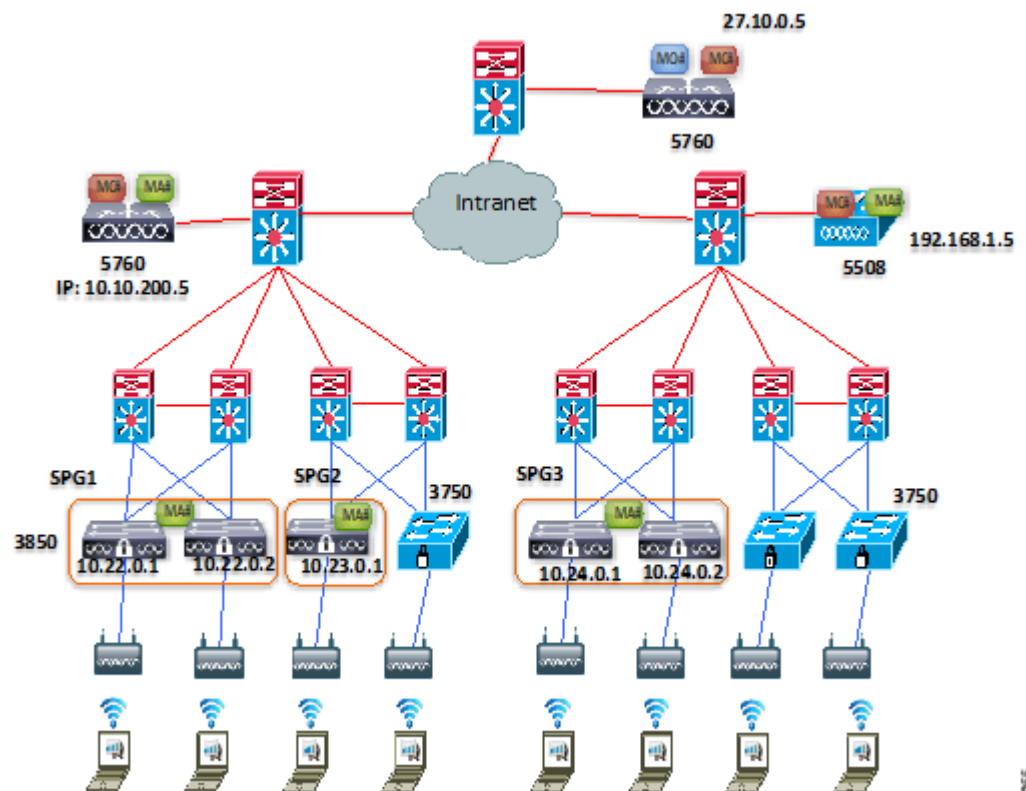
Configuring ClientLink (Beamforming)

Cisco ClientLink uses advanced signal processing techniques and multiple transmit paths to optimize the signal received by 802.11 a/g/n clients in the downlink direction without feedback. By default, ClientLink is disabled. You can see ClientLink general status through the show network command: **ap dot11** {24ghz | 5ghz}.

You can enable ClientLink for all APs, with the global configuration command ap dot11 {24ghz | 5ghz} beamforming. Use the "no" form of the command to disable ClientLink:

ap dot11 5ghz shutdown

ap dot11 5ghz beamforming

no ap dot11 5ghz shutdown

These commands enable ClientLink globally; then, it disables ClientLink on a specific AP radio:

ap dot11 5ghz shutdown

ap dot11 5ghz beamforming

no ap dot11 5ghz shutdown

ap name 3602a dot11 5ghz shutdown

ap name 3602a no dot11 5ghz beamforming

ap name 3602a no dot11 5ghz shutdown

Show commands:

show ap dot11 5ghz network | include Beamforming

Legacy Tx Beamforming setting : Enabled

show ap name 3602a config dot11 5ghz | include Beamforming

Legacy Tx Beamforming Setting: Disabled

Bring Your Own Device (BYOD) and Security Configuration

This section discusses the self-service additions of personal devices securely. An employee registers a new device, and a certificate is automatically provisioned for that user and device. The certificate is installed along with a supplicant profile that is pre-configured to use that certificate and on- board the device into the corporate network. Two BYOD use cases supported for wireless supplicant included are:

- Single authentication of SSID BYOD for Apple device
- Dual authentication of SSID BYOD for Apple device.

Single Authentication of SSID BYOD for Apple Device Use Case

In this use case, there is a single SSID (BYOD-Dot1x) for corporate access that is authenticated and authorized with both Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol Transport Layer Security (EAP-TLS).

1. User associates to BYOD-Dot1x.

2. User enters employee username and password for PEAP authentication.

3. Authenticator authenticates user and performs URL-Redirect based on authorization policy.

4. User opens a browser and is redirected to self-registration portal for device registration.

5. Mac address gets pre-populated in the device registration page for DeviceID, and user enters a description and registers their device.

6. User's supplicant is provisioned, and certificates are installed.

7. After certificate installation, Change of Authorization (CoA) occurs; supplicant is authenticated and authorized using EAP-TLS.

8. Dynamic VLAN assignment occurs, and supplicant is placed in corporate VLAN

Dual Authentication of SSID BYOD for Apple Device Use Case

In a dual SSID use case, there are two SSIDs - one that is BYOD-Open for guest and one that authenticates for corporate access.

1. User associates to guest BYOD-Open SSID.

2. User opens a browser and is redirected to the Identity Services Engine (ISE) Central Web Authentication (CWA) guest portal.

3. Authenticator authenticates the associate user as an employee and directs the user to the employee device registration guest portal.

4. Mac address is pre-populated in the device registration page, and user enters a description and registers their device.

5. User's supplicant is provisioned and certificate is installed.

6. User disconnects from guest SSID.

7. User connects to corporate SSID and is authenticated/authorized to use the new profile.

Topology

Figure 6-1   BYOD Topology with Catalyst 3850 as the Authenticator
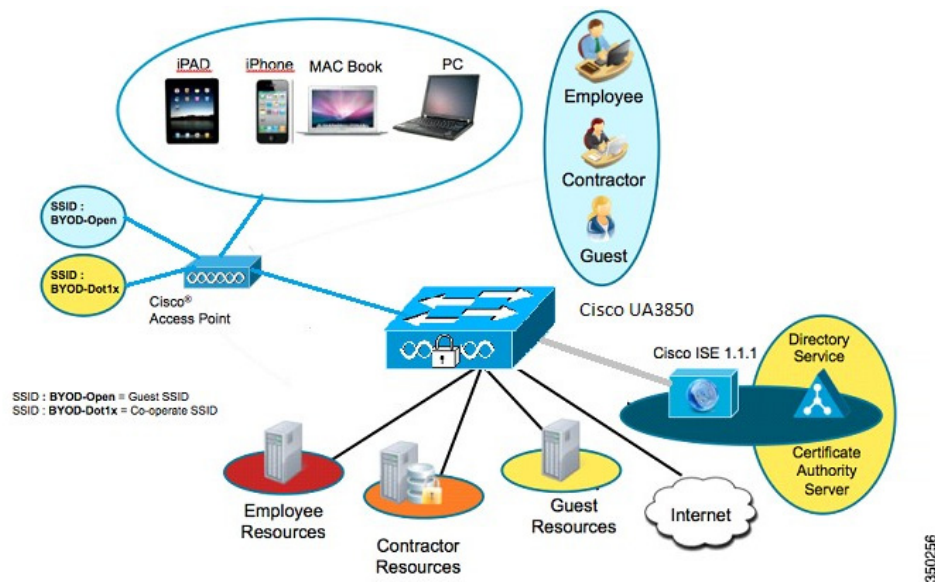
Figure 6-2   BYOD Topology with WLC5760 as the Authenticator
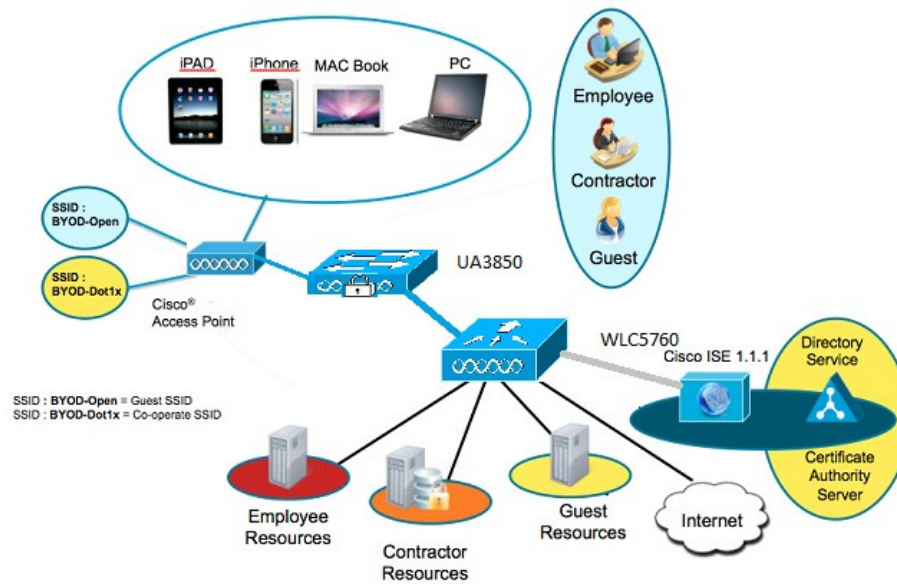
Components

Component	Hardware	Features Tested	Cisco IOS® Software Release
ISE	UCS Server	AAA override, profiler, posture	ISE 1.1.1
Certificate Authority and AD Server	Windows 2008 R2 Enterprise SP2	SCEP, Certificate Authority, Active Directory Server	-
Wireless Controller	UA3850 CT5760	Authentication/ Authorization, URL-Redirection, and CoA	03.07.98.EMP
Apple iOS Device	Apple iPad, iPhone	-	Apple iOS 5.0

Secure WLAN Configuration

Secure WLAN Configuration on Catalyst 3850/WLC5760

Wireless Dot1x Configuration

```
aaa new-model
aaa group server radius Cisco
server 10.10.200.60 auth-port 1812 acct-port 1813
aaa authentication login no_auth none
aaa authentication dot1x default group radius
aaa authentication dot1x Cisco_dot1x group Cisco
aaa authorization network default group Cisco
aaa accounting network default start-stop group Cisco
dot1x system-auth-control
```

