Converged Access Deployment Guide

First Published: January 28, 2016

Last Modified: February 22, 2016

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

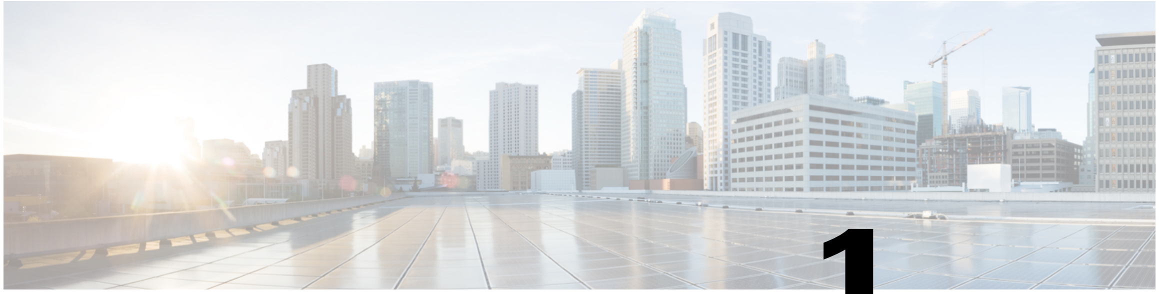
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS



CHAPTER 1

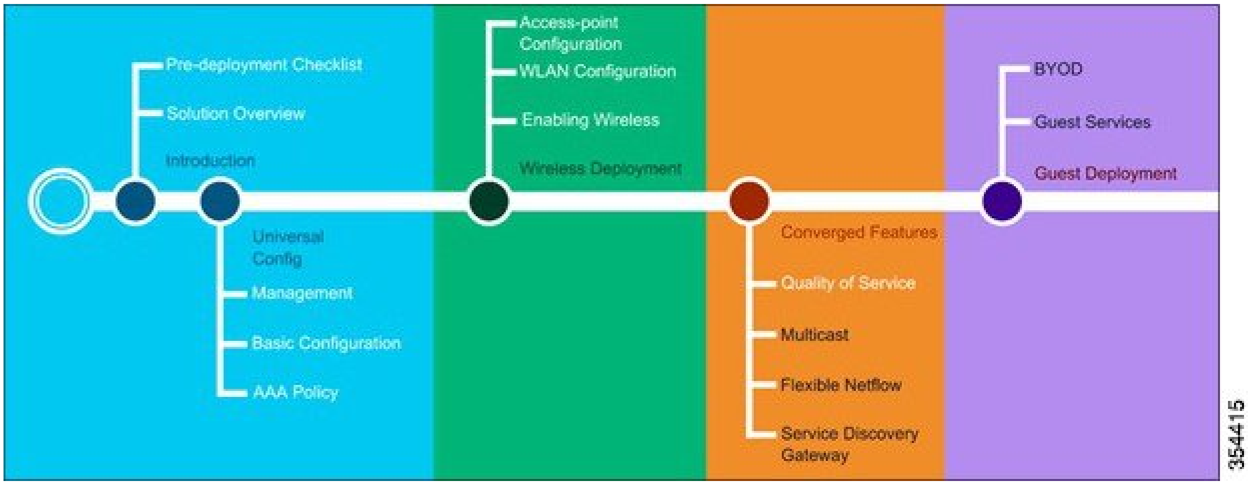
Converged Access: Solution Overview

Converged access represents an architectural change in the way wired and wireless networks are deployed. A converged access network allows policy decisions to be enforced at the network edge, potentially minimizes unnecessary traffic backhaul, and simplifies network management by allowing one policy to be used for both wired and wireless traffic.

This chapter provides step-by-step instructions to deploy a converged access network with the commonly recommended features and configurations. This guide provides information about how to deploy an operating converged access network.

The following figure represents the converged access workflow. The items in white are the topics covered in this guide. The items in dark gray are the work-in-progress topics that will be added to the guide subsequently.

Figure 1: Converged Access Roadmap



Supported Platforms

- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco 5760 Wireless LAN Controller
- Cisco Catalyst 4500E Supervisor Engine 8E

The Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches provide converged wired and wireless network access for devices. Choose a specific switch based on the number of ports and uplink type and capacity required, type of ports, scalability requirement, and Power of Ethernet (PoE) capability needs of the network. The choice of the network uplink module is optional and depends on network requirements.

Note On Cisco Catalyst 4500 Series Switches, the 7R-E chassis should be hardware revision 2 or higher to house a Supervisor Engine 8E.

Note Install boot is a prerequisite on Cisco Catalyst 4500 Series Switches, to support wireless.

Tip The following scale requirements serve as a baseline guide when choosing the platform:

- The Cisco Catalyst 3850 Series Switches support up to 100 access points and 2000 wireless clients on each switching entity (switch or stack).
- The Cisco Catalyst 3650 Series Switches support up to 50 access points and 1000 wireless clients on each switching entity (switch or stack).
- The Cisco Catalyst 4500E Supervisor Engine 8E supports up to 100 acess points.
- PoE-based platforms should be used since wireless access points can be powered using inline power. This simplifies network deployment.

Note For more information about the Cisco Catalyst Series switches, see the Release Notes document at: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3e/release_notes/OL3262101.html

Recommended Software

The recommended software for Converged Access Deployment Guide is Cisco IOS XE Release 3.7.3 E.

Note The support for Supervisor Engine 8E on Cisco Catalyst 4500 Series Switches was added in Cisco IOS XE Release 3.8 E.
On Cisco Catalyst 4500E, the 7R-E chassis should be hardware revision 2 or higher to house a Supervisor Engine 8E.

Note Starting with Cisco IOS 12.2(31)SGA, ISSU is supported on Cisco Catalyst 4500 Series Switches. For more information, refer to Catalyst 4500 Series Switch Software Configuration Guide, IOS XE 3.8.0E and IOS 15.2(4)E

The latest software releases are available on the Cisco website at:

http://software.cisco.com/download/navigator.html.

We recommend that you read the relevant Release Notes before upgrading to a given software release.

Prerequisites for Converged Access Deployment Guide

- Knowledge about converged access as a deployment model is essential. For more information about the overall solution and offering, see the following links:
  - http://www.cisco.com/c/en/us/solutions/enterprise-networks/unified-access/index.html
  - http://www.cisco.com/c/en/us/products/switches/catalyst-3850-series-switches/white-paper-listing.html
- Knowledge about converged access as a deployment model for delivery of wired and wireless services.
- The person performing the deployment should be a Cisco Certified Network Associate (CCNA), and possess knowledge about wired and wireless services.

CLI and Console Access

Before you configure a 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). A controller has both EIA and 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, 8 data bits, 1 stop bit, and no parity. The console ports do not support hardware flow control. Choose a serial baud rate of 9600 or 115200.

PC with Supported Browser Version

The GUI must be used on a PC that is running Windows 8, Windows 7, or Windows 2000 SP4 (or later releases).

The following is a list of supported browser versions:

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

Tip Web GUI is supported from Cisco IOS XE Release 3.2.2 onwards.

Concepts and Definitions

This section provides you with brief descriptions of the key phrases used in converged access deployment.

Mobility Agent

Mobility Agent is the default mobility mode that is configured on a Cisco Catalyst switch when it is shipped from the factory. In this mode, the switch is capable of terminating Control and Provisioning of Wireless Access Points (CAPWAP) tunnels from access points, thereby providing connectivity to wireless clients. When operating as a Mobility Agent, the switch maintains local wireless client databases, and enforces security and quality of service (QoS) policies for wireless clients and access points at the network edge. An IP Base license is required for the Mobility Agent.

Mobility Controller

When acting as a Mobility Controller, a Cisco Catalyst switch can perform all the typical Mobility Agent tasks, in addition to mobility coordination, radio resource management, and Cisco CleanAir coordination within the associated mobility subdomain. The minimum license level required to run a switch as mobility controller is IP Base.

Switch Peer Group

A switch peer group is a logical entity comprising of multiple Mobility Agents acting as a group under a Mobility Controller, within a mobility subdomain. Configuring a switch peer group facilitates fast roaming between converged access switches within the group, and reduces unnecessary roaming traffic across the rest of the mobility subdomain. Mobility Agents within the same switch peer group form a full–mesh topology of CAPWAP tunnels between peer Mobility Agents.

Mobility Group

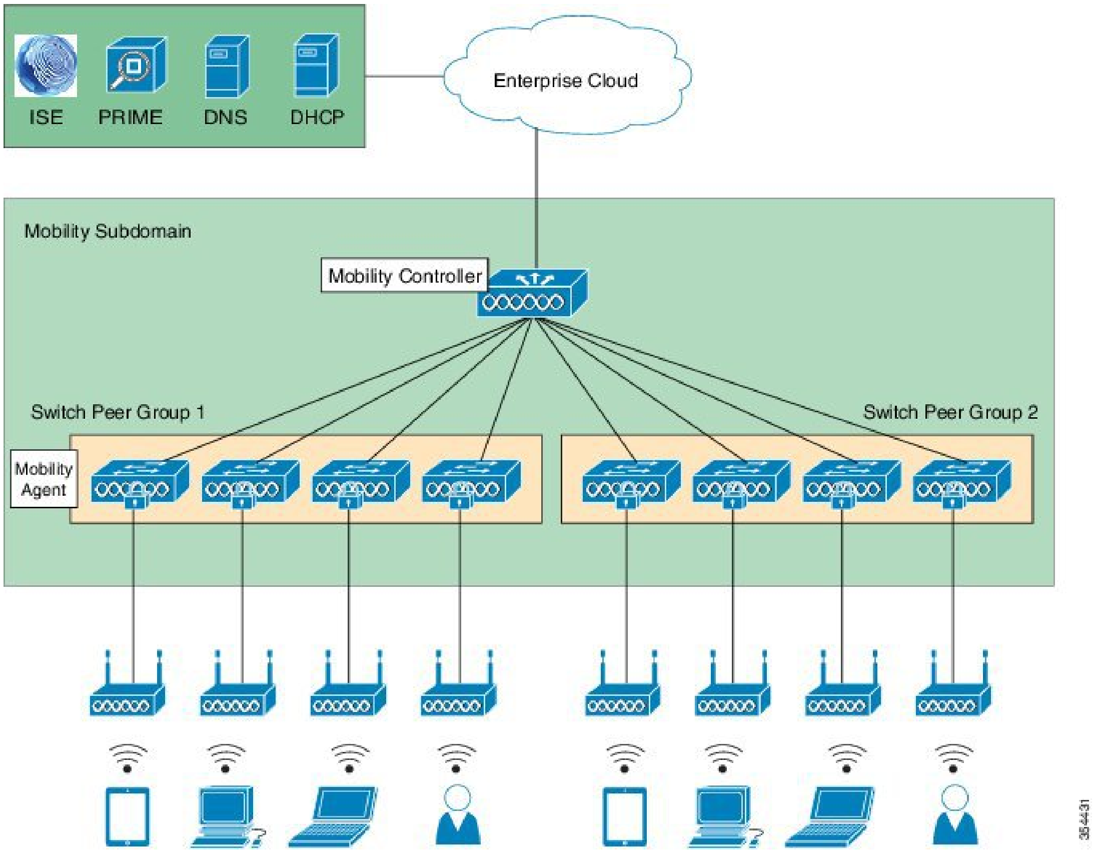
Mobility group is a group of all the wireless LAN controllers in a network that share a mobility group name. These controllers share mobility context, client state, and controller-loading information. Additionally, controllers in the same mobility group can forward data traffic to one another, which enables intercontroller wireless LAN roaming and controller redundancy.

Converged Access Topology Example

The following figure shows a typical converged access deployment scenario. The Mobility Controller is stacked for redundancy purposes. The Mobility Controller stack connects to eight Mobility Agents, which service wireless clients. The eight Mobility Agents are divided equally into two different switch peer groups (SPG). The entire setup belongs to a single mobility subdomain.

Note The access points connect directly to mobility agents, thus terminating CAPWAP tunnels on the Mobility Agents.

Figure 2: Converged Access Deployment Scenario



Supported Platform Product Identifiers

The following table lists the supported platform product identifiers (PIDs), provides information about the license level for a given PID, as well as a description of the product.

Table 1: Product Identifiers for Supported Platforms

Switch Model	Cisco IOS Image	Description
WS-C3850-24P-S	IP Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, and IP Base feature set
WS-C3850-48P-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set
WS-C3850-48F-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, and IP Base feature set
WS-C3850-24PW-S	IP Base	Cisco Catalyst 3850 24-port PoE IP Base
WS-C3850-48PW-S	IP Base	Cisco Catalyst 3850 48-port PoE IP Base
WS-C3850-24P-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, and IP Services feature set
WS-C3850-48P-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, and IP Services feature set
WS-C3850-48F-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, and IP Services feature set
WS-3850-24U-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Cisco Universal Power over Ethernet (UPOE) ports,1 network module slot, and 1100-W power supply
WS-3850-48U-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Cisco UPOE ports,1 network module slot, and 1100-W power supply
WS-X45-SUP8-E	IP Base	Cisco Catalyst 4500E Series Unified Access Supervisor, 928 Gbps

Supported Wireless Access Point Models

The following table lists the access point models that are supported with the converged access solution. Access point models should be chosen based on the scale, wireless client count, and features leveraged.

