Cisco 8500 Series Wireless Controller Deployment Guide

Document ID: 113695

Contents

Introduction

This document introduces the Cisco 8500 Wireless LAN Controller (WLC), and provides general guidelines for its deployment. The purpose of this document is to:

- Provide an overview of the Cisco 8500 WLC, and its deployment within the Cisco Unified Architecture.
- Highlight key Service Provider features
- Provide design recommendations and considerations specific to the Cisco 8500 Controller.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

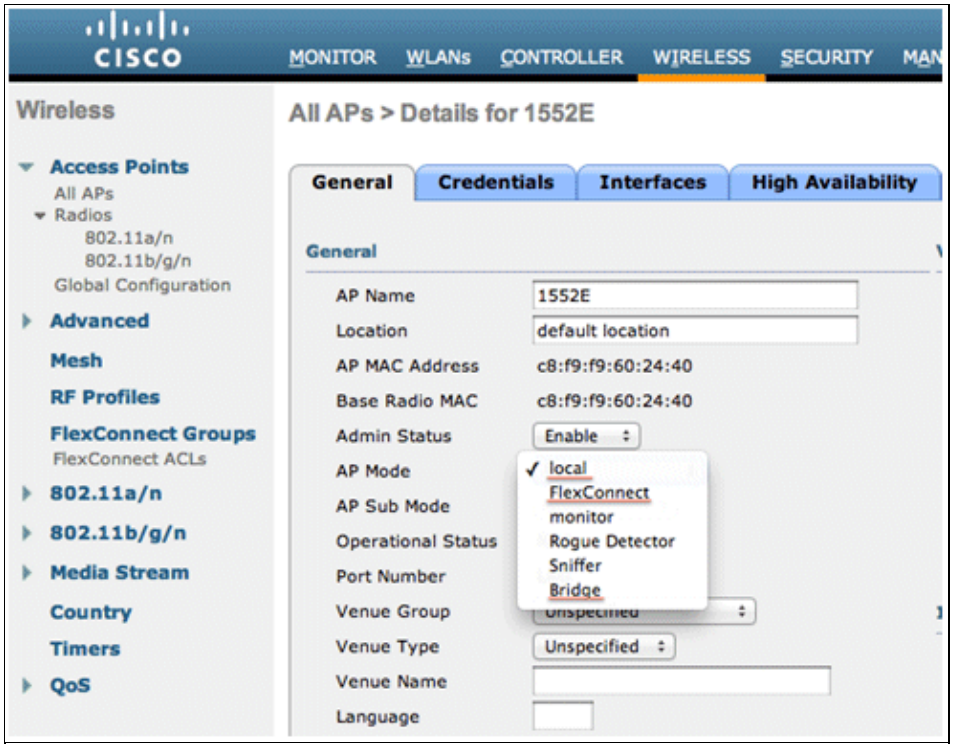
Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Product Overview

In Cisco Unified Architecture, a wireless access point (AP) is deployed in one of three major modes in order to serve wireless clients:

- **Local mode** − A Local mode AP tunnels all traffic to the Controller (via CAPWAP), where the Controller handles tagging the packets and placing them on the wired network.
- **FlexConnect mode** − FlexConnect mode is primarily designed to support wireless branch networks by allowing the data to be switched locally (with support for central switching at the Controller), while the APs are controlled and managed over a WAN connection by a centralized controller. The traffic flow from a FlexConnect AP can take the most efficient path as the administrator has the flexibility to configure certain types of traffic to be switched locally, or have it tunneled to be centrally switched at the Controller in the central site. For more information on FlexConnect Theory of Operations, refer to the H−Reap/FlexConnect Design Guide and the Cisco Flex 7500 Deployment Guide.
- **Bridge mode** − An AP in Bridge mode is configured to build a wireless Mesh network where wired network cabling is not available. For more information on Mesh theory of operation, refer to the Mesh Design and Deployment Guide.