Dynamic Authorization Configuration

```
aaa server radius dynamic-author
client 10.10.200.60 server-key Cisco123
auth-type any
```

Radius Server Configuration

```
radius-server attribute 6 on-for-login-auth
radius-server dead-criteria time 10 tries 3
radius-server deadtime 3
radius-server vsa send accounting
radius-server vsa send authentication
radius server Cisco
address ipv4 10.10.200.60 auth-port 1812 acct-port 1813
key secret
```

URL-Redirect Access-list Configuration

```
ip access-list extended NSP-ACL•  Supplicant Provisioning ACL
denyip any host 10.10.200.60
permit ip any any
```

HTTP Configuration

```
!
ip http server
ip http authentication local
ip http secure-server
ip http secure-client-auth
```

WLAN Configuration

```
wireless mobility controller
wireless management interface 200
wireless client user-timeout600
wlan BYOD-Dot1x 1 BYOD-Dot1x <- Secure Corporate SSID
aaa-override
accounting-list Cisco
client vlan 100
ip access-group NSP-ACL
nac
security dot1x authentication-list Cisco
session-timeout 600
no shutdown
wlan BYOD-Open 2 BYOD-Open <- Guest SSID
aaa-override
client vlan 100
ip access-group NSP-ACL
nac
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list Cisco
no shutdown
```

Verify Wireless Dot1x Session

```
Controller-MC#show access-session method dot1x details
Controller-MC#show access-session interface capwap 1 details
Controller-MC#show access-session mac 6420.0c37.5108 interface capwap 1
Controller-MC#show wireless client summary
```

Deauthenticate Client

```
Controller-MC#wireless client mac-address 6420.0c37.5108 deauthenticate
Controller-MC#show wireless client summary
```

802.11ac Support on WLC5760 and Catalyst 3850

802.11ac is the next generation wireless standard of 802.11. It is designed to provide high throughput and operate in the 5 GHz band. Multiple devices with the 802.11ac capabilities have already been released and available in the consumer market.

The Cisco CT5760 and Cat3850 products support the 11ac module on AP3600 as part of release 3.3.0 and AP3700 as part of 3.3 MR release.

802.11ac Configuration Example

This example discusses the use of AP3600 with 11ac module or the use of AP3700 with built-in 11ac module.

Pre-Requisites

- Check the AP3600 Data Sheet for detailed information about the AP:
  http://www.cisco.com/en/US/prod/collateral/modules/ps12859/ps13128/data_sheet_c78-727794.html
- Check the AP3700 Data Sheet for detailed information about the AP:
  http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps13367/data_sheet_c78-729421.html
- You will need an 11ac module installed on the AP3600 or use AP3700. Please refer to the AP3600 11ac Deployment guide for detailed information:
  http://www.cisco.com/en/US/docs/wireless/technology/apdeploy/7.5/Cisco_Aironet75.html#wp45244
- Have the AP3600 or AP3700 join the controller.
- Once the AP joins the controller, you can configure the radio using a static or dynamic configuration. Both methods are listed below:

Configuring 802.11ac from GUI

Once the APs joins the controller, navigate to **Configuration > Wireless > 802.11a/n/ac > Network**. You need to disable the 802.11a if it is enabled.
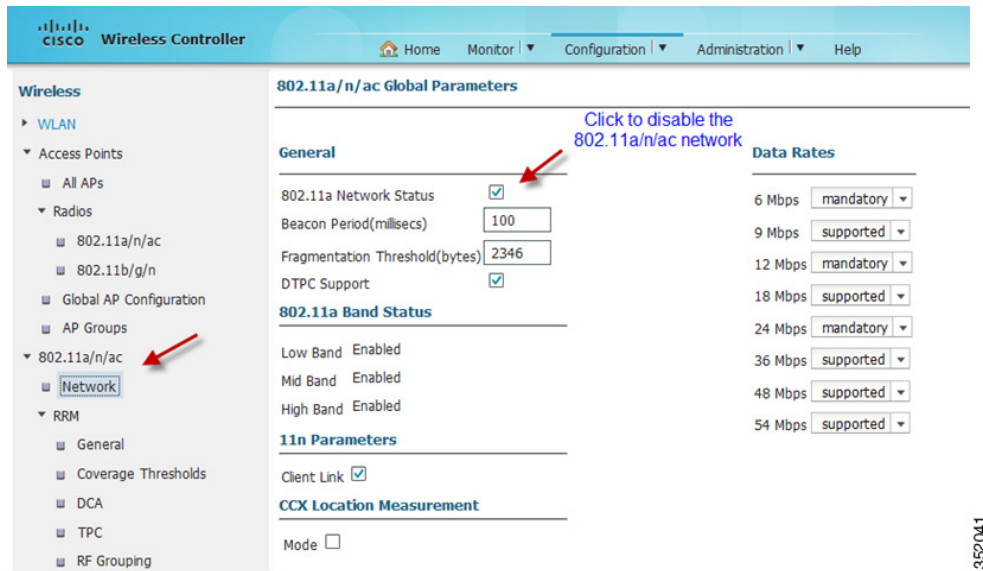
Now, navigate to **Configuration > Wireless > 802.11a/n > RRM > DCA**. Choose **80 MHz** under DCA Channel and Click **Apply**.
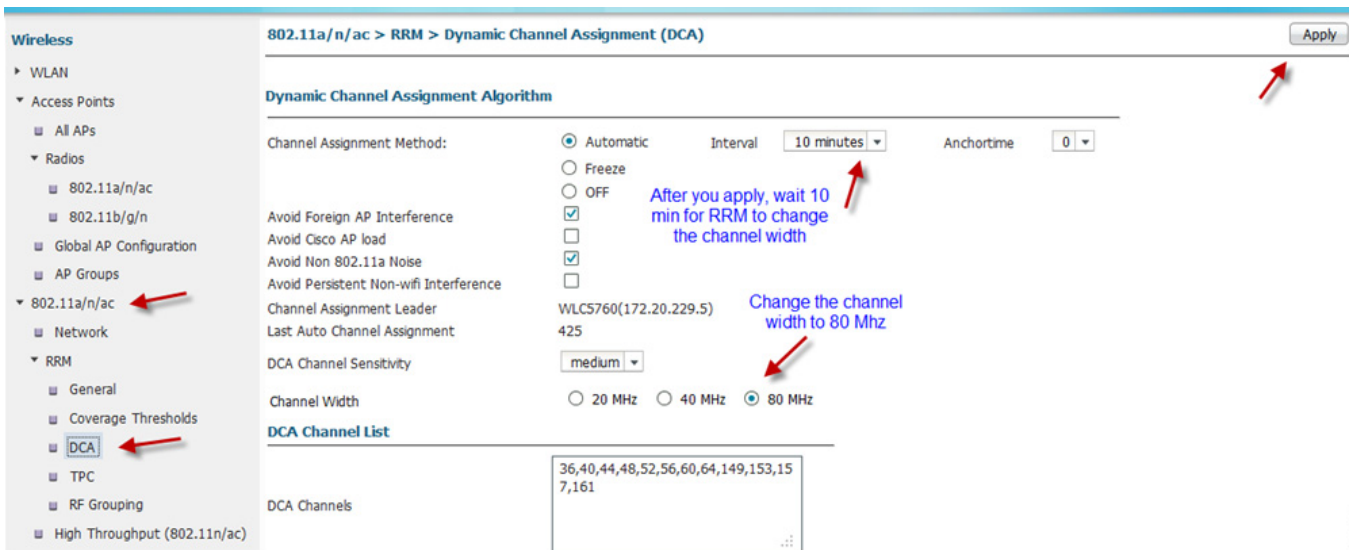
Now, you will need to enable the 802.11a network as shown below:
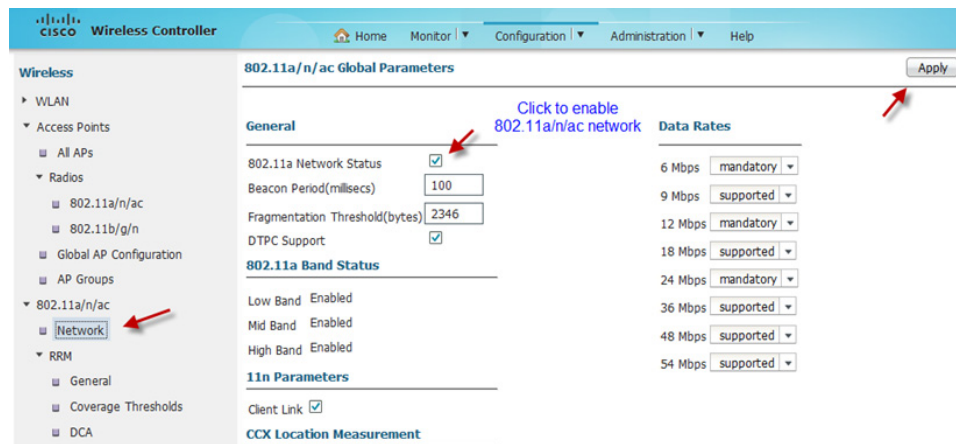
Once you apply the changes, you will need to wait about 10 minutes for RRM to change the channel width. You can check the status of the channels by issuing the following command or from the GUI:

```
WLC5760#show ap dot11 5ghz summary
AP Name           MAC Address       Slot  Admin State  Oper State  Channel                Width  TxPwr
----------------------------------------------------------------------------------------------------
AP3700-1          08cc.68b4.1030      1    Enabled      Up          (157,161,149,153)*       80    8(*)
AP3600_11ac       1ce6.c73e.5ab0      1    Enabled      Up          (157,161)*               40    8(*)
AP3600_11ac       1ce6.c73e.5ab0      2    Enabled      Up          (157,161,149,153)*       80    8(*)
```