Table 2: Supported Wireless Access Point Models

Product Family	AP Model
Cisco Aironet 3700 Series	• AIR-CAP3702I • AIR-CAP3702E
Cisco Aironet 3600 Series	• AIR-CAP3702I • AIR-CAP3702E
Cisco Aironet 3500 Series	• AIR-CAP3501E • AIR-CAP3501I • AIR-CAP3502E • AIR-CAP3502I
Cisco Aironet 2700 Series	• AIR-CAP2702I-x-K9 • AIR-CAP2702E-x-K9
Cisco Aironet 2600 Series	• AIR-CAP2602E • AIR-CAP2602I
Cisco Aironet 1700 Series	• AIR-CAP1702I- x-K9 • AIR-CAP1702I- xK910
Cisco Aironet 1600 Series	• AIR-CAP1602E • AIR-CAP1602I
Cisco Aironet 1530 Series	• AIR-CAP1532I-x-K9 • AIR-CAP1532E-x-K9

Cisco Aironet 1260 Series	• AIR-LAP1261N • AIR-LAP1262N • AIR-AP1261N • AIR-AP1262N
Cisco Aironet 1140 Series	• AIR-AP1141N • AIR-AP1142N • AIR-LAP1141N • AIR-LAP1142N
Cisco Aironet 1040 Series	• AIR-AP1041N • AIR-AP1042N • AIR-LAP1041N • AIR-LAP1042N
Cisco Aironet 700 Series	• AIR-CAP702W-x-K9 • AIR-CAP702I-x-K9 • AIR-CAP702I-xK910

CHAPTER 2

Converged Access: Predeployment Checklist

This chapter provides information about the predeployment checklist that details the various components that are required for successfully deploying converged access, especially in the context of a branch deployment. While planning for converged access, the switch can act either as a Mobility Controller, Mobility Agent, or both. Multiple Mobility Agent switches can be grouped under a single Switch Peer Group (SPG) to form a mobility subdomain.

Predeployment Checklist

Note Before proceeding with the deployment, we recommend that you plan and design your mobility architecture and assign roles to each participating device in the mobility architecture. You must configure at least one Mobility Controller.

For more information about overall switch installation, refer to Catalyst 3850 Switch Hardware Installation Guide.

The predeployment checklist provides the necessary information for deploying a switch at the access layer. In the access layer, a Cisco Catalyst 3850 Series Switch or Cisco Catalyst 3650 Series Switch must be configured as a Mobility Controller or a Mobile Agent, for it to provide all the functionalities of a full wireless controller.

Tip On Cisco Catalyst 3850 Series and Cisco Catalyst 3650 Series Switches, stack the devices to achieve high availability and redundancy.

Table 3: Predeployment Checklist

Check List Item	Notes
Hardware	

Cisco Catalyst 3850, Cisco Catalyst 3650 Series switches	Role can be Mobility Controller or Mobility Agent.
Any supported AP	See Chapter 1, Solution Overview for information about supported APs.
Infrastructure	
Radius Server for Authentication	Cisco Identity Services Engine.
DHCP Server — For AP and Client IP addresses	External or Cisco IOS-XE DHCP Server
DNS Server	Any standard DNS Server
NTP Server	Any standard NTP Server
Software	
Cisco IOS-XE image	See Chapter 1, Solution Overview for information about software support.
License Level — IPBase or IPServices	See Chapter 4, Basic Configuration for information about licensing.
License	
AP licenses	See Chapter 6, Enabling Wireless for procedure related to license activation.

Initial Configuration Values Checklist

Use the following table to document the values that have to be configured before deployment:

Table 4: Initial Configuration Values Checklist

Check List Item	**Value**
Hostname	
DHCP Server IP Address	
Domain Name System (DNS) Server IP Address	
Network Time Protocol (NTP) Server IP Address	
TFTP Server Address	
Network Management IP Address	
Default Gateway IP Address	
RADIUS Server IP Address	
RADIUS Server Key	

Secure Shell (SSH) Login Credentials	
Wireless Management VLAN	
Wireless Management Interface IP Address	
WLAN Profile Names	
Wireless Client VLAN	

CHAPTER 3

Converged Access: Management

This chapter describes the switch configuration that is required to enable access for Web GUI and Cisco Prime.

You can manage converged access platforms using the following methods:

- Web GUI–A web browser or GUI is built into each switch.
- Cisco Prime–Cisco Network management software
- Simple Network Management Protocol (SNMP)
- CLI

Web GUI Access

The Web GUI uses HTTPS, by default. However, you can configure HTTP access using the **ip http server** command in global configuration mode.

To access the Web GUI, configure an IP address and a user with privilege 15. Configure an IP address on the management port, on a regular interface, or a Switch Virtual Interface (SVI); this IP address should be reachable through the network.

Note For information about configuring IP on the management interface, see Chapter 4, Basic Configuration.

To create a user with privilege level 15 and to use the credentials from an authentication server, use the **username user_name privilege 15 password password** command in global configuration mode.

For Web GUI access, perform the following procedure:

Step 1 Open a browser, type your management IP address, and press **Enter**.

Step 2 Enter the configured username and password.

Step 3 On the Home window, click the **Wireless Web GUI** hyperlink.
The Wireless Web GUI home page is displayed.

Converged Access Web GUI

The Web GUI supports the following features:

- The following tasks can be performed from the Configuration tab:
  - Configure a switch for all initial operations using the web Configuration wizard. The wizard allows you to configure user details, management interface, and so on.
  - Configure system, internal DHCP server, management, and mobility management parameters.
  - Configure the switch, WLAN, and radios.
  - Configure and set security policies on the switch.
  - Access the software management commands of the operating system.

- The Configuration wizard–After the initial configuration of an IP address and a local username and password, or authentication through an authentication server (privilege 15), the wizard provides a method to complete the initial wireless configuration.

  Start the wizard by choosing **Configuration** > **Wizard**, and then configure the following:
  - Admin Users
  - SNMP System Summary
  - Management Port
  - Wireless Management
  - RF Mobility and Country Code
  - Mobility Configuration
  - WLANs
  - 802.11 Configuration
  - Set Time

- The Monitor tab displays the following information:
  - Summary details of switch, clients, and access points.
  - All radio and AP join statistics.

  - ◦ Air quality on access points.
  - ◦ List of all the Cisco Discovery Protocol neighbors on all the interfaces and the Cisco Discovery Protocol traffic information.
  - ◦ All the rogue access points based on their classification — friendly, malicious, ad hoc, classified, and unclassified.

- The Administration tab enables you to configure system logs.

Enabling Cisco Prime

To enable Cisco Prime, enable SNMP.

Enabling SNMP v2

To enable SNMP on a switch, configure SNMPv2 or SNMPv3. You can configure read-only or read-write community strings, depending on the requirement.

To configure a Read Only (RO) SNMP community string, use the following command:

```
Device# configure terminal
Device(config)# snmp-server community name RO
Device(config)# end
```

To configure a Read Write (RW) SNMP community string, use the following command:

```
Device# configure terminal
Device(config)# snmp-server community name RW
Device(config)# end
```

To check the SNMP community string, use the following command:

```
Device# show running-config | in snmp-server community
```

Enabling SNMP v3

To enable SNMP v3, perform the following procedure:

Step 1 To create a new group and select a security model, use the following commands:

```
Device# configure terminal
Device(config)# snmp-server group grp-name v3 privilege write write_name
Device(config)# end
```

Step 2 To create a user account, use the following commands:

```
Device# configure terminal
Device(config)# snmp-server user user-name-grp-name v3 auth md5 password privilege aes 128 password
Device(config)# end
Configuring snmpv3 USM user, persisting snmpEngineBoots. Please Wait...
```

Step 3 To verify SNMPv3 configuration, use the following commands:

```
Device# show running-config | in snmp-server group
Device# show snmp user
Device# show snmp group
```

CHAPTER 4

Converged Access: Basic Configuration

This chapter provides information about the basic configuration of the wired features on a device. For information about the deployment of the wired features, refer to the *Cisco Wired LAN Technology Design Guide*.

Concepts and Definitions

The following concepts and terms are used throughout this guide:

NTP

Network Time Protocol (NTP) is a networking protocol for clock synchronization between devices in a network. NTP is implemented using User Datagram Protocol (UDP), which in turn runs over an IP. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices within a millisecond of one another.

SSH

Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote command line login, remote command execution, and other secure-network services between two networked computers. It connects an SSH server and SSH client through a secure channel over a network that is not secure. SSH is typically used to log in to remote machines and execute commands.

Remote shell protocols send information, such as password, in plaintext making the networks susceptible to interception and disclosure. SSH is designed as a replacement for Telnet and other remote shell protocols that are not secure.

VLAN

A VLAN is a switched network that is logically segmented by function, project team, or application, irrespective of the physical location of users. A VLAN has the same attributes as the physical LAN. However, you can group the end stations in a VLAN even if they are not physically located on the same LAN segment. A switch module port can belong to a VLAN, but the unicast, broadcast, and multicast packets are forwarded only to the end stations in the VLAN. A VLAN is often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN.

Interface VLAN membership on a switch module is assigned manually on an interface-by-interface basis and is known as interface-based or static VLAN membership. Traffic between the VLANs must be routed. VLANs are identified with a number ranging from 1 to 4094.

Port Channel

A port channel bundles up to eight individual interfaces into a group to provide increased bandwidth and redundancy. If a member port within a port channel fails, the traffic that is carried over a failed link switches to one of the remaining member ports within the port channel. This traffic switch facilitates the load and balances the traffic across the physical interfaces. A port channel is operational as long as at least one physical interface within the port channel is operational.

You can create a port channel by bundling compatible interfaces. You can configure and run either static port channels or the port channels that run the Link Aggregation Control Protocol (LACP). Any configuration change that you apply to a port channel is applied to each member interface of that port channel.

Use a static port channel with no associated protocol for a simplified configuration. To use a port channel efficiently, you can use LACP, which is defined in IEEE 802.3ad.

ARP

Address Resolution Protocol (ARP) provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. It can be used in the following scenario:

Host B wants to send information to Host A, but does not have the MAC address of Host A in the ARP cache. Host B generates a broadcast message for all the hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All the hosts within the broadcast domain receive the ARP request and Host A responds with its MAC address.

DHCP Snooping and Trust

Dynamic Host Configuration Protocol (DHCP) snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. The DHCP snooping feature validates DHCP messages that are received from the untrusted sources and filters the invalid messages. It limits the rate of DHCP traffic that is sent or received from trusted and untrusted sources. It builds and maintains the DHCP snooping binding database which contains information about untrusted hosts with leased IP addresses. It utilizes the DHCP snooping binding database to validate subsequent requests from the untrusted hosts. DHCP snooping is enabled on a per VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or on a range of VLANs.

DNS

Domain Name System (DNS) is a hierarchical distributed naming system that maps hostnames to IP addresses. When you configure DNS on your switch, you can substitute the hostname for the IP address with the IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations. IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as delimiting characters. For example, Cisco Systems is a commercial organization that the IP identifies by a com domain name. Therefore, its domain name is cisco.com. To keep track of domain names, IP has defined the concept of a domain name server that holds a cache (or database) of names mapped to IP addresses. If you need to map the domain name to the IP addresses, you must identify the hostname, specify the server name that is present on your network, and then enable the DNS.

To map a domain name to an IP address, use the following command on your network and enable the DNS:

serverservpresent

Configuring Converged Access

Configuring a Switch Hostname

You can configure a hostname on a switch to uniquely identify the switch. By default, the system name and the system prompt are **Switch**.

Tip Configure your switch hostname such that you can easily identify the switch in your network. Set the hostname for the switch product family, the role of the switch in your network, and the switch location. For example, 3850-access-Bld1Flr1

To configure a host name, use the **hostname** command in the global configuration mode.

```
Device(config)# hostname 3850-access-Bld1Flr1
```

Viewing System Level Licensing

The switch is preinstalled with the ordered license. If a license is not pre-ordered, the switch is booted with the LAN-base license, by default. Right-to-use (RTU) licensing allows the activation of a specific license type and level, and the management of license usage on the switch.

The following are the available RTU licenses:

- LAN Base — Layer 2 features
- IP Base — Layer 2 and Layer 3 features
- IP Services — Layer 2, Layer 3, and IPv6 features

Tip Wireless functionality is supported only on IP Base licenses or on IP Services licenses.

In case of a switch stack, the switch that is activated with an RTU license is the active switch. The license level for the standby or member switches in the stack can be activated at the same time from the active switch console.

Activating an RTU License

Step 1 To activate an RTU License, use the following command in privileged EXEC mode:

```
Device# license right-to-use activate {ipbase |ipservices | lanbase}{all | evaluation all}[slot
slot-number][acceptEULA]
```

Step 2 To reload the switch stack and complete the activation process for RTU license, use the following command in privileged EXEC mode:

```
Device# reload
```

Step 3 After you configure a specific license type and level, you can manage your license by monitoring the license state. To monitor the license state, use the following command:

```
Device# show license right-to-use usage [slot 9]
```

Working with NTP System Clock and Console Timestamps

If you use any of the following features, it is mandatory to use NTP to synchronize controllers:

- SNMPv3
- Access point authentication
- Management frame protection

Cisco Catalyst 3850 and Cisco Catalyst Series switches also supports synchronization with NTP using authentication.

Note Configure a service timestamp for console messages, logs, and debug outputs to allow accurate and easy cross-referencing of events in a network.

Configuring an NTP Server

Step 1 To configure an NTP server, use the following commands in the global configuration mode:

```
Device(config)#ntp server ip-address
Device(config)# clock timezone zone hours-offset
Device(config)# clock summer-time zone recurring
```

Step 2 To configure service time stamps, use the following commands in global configuration mode:

```
Device(config)# service timestamps debug datetime msec localtime
Device(config)#  service timestamps log datetime msec localtime
```

Step 3 To verify whether the system clock is synchronized with the NTP server, use the following command in privileged EXEC mode:

```
Device# show ntp status
```

Defining DNS

To configure name and address resolution, define a domain name, and specify the IP address for one or more servers, use the following commands in global configuration mode:

```
Device(config)# ip domain-name name
Device(config)# ip name-server server-address1[server-address2 ... server-address6]
```

Note The default domain name is the value set by the **ip domain-name** command.