Both the Cisco 5500 Series Controller and the WiSM2 Controller support all modes of AP operation scaling up to 500 and 1000 APs respectively, and 7000 and 15,000 wireless clients respectively. The explosion of mobile clients in enterprise empowered by bring your own device (BYOD), the deployment of wireless in mission−critical applications, and the adoption of Wi−Fi in service provider networks enabling new business models require wireless networks to provide higher client scale, greater resiliency and seamless IP mobility between cellular and Wi−Fi networks. The Cisco Unified Wireless Network Software Release 7.3 addresses these key challenges. Release 7.3 delivers the new Cisco 8500 Series Wireless Controller with a highly scalable client count, a high−availability (HA) feature that minimizes controller downtime by enabling sub−second failover of thousands of access points to a standby controller, and service provider features such as Wi−Fi Certified Passpoint (HS2.0) for secure public connectivity and Proxy Mobile IPv6 (PMIPv6) to ensure seamless mobility between Cellular and Wi−Fi.

Some of the key attributes of the Cisco 8500 Controller are:

- High client density (64,000 clients in 1 RU)
- Support for 6000 APs, 6000 AP groups, 2000 FlexConnect groups, and up to 100 APs per FlexConnect group
- Support for 4096 VLANs
- Support for 50,000 RFIDs tracking, and the detection and containment of up to 24,000 rogue APs, and up to 32,000 rogue clients
- HA with Sub−second AP Stateful Switchover
- Outdoor AP support
- Support of all AP modes of operation (local, FlexConnect, monitor, Rogue Detector, Sniffer, and Bridge)
- Seamless Mobility with the Packet Core network with PMIPv6 MAG implementation (RFC 5213)
- WFA Passpoint Certified (in progress − check the WFA web site for the latest status)
- 802.11r fast roaming
- Bi−directional Rate limit of traffic flows
- Video Stream for rich media flows
- Right to Use (RTU) licensing for ease of license enablement and ongoing licensing operations

This table shows the Cisco high−scale Controllers comparison at a glance:

	8500	7500	5500	WiSM2
Deployment type	Enterprise Large campus + SP Wi−Fi	Central site Controller for large number of distributed, controller−less branches	Enterprise Campus and full service branch	Enterprise Campus
Operational Modes	Local mode, FlexConnect, Mesh	FlexConnect only	Local mode, FlexConnect, Mesh	Local mode, FlexConnect, Mesh
Maximum Scale	6000 APs	6000 APs	500 APs 7000	1000 APs
AP Count Range	64,000 clients 300 k APs	64,000 clients 300 k APs	clients 12 00 APs	15,000 clients 100™000 APs
Licensing	Right to Use (with EULA)	Right to Use (with EULA)	CISL based (unchanged)	CISL based (unchanged)
Connectivity	2x10G ports	2x10G ports	8x1G ports	Internal connections to the Catalyst Backplanes
Power	AC/DC dual redundant	AC dual redundant	AC (redundant PSU option)	AC/DC Catalyst chassis redundant PSU option
Maximum Number of FlexConnect Groups	2000	2000	100	100
Maximum Number of APs per FlexConnect Group	100	100	25	25
Maximum Number of Rogue APs Management	24,000	24,000	2000	4000
Maximum Number of Rogue Clients Management	32,000	32,000	2500	5000
Maximum Number of RFID	50,000	50,000	5000	10,000

Maximum APs per RRM Group	6000	6000	1000	2000
Maximum AP Groups	6000	6000	500	500
Maximum Interface Groups	512	512	64	64
Maximum Interfaces per Interface Group	64	64	64	64
Maximum VLANs Supported	4096	4096	512	512
Maximum WLANs Supported	512	512	512	512
Supported Fast Secure Roaming (FSR) Clients*	64000	64000	14000	30000

***** Supported number of FSR clients back and forth to this platform (more details in the Design Considerations section under Inter−Platform Mobility).