GUI Verification
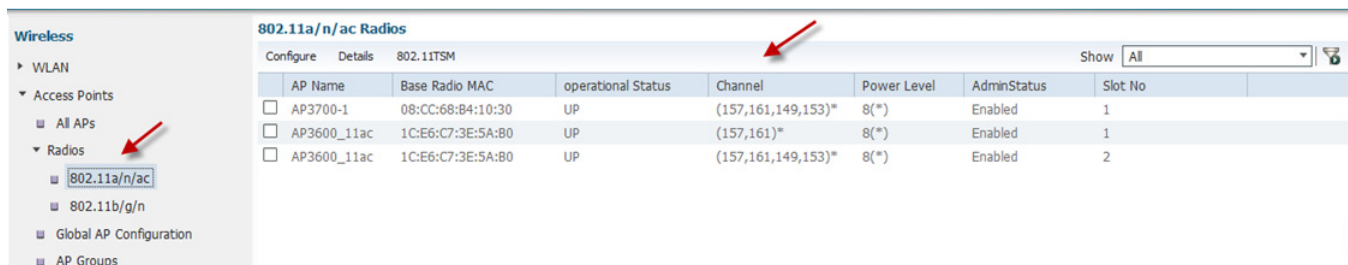
Enabling 802.11ac from CLI

1. 802.11ac Static Configuration

```
WLC5760#ap name AP3600_11ac dot11 5ghz shut

WLC5760#ap name AP3600_11ac dot11 5ghz channel 36 (or use other channels)

WLC5760#ap name AP3600_11ac dot11 5ghz channel width 80

WLC5760#ap name AP3600_11ac no dot11 5ghz shutdown
```

2. 802.11ac Dynamic Configuration

Note   The config below needs to be done on the RF group leader. In order to verify if a controller is an RF group leader, please issue the following command:

```
WLC5760#show ap dot11 5ghz group

Radio RF Grouping


802.11a Group Mode : AUTO

802.11a Group Update Interval : 600 seconds

802.11a Group Leader : WLC5760 (192.90.0.2)

802.11a Group Member WLC5760 (192.90.0.2)

802.11a Last Run : 324 seconds ago

Mobility Agents RF membership information

----------------------------------------------------------

No of 802.11a MA RF-members : 1


MA Member name IP address

-------------------------------------------------

Cat3850 192.80.0.2
```

You will see the RF Group Leader highlighted in bold above along with the IP address. On the RF Group Leader, issue the following command to enable 11ac.

```
WLC5760(config)#ap dot11 5ghz shut

WLC5760(config)#ap dot11 5ghz rrm channel dca chan-width 80

WLC5760(config)#no ap dot11 5ghz  shut
```

Note   After the above commands have been issued, please wait at least 1 RRM cycle which is 600 seconds by default to have the 80 MHz channel width settings enabled. You can use the commands below for verification.

3. 802.11ac Configuration Verification

Once you have configured 11ac on the AP, please check the following:

```
WLC5760#show ap dot11 5ghz summary
```


Note   Under Channel, you should see 4 channels assigned using the entire 80 MHz spectrum.

You can also check the channel width using the command below. Channel width should be 80 MHz.

```
WLC5760#sh ap dot11 5ghz channel

Automatic Channel Assignment

  Channel Assignment Mode                 : AUTO

  Channel Update Interval                 : 600 seconds

  Anchor time (Hour of the day)           : 0

  Channel Update Contribution             : SNI..

  Channel Assignment Leader               : WLC5760 (172.20.229.5)
```

```
Last Run                                    : 417 seconds ago

DCA Sensitivity Level                       : MEDIUM (15 dB)

DCA 802.11n Channel Width                   : 80 MHz

Channel Energy Levels

    Minimum                                 : unknown

    Average                                 : unknown

    Maximum                                 : unknown

Channel Dwell Times

    Minimum                                 : 11 hours 32 minutes 30 seconds

    Average                                 : 11 hours 32 minutes 30 seconds

    Maximum                                 : 11 hours 32 minutes 30 seconds

802.11a 5 GHz Auto-RF Channel List

Allowed Channel List                        : 36,40,44,48,52,56,60,64,149,153,157,161

Unused Channel List                         : 100,104,108,112,116,132,136,140,165

802.11a 4.9 GHz Auto-RF Channel List

Allowed Channel List                        :

Unused Channel List                         :
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26
```

4. 11ac Client Connection

Once 11ac has been enabled on the AP, connect an 11ac capable client. Make sure the client connects at 80 MHz. Issue the `Show wireless client summary` command. Verify that the 802.11ac clients have associated with 802.11ac protocol:

```
WLC5760#show wireless client summary
Number of Local Clients : 2


MAC Address     AP Name                        WLAN State              Protocol
-----------------------------------------------------------------------------------
64a3.cb4c.d68c  AP3600_11ac                    3    UP                 11n(5)
b8e8.5621.a392  AP3600_11ac                    3    UP                 11ac
```

You can verify client connectivity through the GUI:

Example: Using Broadcom 11ac client on Windows
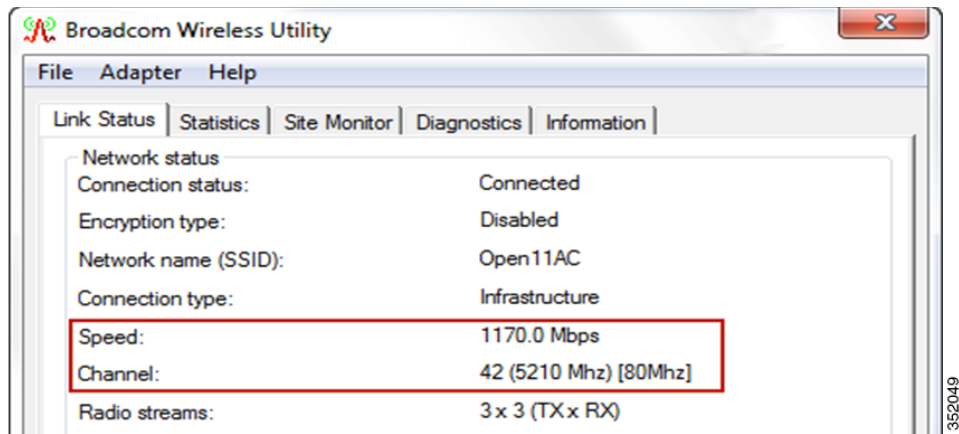
Windows Adapter Speed
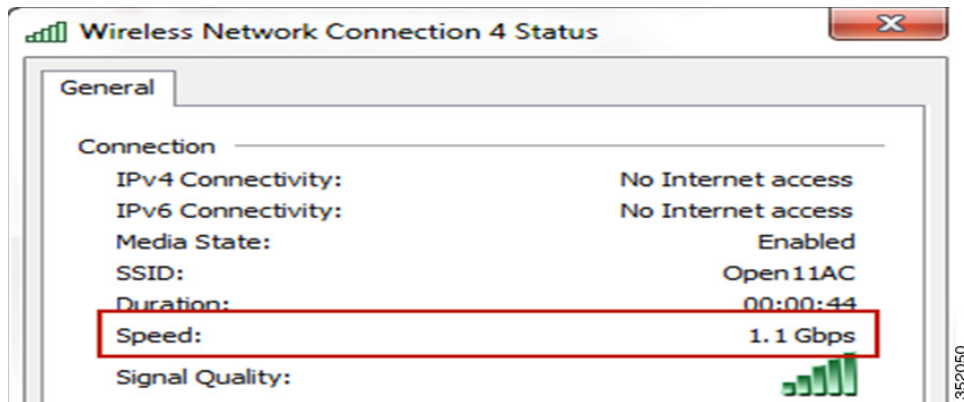
Radio Resource Management Configuration

Radio Resource Management Configuration

Information about Radio Resource Management

The Radio Resource Management (RRM) software embedded in the controller acts as a built-in radio frequency (RF) engineer to provide consistent, real-time RF management of your wireless network. RRM enables controllers to continually monitor their associated lightweight APs:

- **Traffic Load** - the total bandwidth used for transmitting and receiving traffic. It enables wireless LAN managers to track and plan network growth before client demand.

- **Interference** - the amount of traffic coming from other 802.11 sources.

- **Noise** - the amount of non-802.11 traffic that is interfering with the currently assigned channel.

- **Coverage** - the receiver signal strength indicator (RSSI) and signal-to-noise ratio (SNR)for all connected clients.

- **Other** - the number of nearby APs.

RRM can periodically reconfigure the 802.11 RF network for best efficiency. In order to do this, RRM performs these functions:

- Radio resource monitoring

- Transmit power control

- Dynamic channel assignment

- Coverage hole detection and correction.

For initial configuration purposes, the following covers items in the order that they occur in the current WLC GUI and focuses on predictable things that need adjustment from the default values.

RF Group Name

Assign the RF group name that RRM will use to identify members of your group and base the grouping algorithm to choose RF group leaders. Cisco recommends that you assign a distinctly different name to this test system to avoid interactions with established, production networks. In order to configure the RF Group Name, enter configuration mode at the command line of the mobility controller.

```
(config)#wireless rf-network <name> <cr>
802.11a/b network command
```

Several commands require that the network be disabled in order to execute. You can enable and disable the network very easily from the configuration terminal prompt.

```
Switch(config)#ap dot11 24/5ghz shut
Or use the no form to enable
config)# no ap dot11 24/5ghz shut)
```

This is the display of the default data-rates values. You might need to change several of these:

ap dot11 24/5ghz rate <rate> mandatory/supported/disabled:

As an example - disable 1,2,5.5,11 Mbps, enabling 24,54 Mbps as mandatory, all else supported. 5 GHz has 12, 24 Mbps as mandatory, all else supported:

```
ap dot11 2 shut
ap dot11 2 rate RATE_11M disable
ap dot11 2 rate RATE_1M disable
ap dot11 2 rate RATE_2M disable
ap dot11 2 rate RATE_5_5M disable
% Unable to modify rate, Since this is the last available BSS rate.
```

The above warning is issued since there are no other mandatory rates available – you must have at least one mandatory rate.

```
ap dot11 2 rate RATE_24M mandatory
ap dot11 2 rate RATE_5_5M disable
ap dot11 2 rate RATE_54M mandatory
no ap dot11 2 shut
ap dot11 5 shut
ap dot11 5 rate RATE_6M supported
no ap dot11 5 shut
```

The Legacy ClientLink default setting is disabled:

```
ap dot11 24/5ghz beamforming <cr>
```

Use the no form to disable.