Generating Cryptographic Keys

When SSH or HTTPS is configured on a switch, a default cryptographic key is generated. For enhanced security, we recommend that you increase the key length beyond the default size. The recommended key size is 2048.

To generate a cryptographic key, use the following command:

```
Device(config)# crypto key generate rsa modulus 2048
```

Note For more information about additional cryptographic configuration options and examples, refer to the “Configuring SPAN and RSPAN” chapter in the Consolidated Platform Configuration Guide, Cisco IOS XE 3.3SE.

Configuring SSH for User Login

Note Disable the Telnet access to the device.

Step 1 To configure SSH, use the following command in global configuration mode:

```
Device(config)# ip ssh version 2
Device(config)# ip ssh authentication-retries 3
Device(config)# ip ssh time-out 120
Device(config)# line vty 0 15
Device(config-line)# transport input ssh
```

Step 2 To configure local login and password for access, use the following commands in the global configuration mode.

```
Device(config)# username admin privilege 15 secret my-password
Device(config)# enable secret my-secret-password
Device(config)# service password-encryption
Device(config)# exit
```

Note The local login account and password provides basic device access authentication to view platform operations.

Step 3 To verify whether SSH is enabled, use the following command in privileged EXEC mode:

```
Device# show ip ssh
```

Configuring Management Interface Setup

The GigabitEthernet 0/0 interface on the Cisco Catalyst 3850 Series Switches is used for out-of-band management and is located next to the console port on the back panel of the switch. Out-of-band management manages Cisco Catalyst 3850 Series Switches and all other networking devices through a physical network that is separate from the network that carries end-user traffic. The GigabitEthernet 0/0 interface is located on the back panel of the switch, which is next to the console port.

Note On Cisco Catalyst 4500 Series Switches, FastEthernet 0 is used as the management interface

Note

- Management traffic originating from a switch must be associated with GigabitEthernet 0/0 Virtual Routing and Forwarding (VRF).
- The management VRF, *mgmt-vrf* is a built-in VRF. A default route is required for the management VRF.

  > **Note** On Cisco Catalyst 4500 Series Switches, the management VRF is *mgmtvrf*

- The GigabitEthernet 0/0 interface cannot be used as the source interface for sending SNMP traps.
- The GigabitEthernet 0/0 interface is a Layer 3 interface.

Step 1 To configure the interface on Cisco Catalyst 3850 Series Switches, use the following commands:

```
Device(config)# interface GigabitEthernet 0/0 or interface FastEthernet0
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# exit
```

Step 2 To verify the reachability to the default gateway use the following ping utility:

```
Device# ping vrf Mgmt-vrf gateway-ip-address
```

Configuring a VLAN

To configure a VLAN, use the following commands:

```
Device# configure terminal
Device(config)# vlan data-vlan
Device(config)# name data-name

Device(config)# vlan voice-vlan
Device(config)# name  voice-name

Device(config)# vlan wireless-management-vlan
Device(config)# name  management-name
Device(config)# exit
```

Configuring a Default Route

To configure a default route, use the following command in global configuration mode:

```
Device(config)# ip route 0.0.0.0 0.0.0.0
```

Configuring an Uplink Interface

This section describes how to configure Ethernet interfaces that connect a switch stack to distribution switches or routers. Typically, EtherChannels are used for uplink connectivity because they offer additional resiliency.

Note When you stack two or more physical switches into one logical switch, we recommend that you spread the uplink interfaces across the physical members, preventing a complete member failure.

This section provides the options available for configuring uplink interfaces:

- L3 connectivity using port channel

  To configure L3 connectivity using a port channel, use the following commands:

```
Device(config)# interface intf-id1
Device(config-if)# switchport mode trunk
Device(config-if)# switchport trunk allowed vlan 10 <<<<<allowed-vlan-list
Device(config-if)# channel-group 1 mode active  <<<<< Different channel-group modes
can be selected based on the remote interface configuration.
Device(config-if)# no shutdown

Device(config)# interface <intf-id2>
Device(config-if)# switchport mode trunk
Device(config-if)# switchport trunk allowed vlan 15 <<<<<allowed vlan list
Device(config-if)# channel-group 1 mode active <<<< generic
Device(config-if)# no shutdown


Device(config)# interface Port-channel 10
Device(config-if)# no switchport
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# no shutdown
```

  Note To create a port channel, **intf-id1** and **intf-id2** are available.
  For further information on L2 and L3 etherchannel, refer to the Configuring EtherChannelschapter in the Layer 2/3 Configuration Guide.

- L3 connectivity using Switch Virtual Interface (SVI):

  To configure SVI interface, use the following commands:

```
Device(config)# interface vlan X
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# no shutdown

Device(config)# interface type/number
Device(config-if)# no switchport
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device (config-if)# no shutdown
```

Configuring DHCP Snooping and Trust

Step 1 To configure DHCP snooping, use the following commands:

Device(config)# **ip dhcp snooping**

Device(config)# **ip dhcp snooping** *vlan-number*

Step 2 To trust the incoming DHCP packets on the uplink to the network, use the following command:

Device(config-if)# **ip dhcp snooping trust**

Enabling IP ARP Inspection

To enable IP ARP inspection, use the following command:

Device(config)# **ip arp inspection vlan** *data-vlan voice-vlan*

Configuring a Downstream Wired Client Interface

To configure a downstream wired client interface, use the following commands:

```
Device(config)# interface range gigabitethernet1/0/1 - 4
Device(config-if)# switchport access vlan
Device(config-if)# switchport voice vlan 100
Device(config-if)# auto qos voip cisco-phone
Device(config-if)# spanning-tree portfast
Device(config-if)# no shutdown
Device(config-if)# exit
```

Configuring an Access Point Interface

To configure an access point interface, use the following commands:

```
Device(config)# interface range gigabitethernet1/0/1 - 4
Device(config-if)# switchport access vlan management-vlan
Device(config-if)# spanning-tree portfast
Device(config-if)# no shutdown
Device(config-if)# exit
```

Stacking for High Availability

When Cisco Catalyst 3850 Series and Cisco Catalyst 3650 Series Switches are connected using a stack cable, the high availability feature is enabled by default.

Note For more information on stacking, refer to Stack Manager and High Availability Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

Prerequisites for Switch Stack Configuration

The following are the prerequisites for switch stack configuration on Cisco Catalyst 3850 Series and Cisco Catalyst 3650 Series Switches :

- All the switches in the switch stack should run the same license level as the active switch.
- All the switches in the switch stack should run compatible software versions.
- A switch stack can have a maximum of nine stacking-capable switches.
- You cannot have a switch stack containing a mix of Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches.
- During a stateful switchover event, all the clients are deauthenticated and must rejoin the new active switch.

Viewing Stack Details

Use the following command to display the summary information about a stack:

```
Device# show switch
Switch/Stack Mac Address : c800.846a.2080 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------
 1       Standby  c800.840f.7480     1      V05     Ready
*2       Active   c800.846a.2080     1      V05     Ready
 3       Member   c800.846a.3180     0      0      Ready
```

CHAPTER 5

Converged Access: Securing Networks with AAA and Cisco ISE

The Cisco Catalyst 3650 Series Switches and the Cisco Catalyst 3850 Series Switches are capable of providing both wireless connectivity and wired services to end users. Since, wireless networks are equally prone to unauthorized access and attacks, they require the same level of security as wired networks.

This chapter provides a step-by-step instructions for configuring authentication, authorization, and accounting (AAA) and Cisco Identity Service Engine (ISE), to enable the Converged Access on Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches.

Overview of Securing Networks with AAA and Cisco ISE

For wireless clients, AAA enables the Cisco Catalyst 3850 Series Switches to determine who the user is (authentication), what the user can do (authorization), and what the user did (accounting). AAA helps secure the wireless network in the corresponding enterprise against unauthorized access.

The authentication component of AAA is responsible for providing a method to identify (authenticate) wireless users. With AAA, you can define one or more authentication methods the device should use when authenticating a user. For example, you can specify two authentication methods, an external security server and a local user database on the device.

When authentication for a user is completed successfully, AAA's authorization is used to restrict the actions a user can perform and the services a user can access. For example, if network access to a temporary worker in an enterprise network needs to be limited, you can enforce this restriction using AAA's authorization component.

AAA's accounting component is responsible for keeping a record of authentication and authorization actions of wireless users, and related metrics such as tracking users who log in to the network after business hours.

Note

- You can either use authentication by itself or along with authorization and accounting. Authorization requires a user to be authenticated first. If you use multiple security contexts, AAA settings are unique for each context, and are not shared between contexts.
- You can control the access, authorize resources and commands, and perform accounting differently among contexts.
- You can configure local authentication and authorization on the switch.
- For more information, refer to the chapter "Configuring Local Authentication and Authorization" in the Security Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches).

Configuring AAA

Before You Begin

The following are the prerequisites for configuring AAA on Cisco Catalyst 3850 Series Switches:

- Configure Cisco Catalyst 3850 Series Switches or Cisco Catalyst 3650 Series Switches with IP Base or IP Services license.
- Configure Cisco ISE with the following features:
  - IP reachability to the switch.
  - Client Username and Password Database or link to the Active Directory.

Step 1 To enable AAA, use the **aaa new-model** command in global configuration mode:

```
Device(config)# aaa new-model
```

Step 2 To define the AAA server group with a group name, use the **aaa group server radius** command. All the members should be of the group, RADIUS. Use the **server name** command to define the server name and enter server group radius configuration mode:

```
Device(config)#  aaa group server radius  name
 Device(config)#  server name  server-name
```

Step 3 To enable dot1x and 802.1X globally, use the **dot1x system-auth-control** command in global configuration mode:

```
Device(config)# dot1x system-auth-control
```

Step 4 To create an authentication list for 802.1X, use the **aaa authentication dot1x default group** command. This authentication contacts a RADIUS server in the RADIUS group specified using *group-name*.

```
Device(config)#  aaa authentication dot1x default group  group-name
```

To configure network authorization through RADIUS, use the **aaa authorization network default group** command.

```
Device(config)#  aaa authorization network default group  group-name
```

To configure a default accounting method list, where a RADIUS server provides accounting services, use the **aaa accounting identity default start-stop group** command.

```
Device(config)#   aaa accounting identity default start-stop groupgroup-name
```

Step 5 To define the RADIUS server name along with the IP address, port numbers, and the shared key, use the following commands:

```
Device(config)#   radius server  radius-server-name
Device(config-dia-peer)#   address ipv4  IP_Address  auth-port  authentication-port  acct-port   accounting_port
Device(config-keychain)#   key  radius-shared-key
```

Step 6 To configure the SNMP community string for Cisco ISE, use the **snmp-server community** command:

```
Device(config)#   snmp-server community  snmp-community-string  RO
```

Step 7 To configure a RADIUS source interface to connect to the RADIUS server, use the **ip radius source-interface** command:

```
Device(config)#   ip radius source-interface  interface
```

Verifying Dot1x Protocol and RADIUS Server

Use the following command to check if the dot1x protocol is enabled on the switch:

```
Device# show dot1x

sysauthcontrol              Enabled
dot1x Protocol Version            3
```

Use the following command to check the RADIUS server:

```
Device# show radius server-group all

server group group_Name
Server(Radius_Server_IP:Auth_Port,Acct_Port) Transactions:
```

Adding a Cisco Catalyst 3850 Switch to Cisco ISE

Step 1 Choose **Administration > Network Resources > Add**.

Step 2 Enter the **Name**, **Description** (optional), and **IP Address** of the switch.

Step 3 Check the **Authentication Settings** check box .

Step 4 Enter the shared secret key using the **radius_shared_key** field.

Step 5 Enter the SNMP settings and select the SNMP version.

Step 6 Enter the SNMP RO community in the **snmp_commnity_string** field.

Configuring Authentication and Authorization Policies

Cisco ISE comes with prepopulated authentication and authorization policies:

- Choose **Policy** > **Authentication** to check if the Wired_802.1X and Wireless_802.1X authentication policies exist.
- Choose **Policy** > **Authorization** and check if the Wired_802.1X and Wireless_802.1X authorization policies exist.
- Choose **Policy** > **Conditions** > **Compound Conditions**, if required, to edit these policies.

To create an authorization policy for an employee on Corporate WLAN using dot1x, perform the following steps:

Step 1 Choose **Policy** > **Authorization**.

Step 2 Click **Drop First Down Arrow** next to the Edit button and select **Insert New Rule Above**.

Step 3 Enter the name of the rule.

Step 4 Choose the following conditions from the **Condition** field:

- Condition 1: Add Identity groups for the incoming wireless user.
- Condition 2: Select **Wireless dot1x**.

Step 5 Provide the Permit Access using the **Permissions** field.

Step 6 Click **Save**.

Note For information about AAA concepts including converged access details, refer to:

RADIUS Configuration Guide - Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

For information about Cisco ISE, see the:

Wireless LAN802 and wireless–1x Authentication Deployment Guide.

CHAPTER 6

Converged Access: Enabling Wireless

This chapter describes how to deploy a converged access switch, connect it as a mobility member in your converged topology, activate access point licenses, and have the access points ready for physical connection to the corresponding switch.

This chapter covers basic interface-level configuration on a switch, basic converged access wireless configuration, and mobility configuration that is specific to converged access technologies.

This chapter is primarily targeted at individuals who have previous experience with switching infrastructure or wireless technologies, or both, but who may not be familiar with converged access as a model of wireless deployment.

Concepts and Definitions

This section provides you with brief descriptions of the key phrases used in this chapter.

CAPWAP

Control and Provisioning of Wireless Access Points (CAPWAP) is a secured tunneling protocol over which access points connect to wireless controllers. Client traffic is sent from a wireless controller to an access point over a CAPWAP tunnel. Additionally, wireless controllers in a converged access architecture communicate with each other over a secured CAPWAP tunnel.