Product Specifications

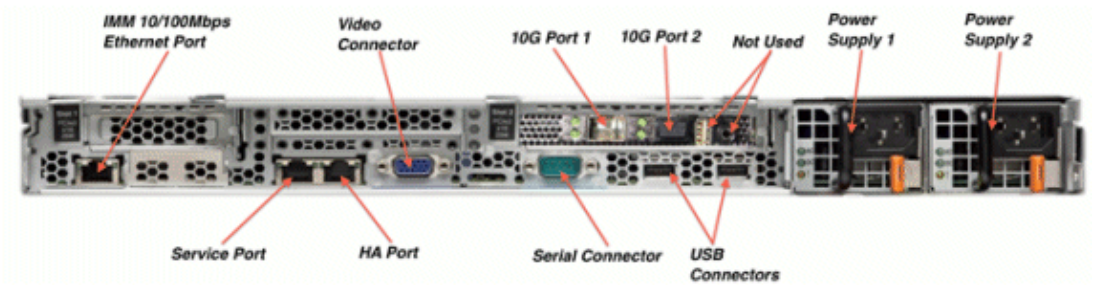
Data Sheet

Refer to the Cisco 8500 Series Controller Data Sheet.

Platform Feature

Front view:

Rear View:



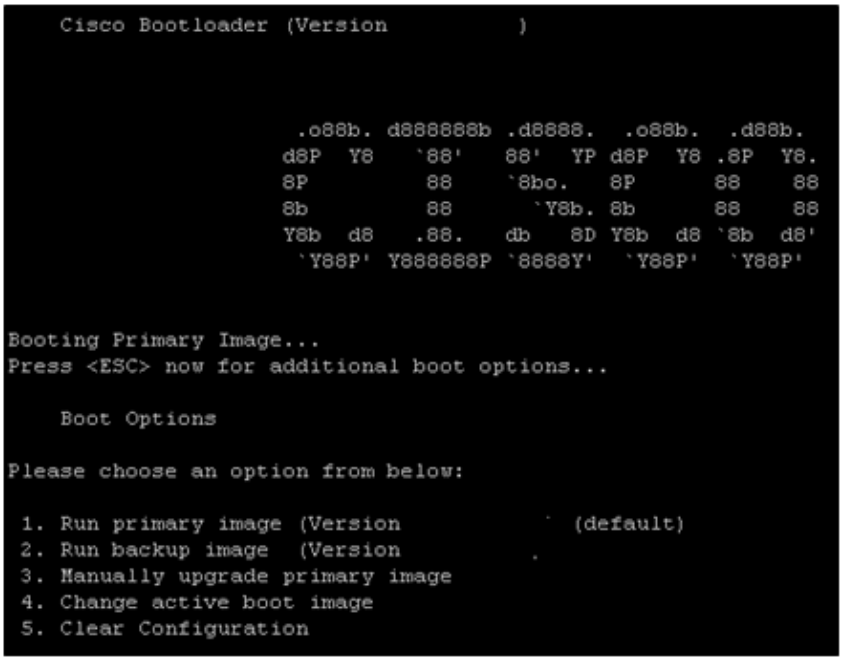
Features not Currently Supported on the 8500 Controller Platform

These features are not currently supported on the 8500 Controller platform:

- Local Authentication (where the Controller acts as the authentication server)
- Internal DHCP server
- Wired Guest
- TrustSec SXP

Look and Feel of the Cisco 8500 Controller

The Cisco 8500 Controller enables console redirect by default with baud rate 9600 simulating a VT100 terminal with no flow control. The 8500 Controller has the same boot sequence as existing controller platforms.