The other Network settings are displayed for reference. Enable 802.11g support (on by default):

```
ap dot11 24ghz dot11g <cr>
```

Beacon interval - default is 100 ms - do not change:

ap dot11 24/5ghz beacon(20-1000 ms)

Short Preamble – on a Cisco AP, short preamble is enabled to allow the AP to adjust the preamble automatically. There is no way to set the preamble to always use short or long preamble. Short preamble is enabled by default. To disable short preamble, use the "no" form of the command:

ap dot11 24/5ghz preamble short<cr>

Fragmentation threshold - default 2346 - Do not change unless you have a significant reason:

ap dot11 24/5ghz fragmentation<256-2346> (bytes)

Dynamic Transmit Power Control (DTPC) support - Default is on. This tells a Cisco Compatible Extension (CCX) client the power level the AP used.

ap dot11 24/5ghz dtpc <cr>

Use the no form of the command to disable.

CCX Location Measurement Q – Default is off; enable if you use the CCX location features:

ap dot11 24/5ghz rrm ccx location-measurement <cr>

Use the no form to disable.

RRM RF Grouping and Next Generation Controller

RF Grouping can be configured for automatic or static modes. For automatic, mobility controllers negotiate with the grouping algorithm in order to choose a group leader. Static mode allows the user to choose a device that will be the group leader as well as add additional members manually. Members must be configured for automatic in order to join the static leader.

Set the RF Grouping Mode

For automatic RF grouping, use this command:

ap dot11 24/5Ghz rrm group-mode auto

For static and adding static members, member mobility controllers must be in automatic grouping mode:

ap dot11 24 rrm group-mode leader
ap dot11 24 rrm group-member Cisco_dd:f8:e4 IP address

Enter this command in order to disable/enable RRM RF Grouping:

ap dot11 24rrm group mode

RRM Transmit Power Control Configuration (TPC)

To configure RRM Transmit Power Control (TPC), choose the mode for the algorithm to operate or disable it. With the exception of the minimum/maximum commands, all TPC configurations are global commands and must be entered on the RF group leader to have an effect on the RF Group.

The default setting for TPC is configured to automatic (auto). In order to change this value, enter this command:

```
ap dot11 24 rrm txpower ?
<1-8>Enter transmit power level
autoEnables auto-RF
maxConfigures maximum auto-RF tx power
minConfigures minimum auto-RF tx power
onceEnables one-time auto-RF
```

If TPC is configured to automatic, then you may need to adjust the TPC-threshold value - (-70 dBm by default) valid range is -80 dBm to -50dBm:

```
ap dot11 24 rrm tpc threshold -70
```

Here is the command that shows the current RRM TPC configuration:

```
show ap dot11 24 txpower
```

RRM DCA Configuration

Dynamic channel assignment (DCA) is a global algorithm. Like TPC, it requires changes to be made to the RF group leader. Making changes to a member will have no effect on the algorithm, unless that member is changed to a leader.

The default DCA is configured to automatic. Other options include on-demand, as well as values for the anchor time and interval:

Use this command in order to enable DCA to run once and freeze:

```
ap dot11 24 rrm channel global once
```

Use this command in order to restore DCA to automatic:

```
ap dot11 24 rrm channel global auto
```

Use this command in order to set DCA to operate on a fixed interval other than the default of 10 minutes:

```
ap dot11 24 rrm channel dca anchor-time 1
ap dot11 24 rrm channel dca interval 8
```

These commands set the anchor time for 1 AM in the RF group leader's time zone and runs DCA every eight hours. Valid interval values are 1,2,3,4,6,8,12 and 24 hours; 0 = 10 minutes (default).

Use this command in order to set the DCA algorithm sensitivity (medium by default) use:

ap dot11 24 rrm channel dca sensitivity low

Options are medium/low/high.

Use this command to assign the channels that DCA will manage. Use one entry per channel, and run for both 2.4 and 5 Ghz bands:

ap dot11 24 rrm channel dca 1

ap dot11 24 rrm channel dca 6

ap dot11 24 rrm channel dca 11

Use the no form of the command to delete a channel from DCA control to manage options for the DCA algorithm, such as noise avoidance, foreign AP avoidance, load, CleanAir persistent device avoidance, and CleanAir Event Driven Radio Resource Management (EDRRM).

ap dot11 24 rrm channel ?

cleanair-event - Configure cleanair event-driven RRM parameters

dca - Config 802.11b dynamic channel assignment algorithm

device - no description - CleanAir PDA

foreign - Configure foreign AP 802.11b interference avoidance

global - Configures all 802.11b Cisco APs

load - Configure Cisco AP 802.11b load avoidance

noise - Configure 802.11b noise avoidance

Default values are foreign and noise.

Commands are entered one line at a time. Device, foreign, load, noise are on/off values. Use the no form of the command to turn off. The CleanAir event also has a sensitivity level associated with it. The default value is low; other options are medium and high.

The channel update contribution line indicates that our AP's Signal Noise, Interference (foreign), and Load (SNIUs) are at that moment added to DCA.

RRM Coverage Hole Detection and Mitigation

The default values for Coverage Hole Detection and Mitigation (CHDM) are sufficient for most environments. Items to change include the data/voice RSSI thresholds that determine when to consider a client in a coverage hole condition, the global coverage exception, and the percentage of failed clients per AP. There are other controls that are exposed at the command line. Unless directed, accept the defaults.

CHDM is a per controller configuration basis, and is not global. In order to enable or disable coverage hole detection, enter this command:

ap dot11 24 rrm coverage

Use the no form of the command to disable.

This command adjusts the RSSI threshold for data/voice clients:

ap dot11 24 rrm coverage data rssi-threshold -80

ap dot11 24 rrm coverage voice rssi-threshold -80

In order to set the level that a client is considered in a coverage hole, the default value is 80 dBm; valid range is -90/-60 dBm. The voice and data clients are two separate commands.

This command sets the minimum failed client count and the coverage exception level per AP:

ap dot11 `24 rrm coverage level global 3`

ap dot11 `24 rrm coverage exception global 25`

Three clients and 25% coverage exception are the default values; the available ranges are 1-75 clients and 0-100%.

The minimum failed client count and the exception level work together as a gating function for the feature. The defaults of three clients and 25% translate as a minimum of three clients must be in a coverage hole, and these three clients must represent at least 25% of the clients currently associated to the AP. This is the criterion for mitigation.

Neighbor Discovery Protocol

Neighbor Discovery Protocol (NDP) establishes RF proximity of all APs in your network. This is the basis for all calculations that RRM uses to balance the network for performance. NDP is an over-the-air open protocol by default. It is possible to secure this using encryption, but every member of the RF group must be in the same mode in order for NDP to function. In order to enable NDP protection, enter this command to every mobility agent and mobility controller on the network.

ap dot11 `24 rrm ndp-type protected`

CleanAir

Cisco CleanAir is a spectrum intelligence solution designed to proactively manage the challenges of a shared wireless spectrum. It allows you to see all of the users of the shared spectrum (both native devices and foreign interferers). It also enables you or your network to act upon this information. For example, you could manually remove the interfering device, or the system could automatically change the channel away from the interference.

Information about CleanAir

A Cisco CleanAir system consists of CleanAir-enabled APs, controllers, and Cisco Prime Infrastructure (PI). These APs collect information about all devices that operate in the industrial, scientific, and medical (ISM) bands. They identify and evaluate the information as a potential interference source and forward it to the controller. The controller controls the APs, collects spectrum data, and forwards the information to PI or to a Cisco Mobility Services Engine (MSE) upon request. The controller provides a local user interface to configure basic CleanAir features and displays basic spectrum information. PI provides an advanced user interface to configure Cisco CleanAir features, display information, and keep records. The MSE is optional for the basic feature set, but is required for advanced features such as tracking the location of non-Wi-Fi interference devices.

For every device operating in the unlicensed band, Cisco CleanAir tells you what it is, where it is, how it is impacting your wireless network, and what actions you or your network should take. It simplifies RF so that you do not have to be an RF expert.

Wireless LAN systems operate in unlicensed 2.4- and 5-GHz ISM bands. Many devices, such as microwave ovens, cordless phones, and Bluetooth devices also operate in these bands and can negatively affect Wi-Fi operations.

Some of the most advanced WLAN services, such as Voice over Wireless (VoWLAN) and IEEE 802.11n radio communications could be significantly impaired by the interference caused by other legal users of the ISM bands. The integration of Cisco CleanAir functionality into the Cisco Unified Wireless Network resolves RF interference problems.

CleanAir Configuration

CleanAir is disabled by default at the WLC/mobility controller level and must be enabled at all mobility controllers just like a WLC installation. In order to enable CleanAir on the switch, enter this command:

```
ap dot11 24 cleanair ap dot11 5
cleanair Controller#show ap dot11 24 sum
```

Enter this command in order to enable or disable CleanAir on a single AP radio:

ap name AP0022.bd18.87c0dot11 24 cleanair

The no form of the command disables CleanAir.

Use this command in order to query CleanAir for devices and AirQuality (AQ) at the AP radio and the global levels:

show ap dot11 24 cleanair device type all

Use this command in order to show the CleanAir configuration for the mobility controller:

show ap dot11 24 cleanair config

High Availability

With the WLC5760 first release 3.2.0, an AP can be configured with primary, secondary, and tertiary controllers. When the primary controller fails, depending upon the number of APs managed by a controller, the access point fails over to the secondary controller. Once it detects that the primary controller is unavailable, the AP rediscovers the controller and reestablishes the CAPWAP tunnel to the secondary controller. Additionally, the client must re-authenticate with the AP. Figure 11-1 illustrates the primary, secondary, tertiary controller redundancy.