Switch Peer Group

A switch peer group is a collection of mobility agents that share a full–mesh CAPWAP tunnel topology and is defined on a Mobility Controller. Mobility Agents within the same switch peer group easily share client context with each other and clients can quickly roam between the Mobility Agents in the same switch peer group.

Mobility Subdomain

A mobility subdomain is defined by a Mobility Controller on a one-to-one basis. A mobility subdomain can contain one or more switch peer groups. Client roaming between devices in different switch peer groups in the same mobility subdomain can be enabled by forwarding traffic through the mobility controller.

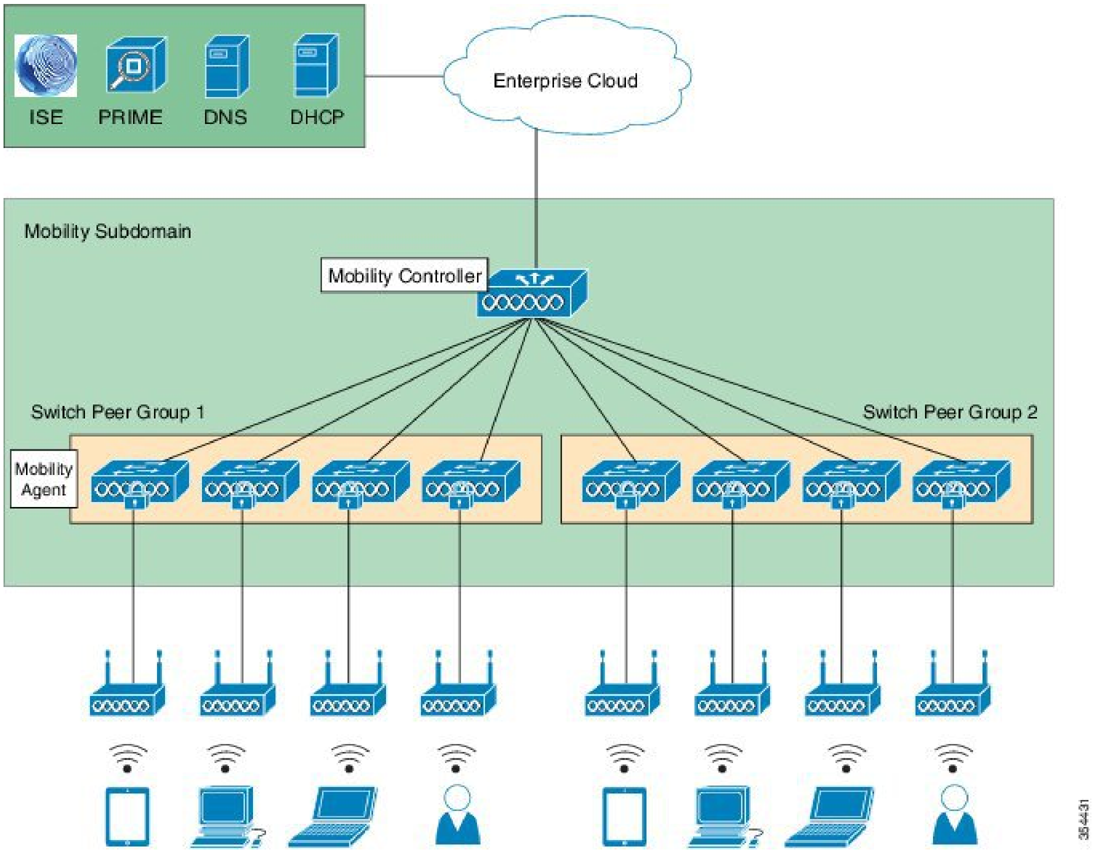
Mobility Domain

A mobility domain can be defined as a collection of mobility subdomains. Mobility domains are created by associating mobility controllers with one another to create a mesh of CAPWAP tunnels. Clients can roam between different mobility subdomains in the same domain by forwarding traffic through two mobility controllers, one in the original subdomain and one in the roamed-to subdomain. Clients cannot roam between different mobility domains.

Converged Access Topology Example

The following figure shows a converged access topology. The topology shows what a typical converged access mobility subdomain looks like. While your topology may differ, the mobility configuration on the individual mobility agents and the mobility controller will be the same as what is referenced in this chapter.

Figure 3: Converged Access Topology



Configuring Wireless Management Interface

To enable the wireless controller functionality on a device, use the **wireless management interface** command. The VLAN interface should be the same as the access point VLAN. After the command is enabled, the switch intercepts the CAPWAP discovery packets on the configured VLAN for the directly connected access points. This allows the access points to join the switch as controllers, and prevents them from joining another controller in the VLAN.

From Cisco IOS XE Release 3.8E, VSS wireless support was added to Cisco Catalyst 4500 Series, Cisco 3850 Series, and Cisco 3650 Series Switches.

Step 1 To configure the wireless management VLAN interface on each switch in your converged access deployment, use the following command:

```
Device(config)# wireless management interface vlan-interface
```

Step 2 To validate your configuration, use the following command. Make sure that the switch recognizes the VLAN interface you have selected, as the management interface.

```
Device# show wireless interface summary

Wireless Interface Summary

Interface Name Interface Type VLAN ID IP Address      IP Netmask     MAC Address
--------------------------------------------------------------------------------
interface      Management     vlan    ip_address      netmask        mac_address
```

Configuring Mobility Architecture

Configuring a Mobility Controller

Each mobility subdomain needs a Mobility Controller. Note that a switch must operate either as a mobility agent or as a Mobility Controller. However, when operating as a Mobility Controller, the switch also performs all the standard functions of a Mobility Agent.

To configure a switch as a Mobility Controller and reload the switch for the configuration to take effect, use the following commands:

```
Device (config)# wireless mobility controller
Device (config)# exit
Device# write memory
Device# reload
```

After the device reloads, additional command options become available, because the switch is operating in Mobility Controller mode.

Note Cisco 5760 Wireless LAN Controllers cannot be configured as Mobility Agents, and are therefore, considered as Mobility Controllers always.

Configuring an Access Point Adder License

The distribution and tracking of access point licenses is handled on the Mobility Controller for a given mobility subdomain. When an access point first connects to a Mobility Agent, the Mobility Agent queries the Mobility Controller for a free access point license. If a free license exists, the access point is allowed to register.

Once purchased, adder licenses should be configured on the Mobility Controller. To configure an adder license, use the following command in privileged EXEC mode:

```
Device# license right-to-use activate apcount license-number
```

The number of unconfigured access point adder licenses can be viewed at any time by looking at the license summary. To view the license summary, use the following command:

```
Device# show license right-to-use summary
.
.
.
Total AP Count Licenses: license_number
AP Count Licenses In-use: used_licenses
AP Count Licenses Remaining: remaining_licenses
```

Note On Cisco Catalyst 4500 Series Switches, the stand-by mobility controller synchronizes the license count from the active mobility controller.

Configuring Multiple Subdomains

Note You can skip this section if you are not deploying multiple mobility subdomains.

Devices acting as Mobility Controllers can form CAPWAP tunnels with other Mobility Controllers, extending a mobility domain across one or more subdomains. This configuration is typical for large deployments or in scenarios where the required number of access points scale beyond what is supported on a single mobility subdomain. When a client roams between mobility subdomains, traffic traverses both mobility controllers through their established CAPWAP tunnels.

Step 1 To configure a Mobility Controller with its peer mobility controllers, use the following commands. This should be done on all the devices, creating a full–mesh mobility topology. Repeat this step for all the Mobility Controllers available in the mobility domain. For example, if you have three Mobility Controllers, repeat this step three times.

Mobility Controller 1:

```
Device(config)# wireless mobility group name group-name
Device(config)# wireless mobility group member ip mc2-ip
Device(config)# wireless mobility group member ip mc3-ip
```

Mobility Controller 2:

```
Device(config)# wireless mobility group name group-name
Device(config)# wireless mobility group member ip mc1-ip
Device(config)# wireless mobility group member ip mc3-ip
```

Mobility Controller 3:

```
Device(config)# wireless mobility group name  group-name
Device(config)# wireless mobility group member ip mc2-ip
Device(config)# wireless mobility group member ip  mc3-ip
```

Step 2 To verify the configuration, use the following command. Ensure that all the Mobility Controllers are able to establish bidirectional functionality with each other.

```
Device# show wireless mobility summary

Mobility Controller Summary:

Mobility Role                                   : Mobility Controller
Mobility Protocol Port                          : 16666
Mobility Group Name                             : group_name
.
.
.
Controllers configured in the Mobility Domain:

IP                Public IP         Group Name        Multicast IP      Link Status
-------------------------------------------------------------------------------
mc1_ip            -                 group_name        0.0.0.0           UP   : UP
mc2_ip            mc2_ip            group_name        0.0.0.0           UP   : UP
mc3_ip            mc3_ip            group_name        0.0.0.0           UP   : UP
```

Configuring a Mobility Agent

Mobility agents must be configured with the wireless management interface IP address of the Mobility Controller for the subdomain they are to join.

Note Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches are configured as Mobility Agents in the factory. Therefore, no configuration is needed to enable Mobility Agent mode.

To configure a Mobility Agent with the IP address of its Mobility Controller, use the following command:

```
Device(config)# wireless mobility controller ip  controller-ip
```

To verify if the Mobility Agent and the Mobility Controller are able to establish a bidirectional connection, use the following command:

```
Device#  show wireless mobility summary

Mobility Agent Summary:

Mobility Role                                   : Mobility Agent
.
.
```

```
.
Link Status is Control Link Status : Data Link Status

The status of Mobility Controller:

IP              Public IP           Link Status
------------------------------------------------
controller_ip   controller_ip       UP   : UP
```

Creating a Switch Peer Group

Before CAPWAP connections complete the mobility architecture, create one or more switch peer groups and specify which Mobility Agents should belong to which peer group. Mobility Agents within a switch peer group form a full–mesh CAPWAP topology, and roaming is fastest between them. When a client roams to another switch peer group in the same mobility subdomain, packets traverse the mobility controller. Splitting switch peer groups can help reduce roaming traffic since a Mobility Agent shares roaming information with the devices in its switch peer group and its Mobility Controller.

Note A switch peer group should include peer Mobility Agents, which provide wireless functionality, in an area that users access most frequently.

Define a switch peer group on a Mobility Controller. After the peer group is configured, add the peer group members to the switch peer group using the **wireless management interface** command. The IP addresses of the peer group member interfaces should be the same as the IP addresses configured.

```
Device(config)# wireless mobility controller peer-group peer-group
Device(config)# wireless mobility controller peer-group  peer-group  member ip  member-ip-1
Device(config)# wireless mobility controller peer-group  peer-group  member ip  member-ip-2
```

Mobility Agents in the switch peer group are associated with the peer group and establish a full–mesh mobility topology with other peers. You can verify the switch peer group from the Mobility Agent for a given switch peer group, or the Mobility Controller for all peer groups.

To verify the configuration on a Mobility Agent, use the following command:

```
Device# show wireless mobility summary

Mobility Agent Summary:

Mobility Role                                   : Mobility Agent
Mobility Protocol Port                          : 16666
Mobility Switch Peer Group Name                 : peer_group
.
.
.
Switch Peer Group members:

IP              Public IP           Data Link Status
-----------------------------------------------------
member_ip_1     member_ip_1         UP
member_ip_2     member_ip_2         UP
```

To verify the configuration on a Mobility Controller, use the following command:

```
Device# show wireless mobility summary

Mobility Controller Summary:
```

```
Mobility Role                                   : Mobility Controller
.
.
.
Switch Peer Group Name            : peer_group
Switch Peer Group Member Count    : 2
Bridge Domain ID                  : 0
Multicast IP Address              : 0.0.0.0

IP               Public IP             Link Status
--------------------------------------------------
member_ip_1     member_ip_1            UP   : UP
member_ip_2     member_ip_2            UP   : UP
```

To verify the configuration on a Mobility Controller on Cisco Catalyst 3850 Series and Cisco Catalyst 4500 Series Switches, use the following command:

```
Device# show wireless mobility summary

Mobility Controller Summary:

Mobility Role                                   : Mobility Controller
Wireless Management VLAN                        : 60
Wireless Management IP Address                  : 10.127.0.66
Mobility Group Name                             : ENG
Mobility Oracle Configured Mode                 : Disabled
Mobility Oracle IP Address                      : 0.0.0.0
DTLS Mode                                       : Enabled
Mobility Keepalive Interval/Count               : 10/3
Mobility Control Message DSCP Value             : 48
Mobility Domain Member Limit/Count              : 8/2

Link Status is Control Link Status : Data Link Status

Controllers configured in the Mobility Domain:

HostName                IP               Public IP        Group Name       Multicast IP
  Link Status
------------------------------------------------------------------------------------------
eng-bgl16-51a-sw1  10.127.0.66            N/A              ENG               0.0.0.0
    N/A
                   10.127.1.76            10.127.1.76      ENG               0.0.0.0
    UP   : UP

Sub-Domain Peer Group Summary
Switch Peer Group Limit/Count                  : 8/2
Switch Peer Group Member Limit/Count           : 32/3

Switch Peer Group Name            : 4th-floor-fd1
Switch Peer Group Member Count    : 1
Bridge Domain ID                  : 0
Multicast IP Address              : 0.0.0.0

HostName          IP               Public IP        MTU     Link Status      Centralized
(Cfgd : Running)
------------------------------------------------------------------------------------------

                 10.127.1.130     10.127.1.130     0         DOWN : DOWN       Disabled
    Disabled

Switch Peer Group Name            : Mingla
Switch Peer Group Member Count    : 2
Bridge Domain ID                  : 0
Multicast IP Address              : 0.0.0.0
HostName          IP               Public IP        MTU     Link Status      Centralized
(Cfgd : Running)
------------------------------------------------------------------------------------------
eng-bgl16-42a-sw1 10.127.1.157     10.127.1.157     1500      UP   : UP         Disabled
     Disabled
                 10.127.1.209     10.127.1.209     1500      UP   : UP         Disabled
```

```
        Disabled
```

Staging for Access Points

Configuring a Physical Port

Configure the downlink interfaces that connect to access points as Layer 2 switch ports. The access VLAN for the ports should be configured as the same VLAN used in the **wireless management interface** command. Enable the Spanning tree Portfast on access ports to flag these ports as edge ports to the spanning tree. This causes the port to immediately transition to the spanning tree forwarding state, allowing traffic to flow without progressing through the typical spanning tree process.