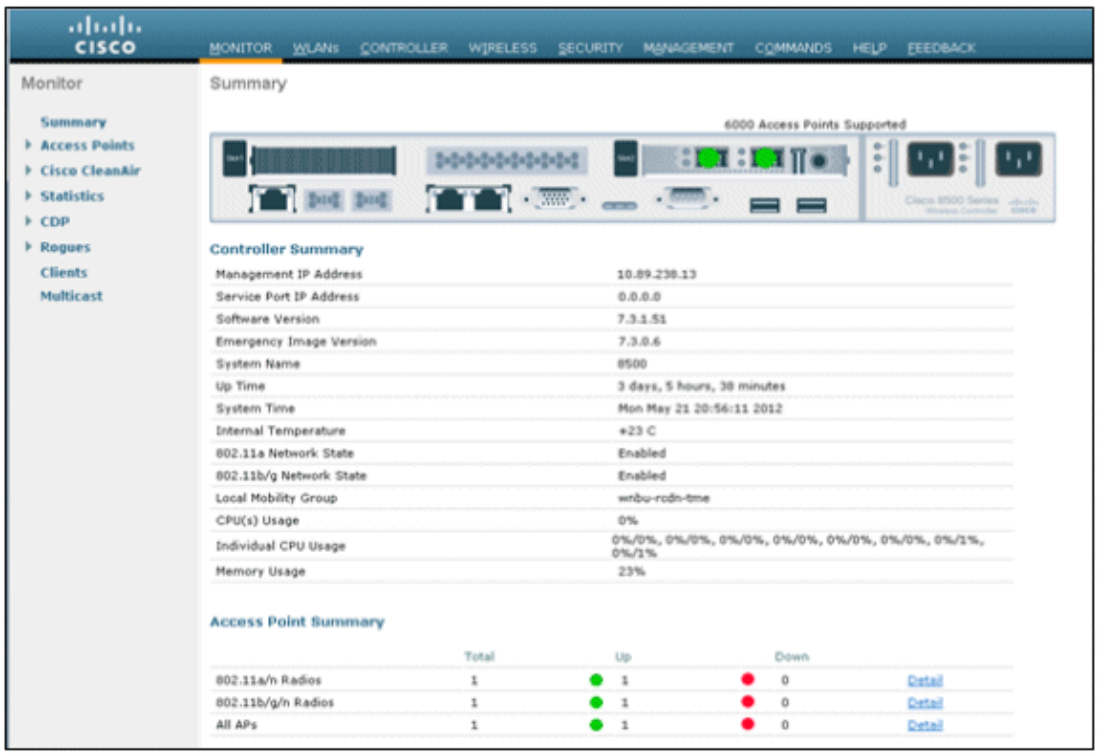


As with all other controller platforms, initial boot up requires configuration using the Wizard menu.

```
Would you like to terminate autoinstall? [yes]:

System Name [Cisco_65:db:6c] (31 characters max):
AUTO-INSTALL: process terminated -- no configuration loaded

Enter Administrative User Name (24 characters max): admin
Default values (admin or Cisco or its variants) in password is not allowed.
Enter Administrative Password (24 characters max): *******
Re-enter Administrative Password                  : *******

Management Interface IP Address: 172.20.227.174
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 172.20.227.161
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 2]: 1
Management Interface DHCP Server IP Address: 172.20.227.161

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: mobility

Network Name (SSID): DataCenter

Configure DHCP Bridging Mode [yes][NO]: NO

Allow Static IP Addresses [YES][no]: Yes

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]:

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: 09/02/10
Enter the time in HH:MM:SS format: 11:50:00

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

Management Port 1: 10G

The GUI also remains the same as previous controllers.



Highlighted Features in the Cisco 8500 Controller

Scalability

The Cisco 8500 Series WLC provides Service−Provider−class scalability in a small 1RU form factor. It allows Service Providers to consolidate multiple controllers and reduce operational costs with a single point of control and management for up to 64,000 clients distributed over 4096 VLANs and 6000 APs.

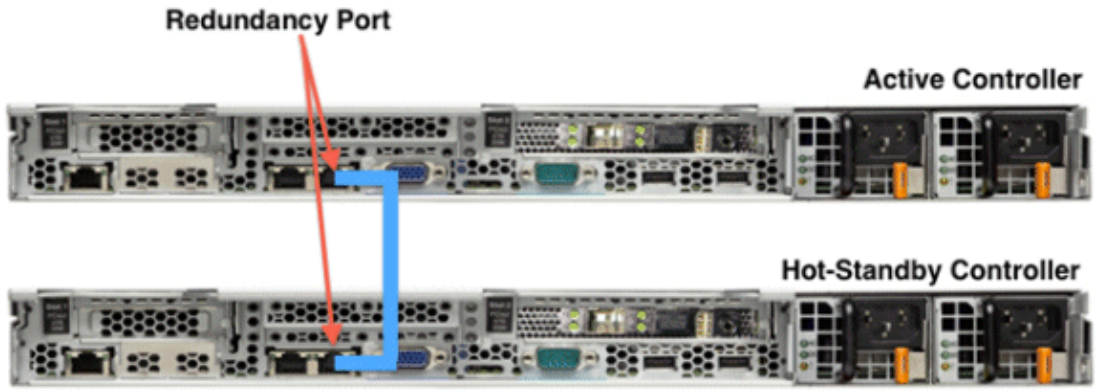
Local Mode Support

The Cisco 8500 Controller platform supports Local mode, Bridge mode, and FlexConnect mode APs. The 8500 Controller supports all AP models supported by a Cisco 5500 Series Controller running software release 7.3.

High Availability AP Stateful Switchover

In the traditional Controller AP Fail−Over model, a unique IP address for the Primary, Secondary, and Tertiary Controller was configured on each AP. When the AP s active Controller went down, the AP went to the discovery state, and a whole joining process to a new Controller was required.

The newly introduced High Availability AP Stateful Switchover (AP SSO) model provides a Box−to−Box redundancy with one Controller in Active state and a second Controller in Hot Standby State where it monitors the health of the Active Controller via a Redundant (HA) Port.



The configuration on the Active Controller is synched to the Standby Controller via the Redundant Port. In HA, both controllers share the same set of configuration including the IP Address of the management interface. Furthermore, the AP's CAPWAP State (for APs in RUN state) are also synched. As a result, APs do not go into Discovery state when the Active Controller fails. This model reduces the Downtime in the case of a Box Failure to sub−second, and to up to three seconds in the case of upstream network connectivity issues (for example, Loss of Gateway).