Figure 11-1   WLC5760 High Availability
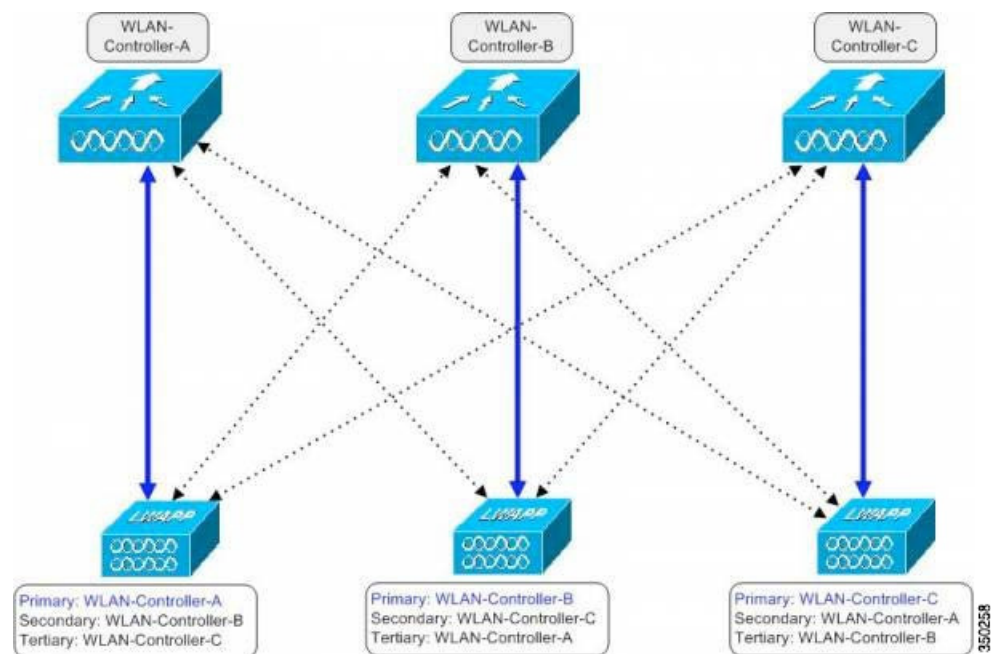
Note   In release 3.3.0 and later, the 5760 controllers support stateful switchover of access points (AP SSO). For additional information about the AP SSO high-availability functionality and deployment guide, please refer to CT 5760 High Availability AP SSO Deployment Guide, Cisco IOS XE Release 3.3.

N+1 Redundancy

The CT5760 supports N+1 redundancy where the controller is placed in the data center and acts as a backup for multiple WLCs. Each AP is configured with a WLC as the primary and all APs turn to the one redundant controller as secondary.
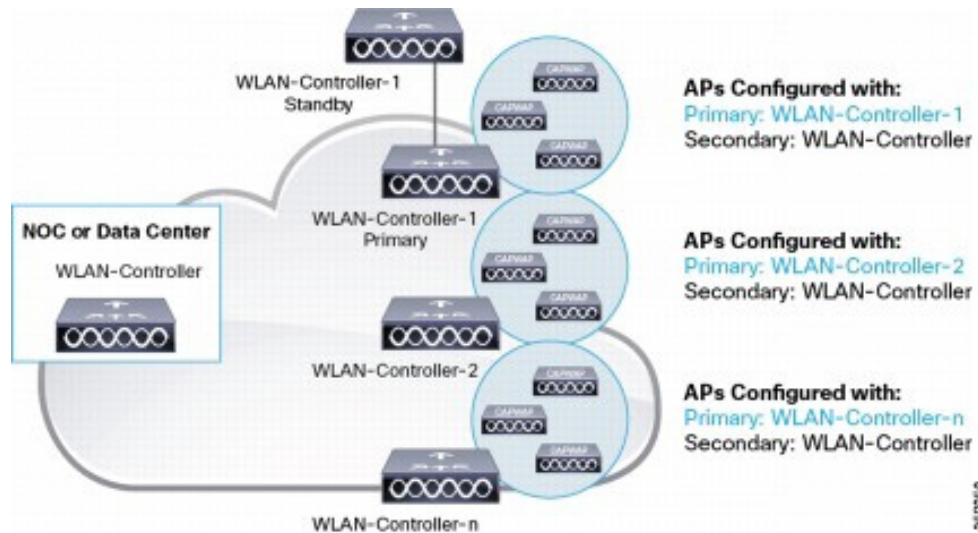
Figure 11-2   N+1 Redundancy

High Availability Configuration

```
#ap name apname controller ?
primaryConfigures primary controller
secondaryConfigures secondary controller
tertiaryConfigures tertiary controller
```

Use this command in order to check the configuration:

```
#show ap name <ap-name> config general
```

In order to reduce the controller failure detection time, you can configure the heartbeat interval between the controller and the AP with a smaller timeout value.

```
#ap capwap timers heartbeat-timeout <1-30>
```

In addition to the option to configure primary, secondary, and tertiary controllers for a specific AP, you can also configure primary and secondary backup controllers for a specific controller. If there are no primary, secondary, or tertiary WLCs configured on the AP side, and a primary and/or secondary backup controller are configured on the controller side (downloaded to the AP), the primary and/or secondary backup controller are added to the primary discovery request message recipient list of the AP. In order to configure a primary backup controller for a specific controller, use this command:

```
(config)#ap capwap backup ?
```

    primaryConfigures primary Controller

    secondaryConfigures secondary Controller

Interface Group

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 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 to which they are connected. 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 acquire VLANs associated from the interface group configured on the WLAN.

You can also configure AAA override for interface groups. This feature extends the current AP group and AAA override architecture where AP groups and AAA override can be configured to override the interface group WLAN to which the interface is mapped. This is accomplished 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.

Configuration of Interface Group

Use this command in order to create VLAN group on WLC:

```
vlan group word vlan-list 100-200
show vlan group
```

Use this command in order to map VLAN group to WLAN:

```
wlan corporate 1 corporate client vlan word
show wlan summary
```

Configure AP Groups

Information about AP Groups

After you create up to 512 WLANs on the controller, you can selectively publish them (using AP groups) to different APs to improve the management of your wireless network. In a typical deployment, all users on a WLAN are mapped to a single interface on the controller. Therefore, all users associated with that WLAN are on the same subnet or VLAN. However, you can choose to distribute the load among several interfaces or to a group of users based on specific criteria such as individual departments (for example, Marketing) through the creation of AP groups. Additionally, these AP groups can be configured in separate VLANs to simplify network administration.

Figure 12-1   Access Point Groups
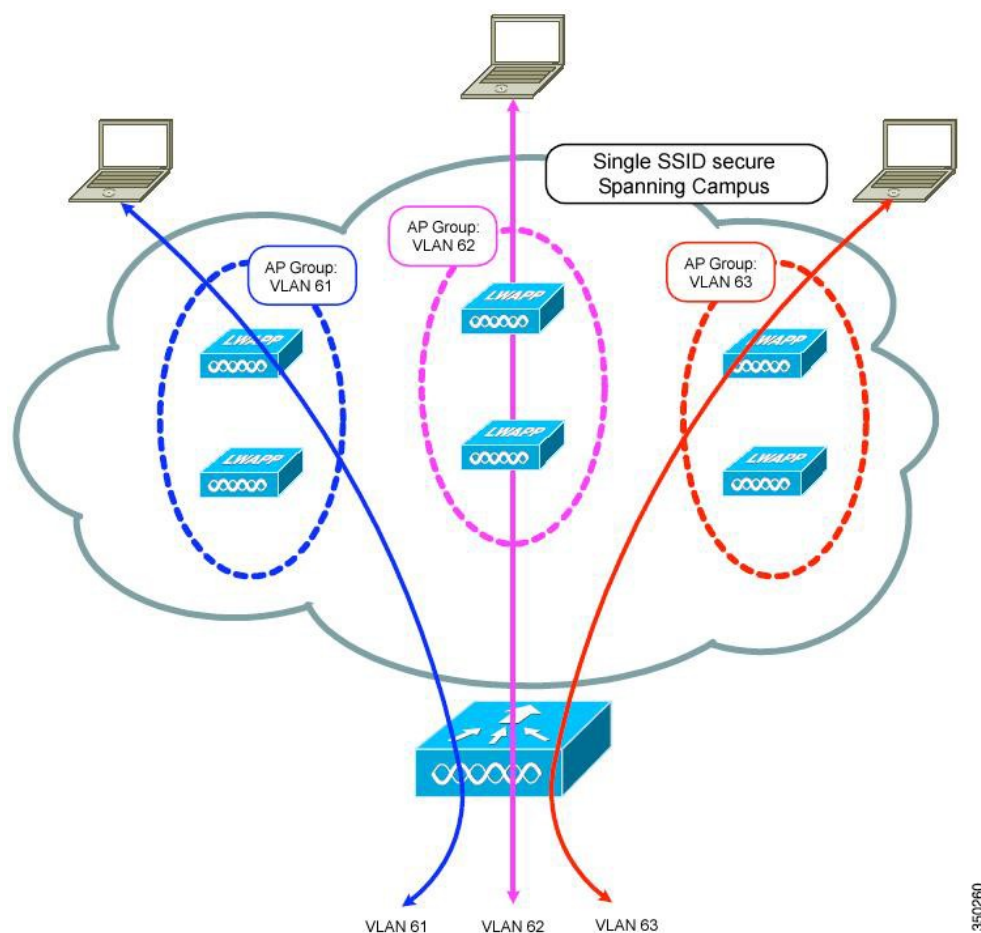
In Figure 12-1, three configured dynamic interfaces are mapped to three different VLANs (VLAN 61, VLAN 62, and VLAN 63). Three AP groups are defined, and each is a member of a different VLAN, but all are members of the same SSID. A client within the wireless SSID is assigned an IP address from the VLAN subnet of which its AP is a member. For example, any user that associates with an AP that is a member of AP group VLAN 61 is assigned an IP address from that subnet.

In the example shown in Figure 12-1, the controller internally treats roaming between APs as a Layer 3 roaming event. In this way, WLAN clients maintain their original IP addresses.

After all APs join the controller, you can create AP groups and assign up to 16 WLANs to each group. Each AP advertises only the enabled WLANs that belong to its AP group. The AP does not advertise disabled WLANs in its AP group or WLANs that belong to another group.

Note   The default access point group can have up to 16 WLANs associated with it. The WLAN IDs for the default access point group must be less than or equal to 16. If a WLAN with an ID greater than 16 is created in the default access point group, the WLAN SSID will not be broadcasted. All WLAN IDs in the default access point group must have an ID that is less than or equal to 16. WLANs with IDs greater than 16 can be assigned to custom AP groups.

Use this command in order to create an AP Group Name:

```
ap group <WORD> wlan <apgroup> vlan < VLAN#>
```

This command maps an AP to an AP Group:

```
ap name <name> ap-groupname <apgroup>
```

AP will reload after the above command is executed.