To configure the physical ports connected to the access points, use the following commands:

```
Device(config)# interface interface_number
Device(config-if)# description Access-point port
Device(config-if)# switchport access vlan wireless-mgmt-vlan
Device(config-if)# switchport mode access
Device(config-if)# spanning-tree portfast
Device(config-if)# spanning-tree bpduguard enable
```

Configuring an Access Point IP Address

After the wireless controller functionality is enabled and the mobility topology built, the device needs to be configured to support the directly connected access points. Typically, DHCP is used to provide IP addresses for access points. The DHCP addresses are provided by an external source or by the switch itself. Configure the addresses by external source or by switch, but not by both.

If an external source is used, the switch should be configured as a DHCP relay agent. To configure using external source, use the following commands:

```
Device(config)# interface vlan apvlan-interface
Device(config-if)# ip helper-address dhcp-server-ip
```

To use the switch as the DHCP server for access points, configure an appropriate DHCP pool on the switch. Configure the default router using the **default-router** command and specify the wireless management IP address. Use the **update arp** command to secure ARP table entries on the switch with the DHCP lease negotiated by the access point.

To configure the DHCP pool, use the following commands:

```
Device(config)# ip dhcp pool name
Device(dhcp-config)# network network-address network-mask
Device(dhcp-config)# default-router wireless-mgmt-vlan-ip
Device(dhcp-config)# update arp
```

After configuring the switch as the DHCP server, you can verify if the access points are obtaining addresses after they are connected. If you have configured an external DHCP server, check that server for bindings to validate this configuration.

To check the local Cisco IOS DHCP server bindings, use the following command:

```
Device# show ip dhcp pool

Pool name:
.
.
.
Leased addresses               : 3
```

Registering Access Points

At this point, access points are ready to be physically connected to the topology. After an access point is connected and has obtained an IP address, it will connect on the wireless management VLAN and broadcast a discovery request. The switch will intercept this request and communicate with the access point. No further intervention is required.

To verify that the access points have successfully registered with the switch, use the following command:

```
Device# show ap summary

Number of APs: 3
.
.
.
```

CHAPTER 7

Converged Access: WLAN Configuration

This chapter provides information about configuring and enabling wireless LANs (WLAN) on your converged access deployment and the recommended WLAN configuration on a switch. It also provides information about how to configure and advertise WLANs for the clients to join. This document also describes how to enhance the functionality of WLANs by enabling various features, and leverage the security policies created in the deployment process for wireless authentication.

WLAN Features

DHCP Server

By default, clients either assign their IP addresses statically or by an enterprise DHCP server. We recommend that the wireless clients get their IP addresses through a DHCP server. This allows addressing policies to be leveraged on the DHCP server, prevent the use of duplicate network addresses, and enhance security.

To configure WLANs such that clients receive their IP addresses through a DHCP server, use the following commands:

```
Device(config)# wlan profile-name
Device(config-wlan)# ip dhcp required
```

To verify the configuration on a per-WLAN basis, use the following command:

```
Device# show wlan id wlan-id
.
.
.
DHCP Address Assignment Required               : Enabled
.
.
.
```

For more information on DHCP in WLANs, refer to the Configuring DHCP for WLANs section in the WLAN Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches).

Protected Management Frame

Control and Management frames are transmitted unencrypted, so that they are understood by all clients. The 802.11w Protected Management frames protect the wireless medium from attacks by adding cryptographic information into control frames for clients that support the standard.

To configure a protected management frame for clients that support the standard, use the following command:

```
Device(config-wlan)# security pmf optional
```

To verify that the protected management frame is configured properly on the WLAN, use the following command:

```
Device# show wlan id wlan_id
.
.
.
    PMF Support                                 : Optional
        PMF Association Comeback Timeout        : 1
        PMF SA Query Time                       : 200
.
.
.
```

For more information about DHCP in WLANs, refer to theConfiguring DHCP for WLANs section in the WLAN Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) WLAN Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches).

Band Selection

Band Selection is a feature that encourages dual-band clients to connect to a 5-GHz network over a 2.4-GHz network advertising the same SSID. This is preferred because 5-GHz networks exhibit less interference on wireless channels. The band selection algorithm works by slightly delaying probe responses to clients on 2.4-GHz channels, thus making the 5-GHz channels more attractive to clients.

Note Band selection only affects the operation of dual-band clients and requires both the radios on the corresponding access point to be operational.

Tip Band selection should not be used with WLANs that provide latency-sensitive services, such as real-time voice or video because of the potential for slightly increased roaming delay. If you are provisioning a WLAN for voice or video, do not enable band selection.

To enable band selection on WLANs used to support data clients, use the following commands:

```
Device(config)# wlan profile-name
Device(config-wlan)# band-select
```

To verify that band selection is configured on a WLAN, use the following command:

```
Device# show wlan id    wlan-id

WLAN Profile Name      : profile_name
.
.
.
Band Select                                     : Enabled
.
.
.
```

Assisted Roaming

The Assisted Roaming feature helps reduce the need for active and passive scanning by 802.11k-enabled clients, and optimizes roaming for 802.11k-compliant and non-802.11k clients. For 802.11k clients, assisted roaming allows clients to request neighbor reports with information about access points that are roaming candidates. For non-802.11k clients, the switch maintains a prediction neighbor list and attempts to ensure that clients roam to the access point with the best signal by denying association requests to less desirable access points.

To configure assisted roaming on data WLANs, use the following commands:

```
Device(config)# wlan    profile-name
Device(wlan)# assisted-roaming neighbor-list
Device(wlan)# assisted-roaming dual-list
Device(wlan)# assisted-roaming prediction
```

To verify that assisted roaming is configured on a WLAN, use the following command:

```
Device# show wlan id  wlan-id
.
.
.
Assisted-Roaming
    Neighbor List                               : Enabled
    Prediction List                             : Enabled
    Dual Band Support                           : Enabled
```

Tip The Assisted Roaming Prediction feature can potentially deny association requests to access points. This is not considered to be the best candidate for the client roam and may induce extra delay during an active client roam. We do not recommend Assisted Roaming Prediction or WLANs that provide real-time or latency-sensitive services, such as voice or real-time video.

Peer-to-Peer Blocking

Peer-to-peer blocking gives an administrator more control to handle wireless-to-wireless client traffic on a switch. For example, one wireless user downloading a shared file from another user, or two phones connected to one another in an enterprise environment are scenarios that are acceptable and expected. However, on a guest WLAN or a hotspot-style WLAN, wireless-to-wireless traffic may be a security hazard and should be blocked.

For enterprise WLANs, the peer-to-peer feature is disabled by default.

To enable peer-to-peer blocking on a guest WLAN with the drop option, use the following commands on the corresponding WLAN:

```
Device(config)# wlan  profile-name
Device(config-wlan)# peer-blocking drop
```

To verify that peer-to-peer blocking is enabled with the drop action for the guest WLAN, use the following command:

```
Device# show wlan id  wlan-id
.
.
.
Peer-to-Peer Blocking Action                   : Drop
.
.
.
```

Wi-Fi Direct Client Policy

Wi-Fi Direct is a client feature that allows clients to form ad hoc connections with one another to conveniently transfer data or provide a service. Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices may associate with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently.

However, this represents a potential security risk because devices connected through Wi-Fi Direct lack any identity information because they do not connect to the wireless infrastructure. Policy decisions cannot be easily applied to the devices connected on the Wi-Fi Direct devices. As a result, we recommend that you do not allow the devices connected through Wi-Fi Direct to access the wireless network in an enterprise environment.

To stop Wi-Fi devices from connecting to enterprise WLAN, use the following commands:

```
Device(config)# wlan  profile-name
Device(config-wlan)# wifidirect policy deny
```

To ensure that the Wi-Fi Direct policy is set to Deny a WLAN, use the following command:

```
Device# show wlan id  wlan-id
.
.
.
WifiDirect                                     : Deny
.
.
.
```

Roaming Fast Transition (802.11r)

802.11r is an IEEE standard to help accelerate client roaming while creating a more seamless experience for a roaming client. Fast-transition roaming works by associating a client and an access point before the client roams to the target AP, such that all the wireless keys are ready for use before roam association actually takes place.

Note By default, fast transition is disabled.

Tip Clients with drivers that do not support 802.11r will not be able to associate to a WLAN with fast transition enabled. Therefore, ensure that fast transition is disabled. If fast transition is required, create a separate SSID. Disabling or enabling fast transition by creating a separate SSID allows even legacy devices to access the enterprise WLAN.

To configure fast transition and an associated SSID, use the following commands:

```
Device(config)# wlan profile-name
Device(config-wlan)# security ft
```

To verify that fast transition is enabled on the appropriate WLAN, use the following command:

```
Device# show wlan id wlan-id
.
.
.
    FT Support                                  : Enabled
        FT Reassociation Timeout                : 20
        FT Over-The-DS mode                     : Enabled
.
.
.
```

For more information about 802.11r fast transition, refer to the Configuring 802.11r BSS Fast Transition guide.

Media Session Snooping

Media session snooping is configured on a per-WLAN basis and allows access points to detect Session Initiation Protocol (SIP) sessions, session establishment, and session termination. An access point reports statistics to the controller, which collects data about VoIP calls for a management station such as Cisco Prime Infrastructure. Further, when media session snooping is enabled, the controller generates a trap log for failed calls, indicating the time and reason for failure.

Tip For successful operation, media session snooping requires call control and establishment to be handled through the SIP. Media session snooping may not operate as expected if call control is performed through Signaling Connection Control Part (SCCP) or a SIP that is noncompliant with RFC 3261.

To configure media session snooping, use the following commands. Ensure that a voice WLAN is configured and SIP is used as a call control mechanism before using the commands.

```
Device(config)# wlan profile-name
Device(config-wlan)# call-snoop
```

To verify that media session snooping is enabled on a voice WLAN, use the following command:

```
Device# show wlan id wlan-id
.
.
.
Call Snooping                                    : Enabled
.
.
.
```

Quality of Service

For information about enabling quality of service (QoS) on the WLANs that service your enterprise network and configuration of QoS feature, see the Wireless QoS chapter.

Deploying WLANs

Defining WLANs

The wireless functionality in the Cisco Catalyst 3850 Series Switches and the Cisco Catalyst 3650 Series Switches supports up to 64 WLANs for lightweight access points (APs). Similarly, the Cisco 5700 Series Wireless Controllers support up to 512 WLANs for lightweight APs. Each WLAN ID has an associated profile name, WLAN identifier, and Service Set Identifier (SSID). A switch can publish up to 16 WLANs to a given AP.

Tip You can select the WLANs to be deployed to a given AP by placing the APs into access-point groups and then publishing the WLANs to that AP group. This helps you to segment and manage your wireless network in larger deployments.

To define a WLAN for corporate users, use the following command:

```
Device(config)# wlan profile-name wlan-id [ssid]
```

Note If you do not provide the SSID option, the *SSID* will be the same as the WLAN profile name.

To associate a WLAN with a client VLAN after the WLAN is created, use the following command:

```
Device(config-wlan)# client vlan vlan-id
```

After you run the command, any client joining the WLAN is placed into the specified VLAN. The *vlan-id* can be the VLAN name, numeric VLAN identifier, or a VLAN group name.

WLAN Security

AAA policies authenticate and authorize clients. To attach a configured AAA client authentication policy to a WLAN, use the following commands:

```
Device(config)# wlan profile-name
Device(config-wlan)# security dot1x authentication-list aaa-method-list
```

Tip WPA2 security with Advanced Encryption Standard (AES) ciphers is the default security for a new WLAN. To configure WPA security, for example, if you changed the security policy, use the **security wpa wpa2 ciphers aes** command.
For more information on WLAN security and configuring additional features, refer to the Configuring WLAN Security guide.

To verify the configuration, use the following command:

```
Device# show wlan id wlan-id
.
.
.
802.1x authentication list name                : aaa_method_list
.
.
.
    Wi-Fi Protected Access (WPA/WPA2)          : Enabled
        WPA (SSN IE)                           : Disabled
        WPA2 (RSN IE)                          : Enabled
            TKIP Cipher                        : Disabled
            AES Cipher                         : Enabled
```

Enabling a WLAN

By default, WLANs are shut down after they are created. This chapter describes how to make configuration changes to a WLAN while it is in the disabled state. Each configuration change to a WLAN requires pushing that configuration to the access points. Therefore, configurations on a WLAN requires the WLAN to be shut down.

To enable a WLAN in order to allow clients to connect, use the following command:

```
Device(config)# wlan  profile-name
Device(config-wlan)# no shutdown
```

To verify that the WLAN is operational, check the controller WLAN summary using the following command:

```
Device# show wlan summary

Number of WLANs: 1

WLAN Profile Name                     SSID                           VLAN Status
--------------------------------------------------------------------------------
id   profile_name                     ssid                           vlan UP
```

CHAPTER 8

Converged Access: Wireless AP and RF

This chapter describes the best recommendation or practices of Radio Resource Management (RRM), beam forming, Fast SSID, and Cisco CleanAir features.

The examples provided in this chapter are sufficient to enable a converged access network. However, we recommended that you familiarize yourself with the validated design topics covered in the technology design guide too.