Multicast Configuration

The default for Multicast forwarding is disabled on the WLC5760 controller. You can enable support for (IPv4 or IPv6) multicast forwarding with this command:

```
(config)#wireless multicast
```

Internet Group Management Protocol (IGMP) Snooping must be enabled on the controller with this command:

```
(config)#ip igmp snooping
```

For IPv6, use this command:

```
(config)#ipv6 mld snooping
```

WLC to AP Forwarding Mode

As soon as multicast is enabled, multicast traffic can be forwarded to the APs. The controller encapsulates the received multicast packet into CAPWAP and then sends this packet to each individual AP. This mode is called Multicast Unicast (MCUC). Alternatively, the controller can encapsulate the multicast packet into another multicast packet, sent once. This mode is more efficient, because only one packet is created on the controller. This mode is called Multicast Multicast (MCMC). To use this mode, you must configure a multicast group on your controller. Each AP connected to the controller subscribes to this multicast group, and can receive the multicast flow. You can enable MCMC and configure the multicast group with this command:

```
(config)#wireless multicast
(config)#ap capwap multicast 239.3.3.3
```

You can revert to the default MCUC mode with the no form in this command:

```
(config)#no ap capwap multicast
```

Just like the legacy solution, multicast groups are created on a VLAN basis. For example, if your WLAN is mapped to VLAN 100, and if a client requests multicast traffic from that WLAN, the controller creates a multicast group identifier (MGID) which maps the multicast source, the multicast address, and the VLAN - in this example, VLAN 100. This is true regardless of the client VLAN in the WLAN.

Multicast VLAN Feature

This example creates two interfaces, and then an interface group maps the two VLANs together:

```
(config)#interface vlan 19
(config-if)#ip address 10.10.19.1 255.255.255.0
(config)#interface vlan 21
(config-if)#ip address 10.10.21.1 255.255.255.0
(config)#vlan group Group19to21 vlan-list 19,21
```

These commands create a WLAN, and map this WLAN to the VLAN group:

```
(config)#wlan open19 4 open19
(config-wlan)# client vlan Group19to21
(config-wlan)#
```

Use the IP Multicast VLAN command that maps multicast traffic to a specific VLAN:

```
(config-wlan)# ip multicast vlan 21
```

The controller uses the VLAN 21 interface to handle multicast traffic for that WLAN.

Note   Once multicast forwarding is configured on the controller, you must also configure your infrastructure for multicast support.

Note   WLC5760 uses IGMP v2. There is no option for the end user to change it.

Broadcast Forwarding

Similar to multicast forwarding, broadcast forwarding is disabled by default (broadcast packets received by the controller are not forwarded to wireless clients). Broadcast forwarding is enabled on a per VLAN basis. You can enable broadcast forwarding for a specific VLAN with this general command:

```
(config)#wireless broadcast vlan 21
```

You can also enable broadcast forwarding for all VLANs, if you do not identify a specific VLAN:

```
(config)#wireless broadcast
```

Then, you can restrict the command by disabling broadcast forwarding for some VLANs:

```
(config)#no wireless broadcast vlan 20
```

Configuration Verification

You can verify multicast in a number of ways. From the controller component, you can display the multicast status, ap multicast mode, and each VLAN's broadcast/non-ip multicast status:

```
#show wireless multicast
```

You can display all (S, G, and V) and the corresponding MGID value:

```
#show wireless multicast group summary
#show ip igmp snooping
# show ip igmp snooping wireless mgid
```

All of these commands are also available for IPv6 MLD monitoring. You must use the ipv6 keyword instead of ip, and mld instead of igmp:

```
show ipv6 mld snooping, show ipv6 mld snooping wireless mgid
```

You can also see all the multicast groups and their active interfaces:

```
#show ip igmp groups
```

In order to see which IGMP version is used and the port associated to the group, use this command:

```
#show ip igmp snooping groups
```

Installing and Upgrading Software Image on a CT5760

Detailed upgrade procedure can be found at
http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/system_management/appendix/swiosfs.html#wp1311040

1. Copy the new image from a USB memory to flash.

```
Controller#copy usbflash0:/ ct5760-ipservicesk9.SSA.03.07.97.EMD.150-7.97.EMD.bin
flash:

Destination filename [ct5760-ipservicesk9.SSA.03.07.97.EMD.150-7.97.EMD.bin]? Copy in
progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

266151060 bytes copied in 36.030 secs (7386929 bytes/sec)

Controller#
```

2. Expand your bundled image from flash by using CLI below for the first install only. If this is not the first install, see Step 5.

```
Controller#software expand file flash:ct5760-ipservicesk9.SSA.03.07.97.EMD.150-
7.97.EMD.bin verbose

Preparing expand operation

[1]: Expanding bundle flash:ct5760-ipservicesk9.SSA.03.07.97.EMD.150-7.97.EMD.bin

[1]: Copying package files

[1]: Package files copied

[1]: Finished expanding bundle flash:ct5760-ipservicesk9.SSA.03.07.97.EMD.150-

7.97.EMD.bin
```

3. Verify the expanded files from flash.

```
Controller#dir flash:

Directory of flash:/

311309-rw-266151060Mar 31 2010 05:58:22 +00:00ct5760-
ipservicesk9.SSA.03.07.97.EMD.150-7.97.EMD.bin

360451-rw-96724320Mar 31 2010 06:00:19 +00:00ct5760- base.SSA.03.07.97.EMD.pkg

360452-rw-1292972Mar 31 2010 06:00:25 +00:00ct5760- drivers.SSA.03.07.97.EMD.pkg

360453-rw-53521356Mar 31 2010 06:00:21 +00:00ct5760- infra.SSA.03.07.97.EMD.pkg

360454-rw-43506528Mar 31 2010 06:00:23 +00:00ct5760-iosd-

ipservicesk9.SSA.150-7.97.EMD.pkg

360455-rw-20646616Mar 31 2010 06:00:22 +00:00ct5760-

platform.SSA.03.07.97.EMD.pkg

360456-rw-50455240Mar 31 2010 06:00:25 +00:00ct5760-
```

```
wcm.SSA.03.07.97.EMD.pkg
360450-rw-1208 Mar 31 2010 06:00:36 +00:00packages.conf
```

4. Configure boot from flash.

```
Controller#conf t
Controller(config)#boot system flash:packages.conf
Controller(config)#end
Controller#
```

5. For future upgrades, enter these commands.

```
software install file flash:ct5760-ipservicesk9.SSA.03.08.58.EMP.150-
8.58.EMP3.bin verbose
Preparing install operation ...
[1]: Starting install operation
[1]: Expanding bundle flash:ct5760-ipservicesk9.SSA.03.08.58.EMP.150-
8.58.EMP3.bin
[1]: Copying package files
[1]: Package files copied
[1]: Finished expanding bundle flash:ct5760-ipservicesk9.SSA.03.08.58.EMP.150-
8.58.EMP3.bin
[1]: Verifying and copying expanded package files to flash:
[1]: Verified and copied expanded package files to flash:
[1]: Starting compatibility checks
[1]: Finished compatibility checks
[1]: Starting application pre-installation processing
[1]: Finished application pre-installation processing
[1]: Old files list:
Removed ct5760-base.SSA.03.08.58.EMP1.pkg
Removed ct5760-drivers.SSA.03.08.58.EMP1.pkg
Removed ct5760-infra.SSA.03.08.58.EMP1.pkg
Removed ct5760-iosd-ipservicesk9.SSA.150-8.58.EMP1.pkg
Removed ct5760-platform.SSA.03.08.58.EMP1.pkg
Removed ct5760-wcm.SSA.03.08.58.EMP1.pkg
[1]: New files list:
Added ct5760-base.SSA.03.08.58.EMP3.pkg
Added ct5760-drivers.SSA.03.08.58.EMP3.pkg
Added ct5760-infra.SSA.03.08.58.EMP3.pkg
Added ct5760-iosd-ipservicesk9.SSA.150-8.58.EMP3.pkg
Added ct5760-platform.SSA.03.08.58.EMP3.pkg
Added ct5760-wcm.SSA.03.08.58.EMP3.pkg
[1]: Creating pending provisioning file
[1]: Finished installing software.New software will load on reboot.
[1]: Committing provisioning file
[1]: Do you want to proceed with reload? [yes/no]:yes
```
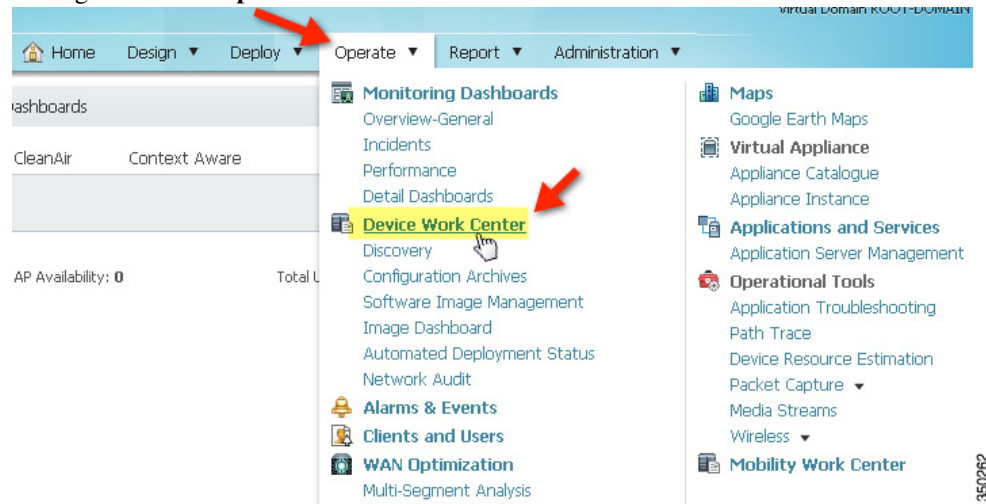
6. Reset the system.