Feature List

RRM Features

The following RRM features are covered in this chapter:

- RRM/RF grouping
- Transmit Power Control

- Dynamic channel assignment
- Coverage hole detection

Wireless AP Features

The following Wireless access point (AP) features are covered in this chapter:

- 802.11ac
- Beamforming
- Fast SSID Changing

Understanding Radio Resource Management

RRM helps in providing seamless wireless connectivity to end users or clients and provides a real-time RF management of a wireless network. RRM enables switches to continuously monitor their associated APs for the following information:

- Traffic load—The total bandwidth used for transmitting and receiving traffic. It enables wireless LAN managers to track and plan network growth ahead of the 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 Received Signal Strength (RSSI) and signal-to-noise ratio (SNR) for all the connected clients.

RRM performs the following functions to provide the best RF quality of wireless access to end users:

- RF Grouping
- Transmit Power control (TPC)
- Dynamic channel assignment (DCA)
- Coverage hole detection mitigation (CHDM)

Mobility Controller

A Mobility Controller performs the following roles in RRM:

- Mobility Controller can either be an RF group leader or a group member.
- One Mobility Controller can act as an RF group leader with other Mobility Controllers, based on RF grouping and RF group selection.
- The order of priority to elect the RF leader is based on the maximum number of APs the controller or switch can support.
- The group leader determines a channel and TX power plan for the network and passes the information back to the RF group members.

- The Mobility Controller pushes the power plan to a Mobility Agent to be used in the radios that belong to the Mobility Agent.
- These channel and power plans are ultimately pushed down to individual radios.

Mobility Agent

A Mobility agent performs the following roles in RRM:

- The Mobility Agent communicates with the Mobility Controller.
- The Mobility Controller includes the MAC or IP address of the switch or controller while communicating with the Mobility Agent.

The Mobility Controller exchanges the following information with the switch or controller (group member):

- Configurations (channel, power, channel width) for individual radios.
- Polling requests for current configurations and RF measurements for individual radios.

The Mobility Agent communicates the following messages with the Mobility Controller (group leader):

- RF measurements from radios (for example, load, noise, and neighbor information).
- RF capabilities and configurations of individual radios.

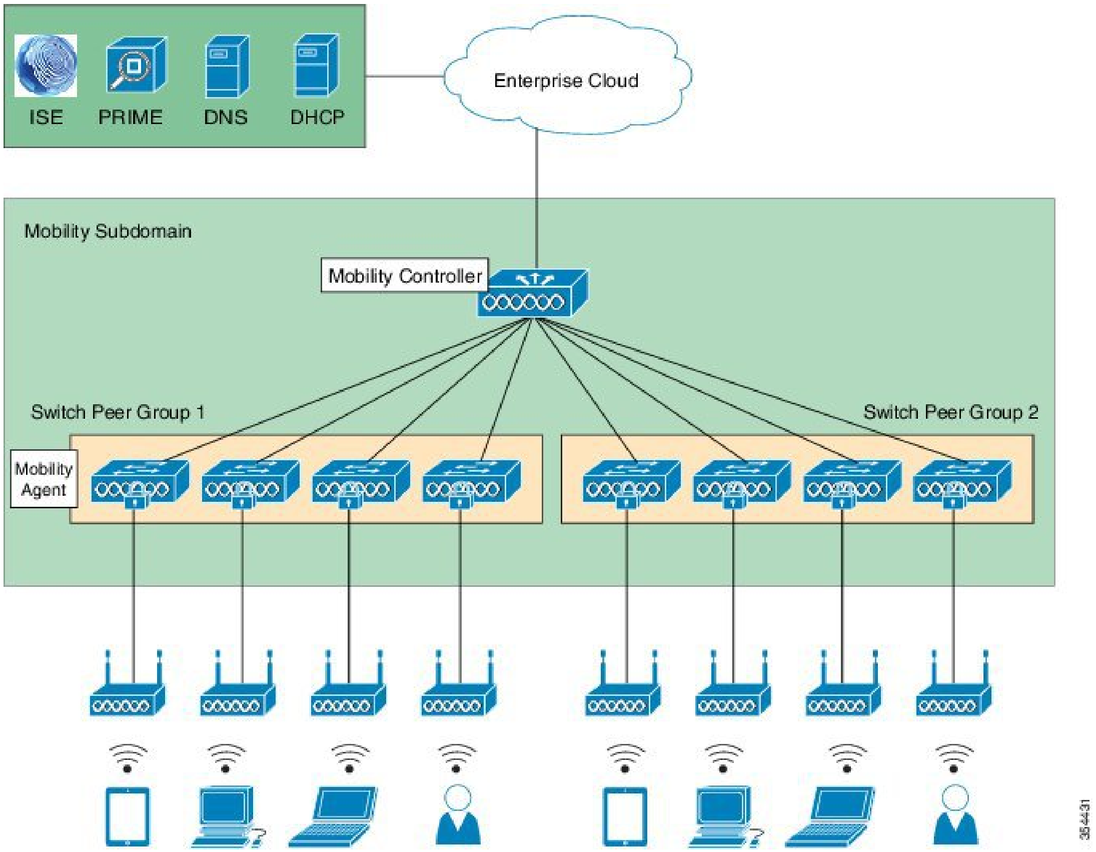
The Mobility Agent sets channel, power, and channel width on the radios when directed by the Mobility Controller.

Dynamic Frequency Selection (DFS), coverage hole detection or mitigation, static channel or power configurations are performed by the Mobility Agent.

Converged Access Topology Example

The following figure is used is to explain a converged access topology and for referencing configuration examples. It represents a typical converged access deployment scenario which covers most use cases. The Mobility Controller is found at the top of the diagram and is set up in as a stack for redundancy purposes. The switch stack connects to eight Mobility Agents which service the wireless clients. The eight Mobility Agents are divided equally into two different Switch Peer Groups (SPG). The entire setup belongs to a single mobility sub-domain. The access points connect directly to Mobility Agents, thus terminating CAPWAP tunnels on the Mobility Agents.

Figure 4: Converged Access Topology



Configuring RF and AP

Make sure you complete the following steps before you proceed:

- To configure RRM, configure the switch as a Mobility Controller.
- To enable RRM in converged access deployment, a mobility tunnel should be active between a Mobility Controller and Mobility Agent.

Note To learn more about RRM, refer to Radio Resource Management Configuration Guide, Cisco IOS XE Release 3E guide.

Configuring RF Grouping

Before You Begin

Before configuring RF grouping, ensure that you have created an RF group name and RF group leader, to run the subfunctions of TPC, DCA, and CHDM. The Mobility Controller is configured with an RF group name, which is sent to all APs points connected to the Mobility Controller. The RF group name is used by the APs as the shared secret for generating the hashed Message Integrity Check (MIC) in the neighbor messages.

Step 1 To create an RF group, configure all the Mobility Agents. Mobility Controllers in a mobility domain should also be included in the group, with the same RF group name. To configure Mobility Agents and include Mobility Controllers, use the following commands:

```
Device# configure terminal
Device(config)# wireless rf-network   name
Device(config)# end
```

Step 2 To verify the RF group name, use the following command:

```
Device# show wireless detail

RF network              : name
```

Configuring an RF Group Leader

Before You Begin

RF grouping must be enabled on the Mobility Controller as a first step to enable RRM in an RF domain. An RF leader contains the following three options:

- Auto—Selects the leader between two Mobility Controllers in a defined RF group.
- Static—Always a Leader.
- Off —Turns off RRM.

Perform the following steps to configure an RF group leader:

Step 1 To check the RF leader configuration, use the following command:

```
Device# show running-config

ap dot11 24ghz rrm group-mode auto
ap dot11 5ghz rrm group-mode auto

Device# end
```

Step 2 To verify the RF group leader on radio basis, use the following commands:

```
Device# show ap dot11 24ghz group
Device# show ap dot11 5ghz group
```

Configuring Transmit Power Control

Transmit Power Control (TPC) is configured to auto by default, per radio basis. We recommend that you retain the default configuration.

The Mobility Controller that is enabled as the RF leader dynamically controls access point (AP) transmit power under a real-time WLAN.

TPC seeks to lower an AP's power to reduce interference. However, in the case of sudden change in the RF coverage, for example, if an AP fails or becomes disabled, TPC can also increase power of the surrounding APs. This feature is different from coverage hole detection. While the coverage hole detection is connected to clients, TPC provides enough RF power to achieve the required coverage and avoid channel interference between APs.

Note TPC is useful in identifying coverage holes and adjust the power accordingly. This provides seemless connectivity to the clients.

Perform the following steps to configure TPC.

Step 1 To view the recommended and default configuration, use the following command. The default value is Auto.

```
Device# show running-config

ap dot11 24ghz rrm txpower auto
```

Step 2 To view the recommended and default configuration, use the following command. The default value is Auto.

```
Device# show running-config

ap dot11 5ghz rrm txpower 24ghz auto
```

Step 3 After configuring the TPC, adjust the TPC-threshold value to -70. Use the following commands to adjust the TPC-threshold:

```
Device(config)# ap dot11 5ghz rrm tpc-threshold -70
Device(config)# ap dot11 24ghz rrm tpc-threshold -70
```

Step 4 To verify the TPC, use the following commands:

```
Device# show ap dot11 24ghz txpower
Device# show ap dot11 5ghz txpower
```

Configuring Dynamic Channel Assignment

Two adjacent APs on the same channel can cause either channel contention or signal collision. In collision, data is not received by the corresponding AP. The dynamic channel assignment (DCA) is useful in minimizing adjacent channel interference between the APs.

DCA is enabled by default on the RF leader, and operates to adjust channels automatically on all the access points in that RF domain.

It is the best practice to let RRM automatically configure all the 802.11a and 802.11b org channels based on availability. The RF leader automatically adjusts the channel unless it is configured to a setting other than auto.

To configure DCA, perform the following steps:

Step 1 The recommended and default DCA configuration is Auto. Therefore, the channels will be picked and selected by RRM to avoid overlapping channels and interference. To verify the recommended and default DCA configuration, use the following commands:

```
Device# show running-config

ap dot11 24ghz rrm channel dca global auto
ap dot11 5ghz rrm channel dca global auto
```

Step 2 To configure DCA–assigned channel width to channel width capable radios, use the following command:

```
Device# ap dot11 5ghz rrm channel dca chan-width <20 | 40 |80>
```

Step 3 To verify DCA, use the following commands:

```
Device# show ap dot11 24ghz channel

  802.11b Auto-RF Allowed Channel List      : 1,6,11
  Auto-RF Unused Channel List               : 2,3,4,5,7,8,9,10

Device# show ap dot11 5ghz channel

  DCA 802.11n/ac Channel Width                 : 20 MHz
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
```

Configuring Coverage Hole Detection and Mitigation

Coverage Hole Detection and Mitigation (CHDM) is a per–controller configuration and not a global configuration. CHDM is enabled by default.

The RRM CHDM algorithm can detect areas of radio coverage in a wireless LAN that are below the level needed for robust radio performance. When an excising access point is relocated a notification is sent for additional access point .

The CHDM default values are sufficient for most environments. Unless directed otherwise, we recommend that you accept the default values.

To learn more about CHDM and coverage hole detection algorithm, refer to Radio Resource Management Configuration Guide, Cisco IOS XE Release 3E guide.

Tip For better CHDM monitoring, connect Cisco Prime to identify the areas for coverage and resolve client issues, if any. TPC gets adjusted automatically if there are issues in coverage, assuming that TPC is kept configured to the default value range.

Perform the following steps to configure and verify CHDM:

Step 1 To check if CHDM is enabled by default, use the following command:

```
Device# show running-config

ap dot11 24ghz rrm coverage
ap dot11 5ghz rrm coverage
```

Step 2 To verify CHDM, use the following commands:

```
Device# show ap dot11 24ghz coverage

Coverage Hole Detection
  802.11b Coverage Hole Detection Mode             : Enabled
  802.11b Coverage Voice Packet Count              : 100 packet(s)
  802.11b Coverage Voice Packet Percentage         : 50%
  802.11b Coverage Voice RSSI Threshold            : -80 dBm
  802.11b Coverage Data Packet Count               : 50 packet(s)
  802.11b Coverage Data Packet Percentage          : 50%
  802.11b Coverage Data RSSI Threshold             : -80 dBm
  802.11b Global coverage exception level          : 25 %
  802.11b Global client minimum exception level    : 3 clients

Device# show ap dot11 5ghz coverage

Coverage Hole Detection
  802.11a Coverage Hole Detection Mode          : Enabled
  802.11a Coverage Voice Packet Count           : 100 packet(s)
  802.11a Coverage Voice Packet Percentage      : 50 %
  802.11a Coverage Voice RSSI Threshold         : -80dBm
  802.11a Coverage Data Packet Count            : 50 packet(s)
```

```
802.11a Coverage Data Packet Percentage       : 50 %
802.11a Coverage Data RSSI Threshold          : -80dBm
802.11a Global coverage exception level       : 25
802.11a Global client minimum exception level   : 3 clients
```

Wireless AP Features

We recommend you to enable the wireless AP features because it helps in providing seamless roaming and connectivity.

Wireless and RF Prerequisites

Prior to wireless deployment, we recommend that you perform a thorough survey to ensure quality of service for your wireless clients. The requirements for voice and location deployments are stricter than for data services. Auto RF helps in channel and power settings management, but cannot correct a poor RF design.

A site survey must be performed with devices that match the power and propagation behavior of the devices to be used i n the real network. For example, do not use an older 802.11b or g radio with omni antenna to study coverage if you actual network will use a more modern dual radio for 802.11a or b org with n and 802.11ac data rates.

802.11ac

802.11ac provides enterprise networks with reliability and superior performance by supporting up to three spatial streams and 80-MHz-wide channels for a maximum data rate of 1.3 Gbps.

11ac feature allows companies to grow their network bandwidth dynamically for pervasive coverage or spot coverage, based on the high bandwidth demands of their user base, for example, in areas of high user congregation, such as libraries, cafeterias, and auditoriums. Companies have full control for how, where, and when to expand their wireless network.

802.11ac Data Rates(5 GHz)

802.11ac can support up to three spatial streams with MCS Index 9 and achieve data rate of 1300 Mbps for 80–MHz bandwidth with a guard interval of 400 ns.

Note 802.11ac with a 80–Mhz bandwidth can support up to a maximum of five non-overlapping channels.

For more information, refer to Cisco Aironet Access Point Module for 802.11ac Data Sheet.

Channel Widths

11ac allows the bonding of 20–MHz channels into an 80–MHz–wide channel for 802.11ac usage and all clients must support 80–MHz. We recommend that you have 80–MHz–wide channel bandwidth set to utilize the 802.11ac functionality.

Configuring Channel Width

To configure 80–MHz channel width on a particular AP point, use the following command: command:

```
Device(config)# ap name AP dot11 5ghz channel width 80
```

Beamforming

Beamforming is the primary method of improving downlink performance (AP to client) that takes advantage of the multiple Multiple-Input Multiple-Output (MIMO) transmitters on the AP. The use of beamforming on downlink transmissions often results in a more balanced level of performance between uplink and downlink.

Cisco ClientLink is an implicit beamforming method that adjusts the downlink phase of each individual orthogonal frequency-division multiplexing (OFDM) subcarrier on each transmit antenna based on uplink channel estimates.

Note The Cisco Aironet 3700 Series Access Point supports the Cisco ClientLink 3.0 and is able to beamform to 802.11ac clients, including 1, 2, and 3 spatial streams. It also supports all Cisco ClientLink 2.0 functionalities with legacy 11a org clients and 802.11n 1, 2, and 3 spatial stream clients.

The Cisco Aironet 3600 Access Points support Cisco ClientLink 2.0 which beamforms to legacy 11a or g clients and 11n 1, 2, 3 spatial stream, but does not support Cisco ClientLink 3.0 (beamforming to 11ac clients).

Configuring Beamforming

Perform the following steps to configure beamforming:

Step 1 To enable beamforming, use the following commands:

```
Device# configure terminal
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz beamforming
Device(config)# no ap dot11 5ghz shutdown
```

Step 2 To verify the beamforming status, use the following command:

```
Device# show ap dot11 5ghz network
```

```
Legacy Tx Beamforming setting: Enabled
```

Step 3 To disable beamforming, use the following command:.

```
Device(config)# no ap dot11 5ghz beamforming
```

Fast SSID Changing

When fast SSID changing is enabled, the controller allows clients to move faster between SSIDs. Also, the client entry is not cleared and the delay is not enforced.

Configuring Fast SSID Changing

Perform the following steps to configure the fast SSID changing feature:

Step 1 To enable fast SSID change, use the following commands:

```
Device# configure terminal
Device(config)# wireless client fast-ssid-change
```

Step 2 To verify the fast SSID change status, use the following command:

```
Device# show wireless detail
!
Fast SSID                  : Enabled
```

Cisco CleanAir

Cisco CleanAir technology uses silicon-level intelligence to create a spectrum-aware, self-healing, and self-optimizing wireless network that mitigates the impact of wireless interference, and offers performance protection for 802.11n and 802.11ac networks. All users of the shared spectrum can be seen (both native devices and foreign interferers). It also enables the network to act upon this information. For example, the interfering device can be manually removed or the system can automatically move the channel away from the source of interference.

To effectively detect and mitigate RF interference, enable Cisco CleanAir whenever possible.

Note Only Cisco CleanAir-enabled APs can perform Cisco CleanAir spectrum monitoring.

Enabling Cisco CleanAir

Cisco CleanAir is disabled by default and can only be enabled from a Mobility Controller. To enable Cisco CleanAir, perform the following steps:

Step 1 To configure the Cisco CleanAir functionality to receive spectrum data on a 802.11 network, use the following commands:

```
Device(config)# ap dot11 24ghz cleanair
Device(config)# ap dot11 5ghz cleanair
```

Step 2 To enable interference detection, for example, from a jammer, use the following commands:

```
Device(config)# ap dot11 5ghz cleanair device jammer
Device(config)# ap dot11 24ghz cleanair device bluetooth
```

Step 3 To verify if Cisco CleanAir is enabled on the 802.11 networks, use the following command:

```
Device# show ap dot11 24ghz cleanair config

CleanAir Solution............................... : Enabled
```

For more information, refer to Configuring Cisco CleanAir Guide.

Data Rates

You must carefully plan the process to disable or enable data rates. If your coverage is sufficient, you can incrementally disable lower data rates one by one. Management frames such as ACK or beacons will be sent at the lowest mandatory rate (typically 1 Mbps), which slows down the entire throughput (the lowest mandatory rate consumes the most airtime).

We recommend that you do not have too many supported data rates so that clients can downshift their rate faster when re-transmitting. Typically, clients try to send at the fastest data rate they can, and if the frame does not make it through, they retransmit at the next lowest data rate, and so on until the frame goes through. The removal of some supported rates means that clients who retransmit a frame directly, downshift several data rates, which increases a frame's chance to go through at the second attempt.

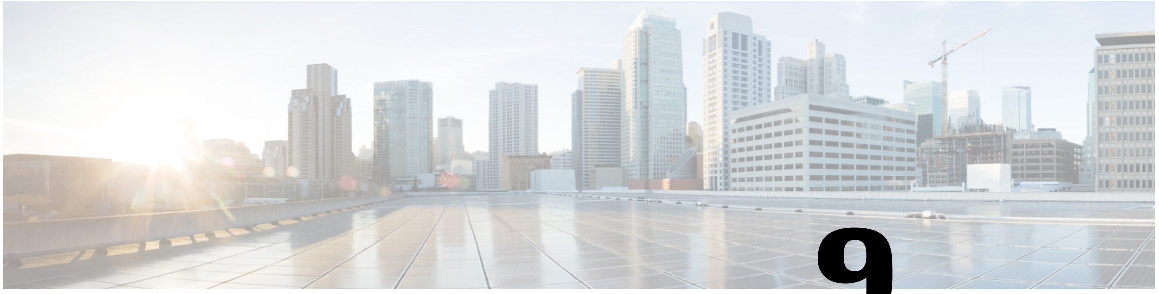
- If your design does not require low data rates, consider disabling the 802.11b data rates (1, 2, 5.5, and 11) and leave the rest enabled.
- You by make a conscious decision to not disable rates below 11 Mbps in order to not stop the support of 802.11b-only clients.

Note The following example should not be used as a strict guideline for every design. Note that these changes are sensitive and dependent on your RF coverage design. Conversely, if you are designing for a high-speed network that already has good RF coverage, disable the lowest data rate.

The following example shows how to disable low data rates (5 GHz and 2.4 GHz):

```
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz rate RATE_6M disable
Device(config)# ap dot11 5ghz rate RATE_9M disable
Device(config)# ap dot11 5ghz rate RATE_12M disable
Device(config)# ap dot11 5ghz rate RATE_18M disable
Device(config)# ap dot11 5ghz rate RATE_24M mandatory
Device(config)# ap dot11 5ghz rate RATE_36M supported
Device(config)# ap dot11 5ghz rate RATE_48M supported
Device(config)# ap dot11 5ghz rate RATE_54M supported
Device(config)# no ap dot11 5ghz shutdown

Device(config)# ap dot11 24ghz shutdown
Device(config)# ap dot11 24ghz dot11g
Device(config)# ap dot11 24ghz dot11n
Device(config)# ap dot11 24ghz rate RATE_24M mandatory
Device(config)# ap dot11 24ghz rate RATE_1M disable
Device(config)# ap dot11 24ghz rate RATE_2M disable
Device(config)# ap dot11 24ghz rate RATE_5_5M disable
Device(config)# ap dot11 24ghz rate RATE_6M disable
Device(config)# ap dot11 24ghz rate RATE_9M disable
Device(config)# ap dot11 24ghz rate RATE_11M disable
Device(config)# ap dot11 24ghz rate RATE_12M supported
Device(config)# ap dot11 24ghz rate RATE_18M supported
Device(config)# ap dot11 24ghz rate RATE_36M supported
Device(config)# ap dot11 24ghz rate RATE_48M supported
Device(config)# ap dot11 24ghz rate RATE_54M supported
Device(config)# no ap dot11 24ghz shutdown
```



CHAPTER 9

Converged Access: Wireless QoS

This chapter describes how to configure the granular wireless quality of service (QoS) feature on a converged access network, which contains Cisco Catalyst 3850 Series and Cisco Catalyst 3650 Series Switches. This chapter also provides information on Wired QoS with reference to Wired AutoQoS.

Converged Access QoS

Converged Access QoS consists of Wired and a Wireless QoS components. In the context of wired QoS, you can use the Wired AutoQoS depending on the type of wired devices attached to the converged access switches (such as, Cisco-Phone, Cisco-Softphone, Cisco Telepresence System (CTS), Cisco video surveillance camera, Cisco Delivery Protocol (CDP)-capable Cisco digital media player, trusted devices, untrusted devices, and so on).

In the context of wireless QoS, the Cisco Catalyst 3850 Series and the Cisco Catalyst 3650 Series Switches have advanced wireless QoS capabilities. This ensures guaranteed bandwidth or services at a granular level, that includes access-point port, radio, SSID, and client levels. In the past, wireless networks lacked QoS visibility and enforcement and were vulnerable to unfair bandwidth allocation because QoS could not be applied inside the wireless tunnels. Converged Access switches terminate the wireless tunnels. Hence, QoS can be applied much closer to users.

For more information about configuring wired and wireless components, refer to the “Configuring Auto-QoS” chapter in the *QoS Configuration Guide*.

Note An Auto QOS policy, CAPWAP AP, is added on the AP connected port on Cisco Catalyst 4500 Series Switches, to prioritize wireless traffic.

```
Device# show run interface GigabitEthernet 1/43
Building configuration...

Current configuration : 196 bytes

!

interface GigabitEthernet 1/43

 switchport access vlan 60

 switchport mode access

 datalink flow monitor mac input

 spanning-tree portfast

 service-policy output Capwap-SRND4-Queuing-Policy

end

Policy Map Capwap-SRND4-Queuing-Policy

    Class Capwap-Priority-Queue

      priority

    Class Capwap-Control-Mgmt-Queue

      bandwidth remaining 10 (%)

    Class Capwap-Multimedia-Conf-Queue

      bandwidth remaining 10 (%)

    Class Capwap-Multimedia-Stream-Queue

      bandwidth remaining 10 (%)

    Class Capwap-Trans-Data-Queue

      bandwidth remaining 10 (%)

    Class Capwap-Bulk-Data-Queue

      bandwidth remaining 4 (%)

    Class Capwap-Scavenger-Queue

      bandwidth remaining 1 (%)

    Class class-default

      bandwidth remaining 25 (%)
```

A converged access switch is capable of automatically allocating equal bandwidth among the connected users within a given SSID, with the help of the Approximate Fair Dropping (AFD) algorithm. This algorithm ensures that all the users within an SSID receive a fair share of the available bandwidth while they are connected to the network.

The purpose of the Converged Access: Wireless QoS chapter is to provide necessary guidance with the help of template policy definitions. These can either be utilized as-is or can be used as base policies that can be modified for a particular deployment.

To simplify the guidance, we have selected WLAN Enterprise, which is a commonly used SSID in most deployments, and also recommended the relevant Wireless QoS policies.

Supported Policies for Wireless Targets

Note

- Downstream Direction—From Controller to Access Point Traffic
- Upstream Direction—From Access Point to Controller Traffic

The following table provides information about the supported policies for wireless targets:

Table 5: Supported Policies for Wireless Targets

Wireless Target	Policy Supported on Wireless Targets	Policy Supported in Downstream Direction	Policy Supported in Upstream Direction
Wireless Port	Yes	Yes—User configurable	No
Radio	Yes	Yes—Not user configurable	No
SSID	Yes	Yes—User configurable	Yes—User configurable
Client	Yes	Yes—User configurable	Yes—User configurable

Note For more information on the Converged Access QoS concepts and configurations, refer to the "Configuring QoS" chapter in the *QoS Configuration Guide*.