Adding WLC to Prime
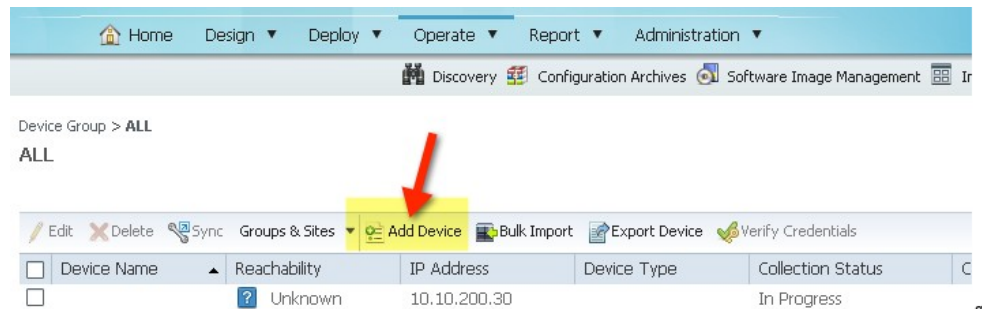
Complete these steps to add controllers:

1. Login to Cisco Prime.

2. Navigate to **PI > Operate > Device Work Center**.

3. Click **Add Device**.

4. Enter CT5760 parameters:

a. IP address - CT5760 mgt IP

b. Read-Write SNMP string (private)

c. Telnet credentials

5. Confirm Cisco Prime Infrastructure discovery of the CT5760 - if reachable and successful, status shows complete with the correct device type.

6. Explore Cisco Prime Infrastructure GUI in management of CT5760, for example, client statistics, details, reports, and so on.

Application Visibility and Flexible Netflow

With the 5760 and 3850 IOS-XE release 3.3, Application Visibility support was introduced on both platforms. Detailed Deployment Guide for Application Visibility can be found at: Converged Access CT 5760 AVC Deployment Guide, Cisco IOS XE Release 3.3

Flexible Netflow

Cisco IOS® Flexible NetFlow is the next-generation in flow technology. It optimizes the network infrastructure, which reduces operation costs and improves capacity planning and security incident detection with increased flexibility and scalability. The ability to characterize IP traffic and identify its source, traffic destination, timing, and application information is critical for network availability, performance, and troubleshooting. When IP traffic flows are monitored, this increases the accuracy of capacity planning and ensures that resource allocation supports organizational goals. Flexible NetFlow helps you determine how to optimize resource usage, plan network capacity, and identify the optimal application layer for QoS. It plays a vital role in network security by the detection of Denial of Service (DoS) attacks and network-propagated worms.

Here are the commands in order to configure Flexible Netflow:

```
!
flow record IPv4flow
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match flow direction
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
!
!
flow exporter IPv4export-1
destination 10.1.1.6 (IP address of your Netflow Collector. It should be v9 netflow.)
transport udp 2055
!
!
```

```
flow monitor IPv4flow (you can view the flows on the switch using CLI if netflow Collector
is not available)
description Monitor all IPv4 traffic
exporter IPv4export-1
cache timeout active 30
record IPv4flow
!
```

Here are the Show Commands:

```
show flow monitor name monitor-name cache
show flow record
show flow-sampler
show flow monitor
```

For additional information on Netflow Configuration, please refer to Cisco Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches).

Service Discovery Gateway(mDNS Gateway)

Cisco's Service Discovery Gateway is an IOS component that implements the Zeroconf suite of technologies in IOS. Zeroconf is a widely used standard for plug-and-play service discovery, including Apple Bonjour® services. Zeroconf has been designed with the local network in mind and operates only in its local network. However, due to the huge success of the BYOD device in enterprises and educational institutions, the need to support Zeroconf enabled services beyond the boundaries of a local subnet has become top of mind.

Cisco's Service Discovery Gateway allows for controlled and secure access to services and devices across subnets. It listens to service announcements on all configured network segments and builds a cache of services and addresses. It proxies these requests to other segments and can also apply filters based on various service attributes. These filters can limit what services will be requested or advertised.

For detailed information about Service Discovery Gateway feature configuration, please refer to Service Discovery Gateway Deployment Guide, Cisco IOS-XE Release 3.3.

CHAPTER **18**

QoS Configuration

The introduction of Cisco IOS® software on the WLC5760 controller brings a wide-range of wired/wireless QoS supports and capabilities:

- Consistent configuration CLI for both wired and wireless QoS through Modular QoS CLI
- Granular QoS policies per AP, SSID, radio, and client
- Fair bandwidth allocation across wireless clients on an AP
- Leverages proven Cisco IOS® and ASIC technology to provide line rate performance

Enabling QoS

Based on the Modular QoS CLI model, QoS is enabled by default on the WLC5760. Explicit marking of traffic is required in order to modify Class of Service (CoS) or Differentiated Services Code Point (DSCP) values for traffic from and to wired ports. Traffic from wireless to wireless ports or wireless to wired ports is considered untrusted. Though QoS is globally enabled if traffic passes through an SSID, it must be marked or trusted specifically, or all QoS values (DSCP, CoS) will be set to default (0).

Managing QoS

QoS policies on the WLC5760 are provisioned in a couple of ways.

- Via CLI
- Via AAA

The configuration examples herein demonstrate attachment of policies via CLI. AAA configuration of policies is shown later in this specific section. The QoS policy name, not the actual QoS policy, is passed from the AAA server to the WLC5760 platform. Due to this fact, the QoS policy configuration must be local to the platform regardless of which method is used to manage QoS on the platform.

Marking Models

The WLC5760 supports several marking models:

- Per-Port Marking (wired)
- Per-Client Marking (wireless)

- Per-SSID Marking (wireless)

- Per-VLAN Marking (wired)

From a unified policy standpoint, the Per-Port and Per-Client marking policy can be synonymous but applied to a different target (wireless client, physical client port). Each model is discussed herein.

Per-Port or Per-Client Marking

Similar to the Catalyst 4500, the Per-Port or Per-Client marking model matches VoIP on UDP/RTP ports 16384-32767. The signaling traffic is matched on SCCP ports (TCP 2000-2002), as well as on SIP ports (TCP/UDP 5060-5061). Transactional data traffic are matched on various ports. Unlike the Catalyst 3750-E examples, no explicit default class is required, because the implicit class default performs policy actions (such as marking or policing) on the WLC3850/5760.

!ACL configuration

```
ip access-list extended VOIP
remark Voice
permit udp any any range 16384 32767
ip access-list extended SIGNALING
remark SCCP
permit tcp any any range 2000 2002
remark SIP
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended TRANSACTIONAL-DATA
remark HTTPS
permit tcp any any eq443
remark ORACLE-SQL*NET
permit tcp any any eq1521
permit udp any any eq1521
remark ORACLE
permit tcp any any eq1526
permit udp any any eq1526
permit tcp any any eq1575
permit udp any any eq1575
permit tcp any any eq1630
permit udp any any eq14002
permit udp any any eq14006
```

!Class-map configuration

```
class-map match-all VOIP
match access-group name VOIP
class-map match-all SIGNALING
match access-group name SIGNALING
class-map match-all TRANSACTIONAL-DATA
```

```
match access-group name TRANSACTIONAL-DATA
```

!Per-Port or Per-Client Ingress Marking Policy-map Configuration

```
policy-map PER-PORT-MARKING
class VOIP
set dscp ef
class SIGNALING
set dscp cs3
class TRANSACTIONAL-DATA
set dscp af21
class class-default
set dscp default
```

!Policy attachment to interfaces

!Wireless Clients associating to WLAN OPEN

```
wlan OPEN 2 OPEN
band-select
client vlan 3
ip dhcp server 10.17.1.9 load-balance
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
service-policy client input PER-PORT-MARKING
session-timeout 1800
no shutdown
```

Policing Models

Several policing models are available on the WLC5760.

- Per-Port Policing
- Per-Client Policing
- Per-SSID Policing

Policing is offered in a number of ways and can be used in a hierarchical fashion as will be shown in the instance of client-based policies. In this instance, a policer can be used bi-directionally to police a client's traffic as an aggregate, as well as specific traffic classes associated with the client, such as voice.

Here is an example of FLAT Per-Port or Per-Client Policing configuration:

!ACL configuration

```
ip access-list extended VOIP
remark Voice
```

```
permit udp any any range 16384 32767
ip access-list extended SIGNALING
remark SCCP
permit tcp any any range 2000 2002
remark SIP
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended TRANSACTIONAL-DATA
remark HTTPS
permit tcp any any eq443
remark ORACLE-SQL*NET
permit tcp any any eq1521
permit udp any any eq1521
remark ORACLE
permit tcp any any eq1526
permit udp any any eq1526
permit tcp any any eq1575
permit udp any any eq1575
permit tcp any any eq1630
permit udp any any eq14002
permit udp any any eq14006
```

!Class-map configuration

```
class-map match-all VOIP
match access-group name VOIP
class-map match-all SIGNALING
match access-group name SIGNALING
class-map match-all TRANSACTIONAL-DATA
match access-group name TRANSACTIONAL-DATA
```

!Per-Port or Per-Client Ingress Policing Policy-map Configuration

```
policy-map PER-PORT-POLICING
class VOIP
set dscp ef
police 128000conform-action transmitexceed-action drop
class SIGNALING
set dscp cs3
police 32000conform-action transmitexceed-action drop
class TRANSACTIONAL-DATA
set dscp af21
class class-default
set dscp default
```

!Policy attachment to interfaces

!Wireless Clients associating to WLAN OPEN Policed bi-directionally

```
wlan OPEN 2 OPEN
band-select
client vlan 3
ip dhcp server 10.17.1.9
load-balance
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
service-policy client input PER-PORT-POLICING
service-policy client output PER-PORT-POLICING
session-timeout 1800
```

Here is an example of Hierarchical Per-Client Policing configuration:

!Wireless Client Policy-map Client Aggregate policed to 2Mbps, Voice as a subset to 128k, signaling 32k

```
policy-map AGG-POLICE
class class-default
police 2000000 conform-action transmit exceed-action drop
service-policy PER-PORT-POLICING
policy-map PER-PORT-POLICING
class VOIP
set dscp ef
police 128000 conform-action transmit exceed-action drop
class SIGNALING
set dscp cs3
police 32000 conform-action transmit exceed-action drop
class TRANSACTIONAL-DATA
set dscp af21
class class-default
set dscp default
```

Wireless Queuing

Wireless queuing by default provides a queuing policy. This policy is shown in the show run command and contains a static traffic class, which cannot be modified. This class is attached to multicast non-real-time traffic associated with the wireless port only. In order to enable the additional queues on egress of the wireless port, the static policy-map port_child_policy must be modified to include the three additional classes. Priority queuing is supported for two of the queues, while class-default makes up the rest of the queue.

Here is an example of egress wireless queuing policy:

```
policy-map port_child_policy
```

```
class non-client-nrt-class
bandwidth remaining ratio 7
class RT1
priority level 1
police 6400000 conform-action transmit exceed-action drop
class RT2
priority level 2
police 19200000 conform-action transmit exceed-action drop
class class-default
bandwidth remaining ratio 63
```

In this example, the policy limits as an aggregate the priority queues RT1 and RT2 to an aggregate policed rate as shown. The policy also provides the additional non-real-time classes with a bandwidth associated with the bandwidth remaining ratio command. This ratio of available bandwidth is provided to the non-client-nrt (or multicast and non-client non-real-time traffic queue) and class-default queues.

Wireless MultiMedia Configuration

Wireless MultiMedia (WMM) separates traffic types into four QoS access categories: background, best effort, video, and voice.

```
(config) wlan <your WLAN name> (config-wlan) shutdown
(config-wlan) broadcast
(config-wlan) radio all (to enable this WLAN configuration on both AP radios and all Wi-Fi
protocols)
(config-wlan) wmm require
(config-wlan) no security <your Current security setting>
(config-wlan) no shutdown
```

WMM configuration options include:

- WMM Required - only WMM enabled clients can join the WLAN

- WMM Optional - both non-WMM clients and WMM enabled client can join the WLAN

  – WMM enabled clients transmit all packets with WMM QoS header.

  – Non-WMM clients transmit no packets with WMM QoS header.
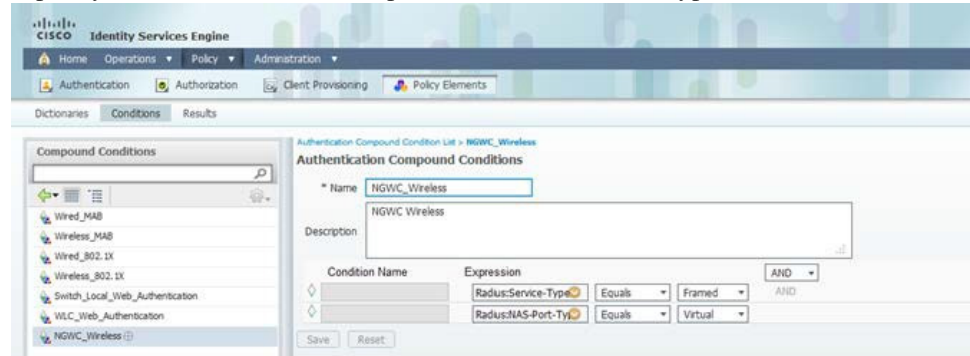
Note   Note that non-WMM cannot receive packets from the AP that have a WMM QoS header.

  – All packets from and to non-WMM clients are sent with best effort Wi-Fi channel access.
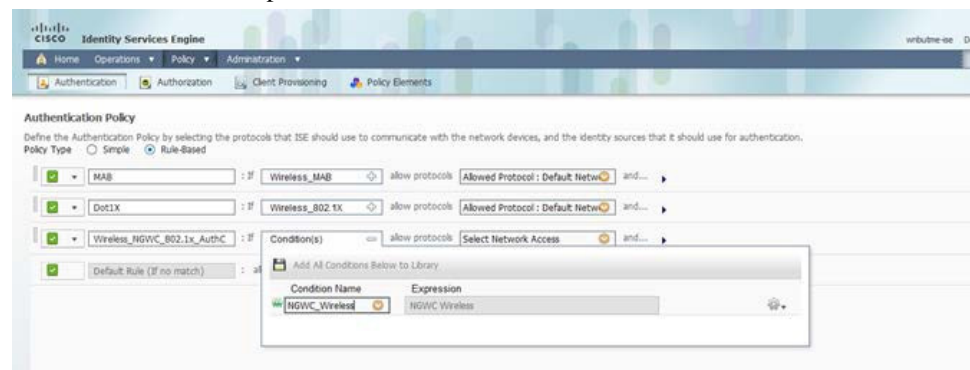
Configure ISE in order to Authenticate and Push QoS Policies

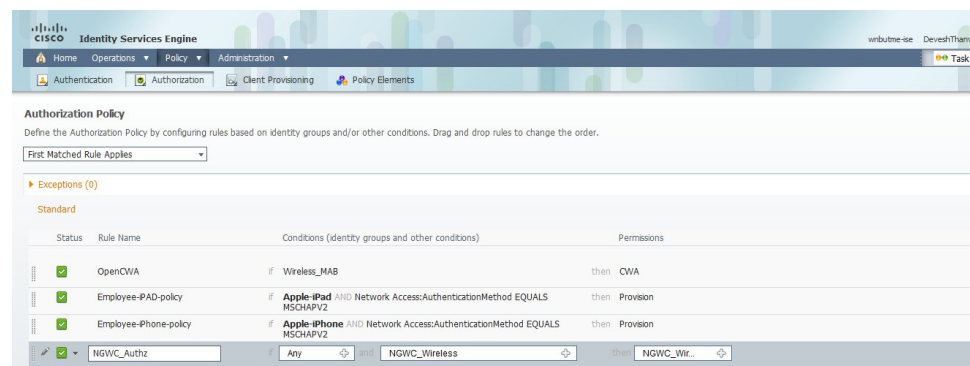Complete these steps to authenticate and push QoS policies.

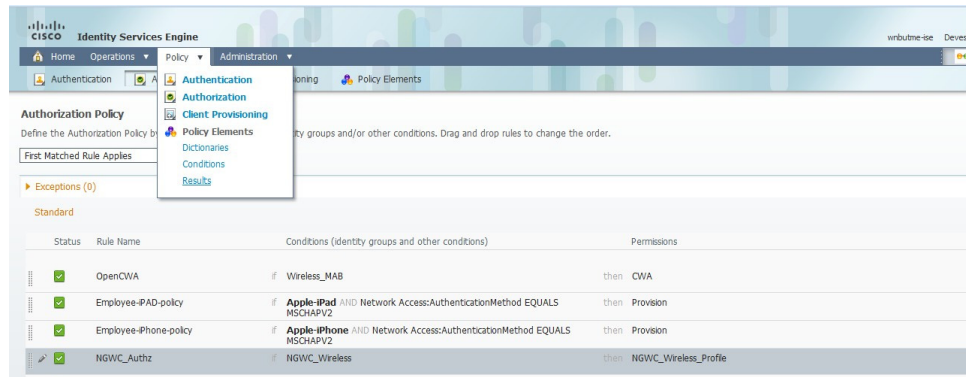**1.** Specify a condition where the expression is of NAS-Port-Type **Virtual**.

2. Create authentication parameters.

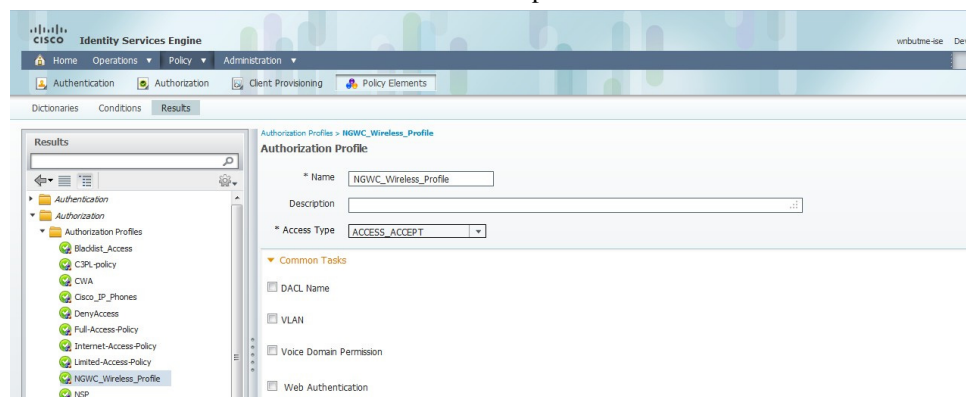**3.** Authorization - Define result and use same condition.

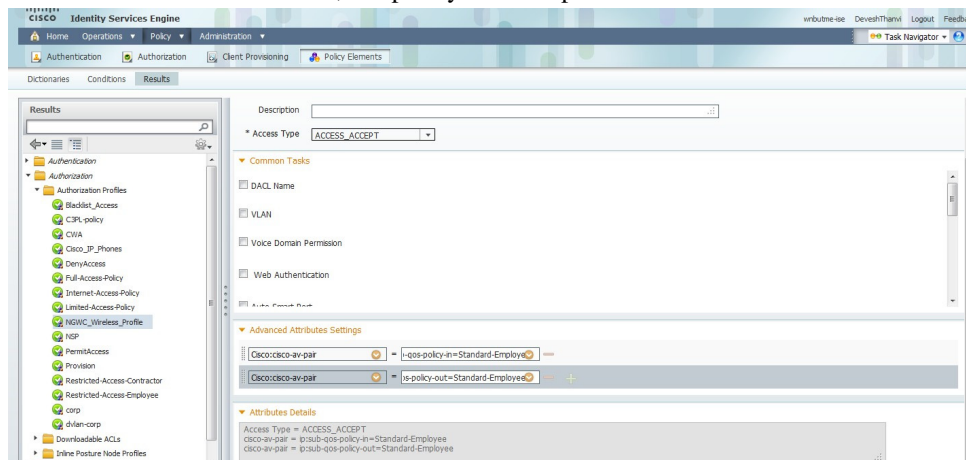4. Go to **Policy > Results**.

350268

5. Choose Cisco-AV-Pair at bottom shown in Step 6.

350269

6. Modify **Advanced Attribute Settings** with the **Cisco av-pair name**, **ip:sub-qos-policy-in**, or **ip:sub-qos-polify-out**, plus name of QoS policy local to the WLC3850/5760. When clients are associated and authenticated, the policy name is pushed to the WLC3850/5760.

350270

Cisco IOS® Tool Command Language Scripting

With the introduction of the Cisco IOS® software on the WLC5760 controller, users can now implement the Tool Command Language (TCL) scripting feature on the controller.