Configuring ACL and Class Map

Configuring ACL Definitions

To configure ACL definitions, use the following commands:

```
!!
!!
!! Ingress Access Lists for QoS
!
!
Device(config)# ip access-list extended MultiEnhanced-Conf
```

```
 ! Real-Time Transport Protocol Traffic

Device(config-ext-nacl)# permit udp any any range 16384 32767
Device(config-ext-nacl)# exit

Device(config)# ip access-list extended Transactional-Data
 ! HTTPS

Device(config-ext-nacl)# permit tcp any any eq 443
 ! Oracle application

Device(config-ext-nacl)# permit tcp any any eq 1521
 ! nCube License Manager

Device(config-ext-nacl)# permit udp any any eq 1521
 ! Oracle Database common alternative

 Device(config-ext-nacl)# permit tcp any any eq 1526
 ! Prospero Data Access

 Device(config-ext-nacl)# permit udp any any eq 1526
 ! Oraclenames

 Device(config-ext-nacl)# permit tcp any any eq 1575
 ! Oraclenames

Device(config-ext-nacl)# permit udp any any eq 1575
 ! Oracle Net8 Cman

Device(config-ext-nacl)#  permit tcp any any eq 1630
 ! Oracle Net8 Cman

Device(config-ext-nacl)# permit udp any any eq 1630
Device(config-ext-nacl)# exit

Device(config)# ip access-list extended Bulk-Data
 ! SSH

Device(config-ext-nacl)# permit tcp any any eq 22
 ! SMTP-SSL

Device(config-ext-nacl)# permit tcp any any eq 465
 ! IMAP

Device(config-ext-nacl)# permit tcp any any eq 143
 ! IMAP-SSL

Device(config-ext-nacl)# permit tcp any any eq 993
 ! POP3-SSL

Device(config-ext-nacl)# permit tcp any any eq 995
 ! Elm-Momentum

Device(config-ext-nacl)# permit tcp any any eq 1914

 Device(config-ext-nacl)# permit tcp any any eq ftp

Device(config-ext-nacl)# permit tcp any any eq ftp-data

Device(config-ext-nacl)# permit tcp any any eq smtp

Device(config-ext-nacl)# permit tcp any any eq pop3
Device(config-ext-nacl)# exit

Device(config)# ip access-list extended Scavenger
 ! Chessmaster

Device(config-ext-nacl)# permit tcp any any range 2300 2400
 ! Chessmaster

Device(config-ext-nacl)# permit udp any any range 2300 2400
 ! Bit Torrent
```

```
Device(config-ext-nacl)# permit tcp any any range 6881 6999
 ! MSN Game Zone

Device(config-ext-nacl)#  permit tcp any any range 28800 29100
 ! Kazaa, Grokster

Device(config-ext-nacl)# permit tcp any any eq 1214
 ! Kazaa, Grokster

Device(config-ext-nacl)# permit udp any any eq 1214
 ! iTunes Music sharing

Device(config-ext-nacl)# permit tcp any any eq 3689
 ! Digital Audio Access Protocol

Device(config-ext-nacl)# permit udp any any eq 3689
 ! Yahoo Games

Device(config-ext-nacl)#  permit tcp any any eq 11999
```

Configuring Class Map Definitions

To configure class map definitions, use the following commands:

```
!!
!!
!! Class-Maps for Ingress Policies
!
!
Device(config)# class-map match-any Voip-Data-Class
Device(config-cmap)# match dscp ef
Device(config-cmap)# exit

Device(config)# class-map match-any Voip-Signal-Class
Device(config-cmap)# match dscp cs3
Device(config-cmap)# exit

Device(config)# class-map match-any Multimedia-Conf-Class
Device(config-cmap)# match access-group name MultiEnhanced-Conf
Device(config-cmap)# exit

Device(config)# class-map match-any Transaction-Class
Device(config-cmap)# match access-group name Transactional-Data
Device(config-cmap)# exit

Device(config)# class-map match-any Bulk-Data-Class
Device(config-cmap)# match access-group name Bulk-Data
Device(config-cmap)# exit

Device(config)# class-map match-any Scavenger-Class
Device(config-cmap)# match access-group name Scavenger
Device(config-cmap)# exit
!!
!!
!! Two realtime classes for Voice and Video used with egress policies
!
!
Device(config)# class-map match-any RT1-Class
Device(config-cmap)# match dscp ef
Device(config-cmap)# match dscp cs6
Device(config-cmap)# exit

Device(config)# class-map match-any RT2-Class
Device(config-cmap)# match dscp cs4
Device(config-cmap)# match dscp cs3
Device(config-cmap)# exit
```

Wireless Ingress QoS

For wireless ports, the default system behavior is non-trust, which implies that when the switch is booted, all markings for the wireless ports are defaulted to zero and no traffic is prioritized. Disable the non-trust configuration before you continue with the wireless ingress configuration.

To disable the default non-trust of QoS markings, use the following command:

```
Device(config)# no qos wireless-default-untrust
```

Enterprise WLAN Client Ingress Policy

Before you begin, make sure that the relevant Enterprise WLAN already exists on the switch.

In the context of Enterprise WLAN, the enterprise WLAN client ingress policy re-marks the ingress traffic as per the traffic type at the client level. We recommend that you re-mark the various types of ingress traffic at the client-level.

To re-mark the ingress traffic using enterprise WLAN client ingress policy, use the following commands:

```
Device(config)# policy-map client_input_policy
Device(config-pmap)# class Voip-Data-Class
Device(config-pmap-c)# set dscp ef
Device(config-pmap-c)# exit

Device(config-pmap)# class Voip-Signal-Class
Device(config-pmap-c)# set dscp cs3
Device(config-pmap-c)# exit

Device(config-pmap)# class Multimedia-Conf-Class
Device(config-pmap-c)# set dscp af41
Device(config-pmap-c)# exit

Device(config-pmap)# class Transaction-Class
Device(config-pmap-c)# set dscp af21
Device(config-pmap-c)# exit

Device(config-pmap)# class Bulk-Data-Class
Device(config-pmap-c)# set dscp af11
Device(config-pmap-c)# exit

Device(config-pmap)# class Scavenger-Class
Device(config-pmap-c)# set dscp cs1
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp default
Device(config-pmap-c)# exit
```

To apply the enterprise WLAN client ingress policy, use the following commands:

```
Device(config)# wlan profile-name
Device(config-wlan)# service-policy client input client_input_policy <<<< The client keyword
 is included since this policy is applied at the client level.
```

Wireless Egress QoS

Wireless egress QoS can be applied at multiple places in the wireless egress path such as the port, radio, SSID, and Client levels. The wireless egress policy enables you to fine-tune the performance of the converged access switches during congestion.

An effective port-level egress QoS policy uses class maps to classify traffic into priority and nonpriority queues. The port-child-policy port-level egress policy defines the QoS policy of the directly connected access point. All the access points receive the same egress QoS policy. If you do not apply the QoS policies at instances such as radio and client, all the egress traffic for wireless interfaces are subjected to the same behavior, as per the policy.

At the port-child-policy port level, the policy model has four Egress Queues, two priority queues, and two non-priority queues. The policy model does not have any drop thresholds. The port-child-policy is a built-in policy map that is implicitly applied to the wireless interfaces. To modify the port-level policy, use the following commands:

```
Device(config)# class-map RTI-class
Device(config-cmap)# exit
Device(config)# class-map RT2-class
Device(config-pmap-c)# exit
!

Device(config)# policy-map port-child-policy
Device(config-pmap)# class non-client-nrt-class
Device(config-pmap-c)# bandwidth remaining ratio 7
Device(config-pmap-c)# exit
Device(config-pmap)#   class RTI-class
Device(config-pmap-c)# priority level 1 percent 10
Device(config-pmap-c)# exit
Device(config-pmap)#   class RT2-class
Device(config-pmap-c)# priority level 2 percent 20
Device(config-pmap-c)# exit
Device(config-pmap)#  class class-default
Device(config-pmap-c)# bandwidth remaining ratio 63
Device(config-pmap-c)# end
```

Note The port-child-policy is applied implicitly, as soon as an access point is connected and is detected on the interface.

Enterprise WLAN SSID Egress Policy

Use the SSID-level policy maps to allocate bandwidth as per the SSID. This enables you to prioritize the traffic of one SSID during congestion.

Enterprise WLAN SSID egress is a hierarchical policy in which the parent policy shapes up to 100% of the available radio bandwidth. The child policy defines the relevant policy values for the real time priority queues (for voice and video). The **bandwidth remaining ratio** command ensures that the required bandwidth is maintained as compared to the remaining SSIDs. You can change this value based on a specific requirement.

To run the Enterprise WLAN SSID egress policy, use the following commands:

```
Device(config)# policy-map SSID_child_policy
Device(config-pmap)# class RT1-Class
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police 15000000 conform-action transmit exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class RT2-Class
Device(config-pmap-c)# priority level 2
Device(config-pmap-c)# police 30000000 conform-action transmit exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap)# exit

Device(config)# policy-map SSID-output-policy
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average percent 100
Device(config-pmap-c)# queue-buffers ratio 0
Device(config-pmap-c)# bandwidth remaining ratio 70
Device(config-pmap-c)# service-policy SSID-child-policy
```

To apply the Enterprise VLAN SSID egress policy, use the following commands:

```
Device(config)# wlan profile-name
Device(config-wlan)# Service-policy output SSID-output-policy
```

Note After you configure the **bandwidth remaining ratio** command on one SSID, it must be configured on all the available SSIDs in the deployment in order to have a predictable behavior.

Note The radio-level egress policies and the client-level egress policies cannot be defined as already mentioned in this document.

Verifying a Policy Installation

To verify the port-level policy that is installed, use the following commands. The interface in the example below is the interface connected to the access point.

```
Device# show platform qos policies PORT

Loc Interface          IIF-ID             Dir Policy             State
--- ------------------ ------------------ --- ------------------ ---------------
.
.
.
L:1 interface          iif-id             OUT port_child_policy  INSTALLED IN HW

Device# show policy-map interface interface
 interface
.
.
.
        Class-map: non-client-nrt-class (match-any)
          Match: non-client-nrt
            0 packets, 0 bytes
            5 minute rate 0 bps
          Queueing

          (total drops) 0
          (bytes output) 68206789
          bandwidth remaining ratio 7

        Class-map: RT1-Class (match-any)
          Match:  dscp ef (46)
            0 packets, 0 bytes
            5 minute rate 0 bps
          Match:  dscp cs6 (48)
            0 packets, 0 bytes
            5 minute rate 0 bps
          Priority: 10% (60000 kbps), burst bytes 1500000,

          Priority Level: 1

        Class-map: RT2-Class (match-any)
          Match:  dscp cs4 (32)
            0 packets, 0 bytes
            5 minute rate 0 bps
          Match:  dscp cs3 (24)
            0 packets, 0 bytes
            5 minute rate 0 bps
          Priority: 20% (120000 kbps), burst bytes 3000000,

          Priority Level: 2

        Class-map: class-default (match-any)
          Match: any
            0 packets, 0 bytes
            5 minute rate 0 bps
          Queueing

          (total drops) 0
          (bytes output) 0
          bandwidth remaining ratio 63
```

To verify an SSID-level policy that is installed, use the following commands:

```
Device# show platform qos policies SSID

Loc Interface     IIF-ID   Dir Policy                         State
--- ------------- -------- --- ----------------------------- ---------------
.
.
.
L:1 interfaceID   iif-id   OUT SSID_output_policy            INSTALLED IN HW
L:1 interfaceID   iif-id   OUT SSID_child_policy             INSTALLED IN HW

Device# show policy-map interface wireless SSID name profileName

SSID profileName iifid: 0x0108B80000000025.0x00E447800000010B.0x00EF19000000012E

  Service-policy output: SSID_output_policy

    Class-map: class-default (match-any)
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      shape (average) cir 200000000, bc 800000, be 800000
      target shape rate 200000000
      queue-buffers ratio 0
      bandwidth remaining ratio 70

      Service-policy : SSID_child_policy

        Class-map: RT1-Class (match-any)
          Match:  dscp ef (46)
            0 packets, 0 bytes
            30 second rate 0 bps
          Match:  dscp cs6 (48)
            0 packets, 0 bytes
            30 second rate 0 bps
          Priority: Strict,

          Priority Level: 1
          police:
              cir 15000000 bps, bc 468750 bytes
            conformed 0 bytes; actions:
              transmit
            exceeded 0 bytes; actions:
              drop
            conformed 0000 bps, exceed 0000 bps

        Class-map: RT2-Class (match-any)
          Match:  dscp cs4 (32)
            0 packets, 0 bytes
            30 second rate 0 bps
          Match:  dscp cs3 (24)
            0 packets, 0 bytes
            30 second rate 0 bps
          Priority: Strict,

          Priority Level: 2
          police:
              cir 30000000 bps, bc 937500 bytes
            conformed 0 bytes; actions:
              transmit
            exceeded 0 bytes; actions:
              drop
            conformed 0000 bps, exceed 0000 bps

        Class-map: class-default (match-any)
          Match: any
            0 packets, 0 bytes
            30 second rate 0 bps
.
.
.
```

To verify a client-level policy that is installed, use the following commands:

```
Device# show platform qos policies CLIENT

Loc Interface        IIF-ID Dir Policy                        State
--- ---------------- ------ --- ----------------------------- ---------------
L:1 ClientMACAddress iif-id IN  client_input_policy INSTALLED IN HW
.
.
.

Device# show policy-map interface wireless client mac ClientMACAddress

Client ClientMACAddress ..
.
.
.

  Service-policy input: client-input-policy

    Class-map: Voip-Data-Class (match-any)
      Match:  dscp ef (46)
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp ef

    Class-map: Voip-Signal-Class (match-any)
      Match:  dscp cs3 (24)
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp cs3
    Class-map: Multimedia-Conf-Class (match-any)
      Match: access-group name MultiEnhanced-Conf
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp af41

    Class-map: Transaction-Class (match-any)
      Match: access-group name Transactional-Data
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp af21

    Class-map: Bulk-Data-Class (match-any)
      Match: access-group name Bulk-Data
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp cs1

    Class-map: class-default (match-any)
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp default

Device# show policy-map client mac-address ClientMACAddress service-policy input

Wireless Client QoS Service Policy
Policy Name  : client_input_policy
Policy State : Installed
```

To verify a radio-level policy, which is on by default, use the following command:

```
Device# show platform qos policies RADIO

Loc Interface          IIF-ID             Dir Policy             State
--- ------------------ ------------------ --- ------------------ ---------------
L:1 R71187880340357388 0x00fce9000000010c OUT def-11an           INSTALLED IN HW
.
.
.
```

To verify a QoS policy based on the WLAN, use the following commands:

```
Device# show wlan name profileName | include Policy

AAA Policy Override                            : Disabled
QoS Service Policy - Input
  Policy Name                                  : unknown
  Policy State                                 : None
QoS Service Policy - Output
  Policy Name                                  : SSID-output-policy
  Policy State                                 : Validated
QoS Client Service Policy
  Input  Policy Name                           : client_input_policy
  Output Policy Name                           : unknown
Radio Policy                                   : All
```