Note: The HA/AP SSO feature is also supported on the 5500, 7500, and WiSM−2 platforms running the 7.3 release code.

A dedicated Standby Controller SKU (AIR−CT8510−HA−K9) is available and supports standby operation for up to 6000 APs when connected to the primary 8500 Controller as described here.

For more information on the HA feature, refer to the High Availability (AP SSO) Deployment Guide.

New Licensing Model

Release 7.3 also introduces a new Right to Use (RTU) licensing model to the Cisco Flex 7500 and Cisco 8500 Series Controllers. This is an Honor−based licensing scheme that allows AP licenses to be enabled on supported controllers with End User License Agreement (EULA) acceptance The RTU license scheme simplifies addition, deletion, or the transfer of AP adder licenses in the field by eliminating the need for an additional step, additional tools, or access to Cisco.com for PAK license or return materials authorization (RMA) transfers.

Evaluation licenses are valid for 90 days. Notifications will be generated in order to inform you to buy a permanent license starting 15 days prior to the evaluation license expiration.

In the event that you have more APs connected than those purchased, the licensing status for the controller tracked within the Cisco Prime Infrastructure 1.2 will turn red.

For more information on the RTU License model, refer to the document Cisco Right to Use Licensing (RTU).

License Types

These are the three license types:

- **Permanent Licenses** − The AP count is programmed into NVM by manufacturing; this is also referred to as Base AP count Licenses. This type of license is not transferable.
- **Adder access point Count Licenses** − May be activated by you through the acceptance of the EULA. Adder licenses are transferable.
- **Evaluation Licenses** − Used for demo and/or trial periods, are valid for 90 days, and default to the full capacity of the controller. The Evaluation License may be activated at any time using a CLI command.

License CLI Commands:

```
(8500) >show license ?

all             Displays All The License(s).
capacity        Displays License currently used by AP
detail          Displays Details Of A Given License.
evaluation      Displays Evaluation License(s).
expiring        Displays Expiring License(s).
feature         Displays License Enabled Features.
in-use          Displays License That Are In-Use.
permanent       Displays Permanent License(s).
statistics      Displays License Statistics.
status          Displays License Status.
summary         Displays Brief Summary Of All License(s).
```

Seamless IP Mobility For Packet Core Integration with the WLC as a PMIPv6 MAG

Proxy Mobile IPv6 (PMIPv6) is an IETF standard network−based mobility management protocol for building common and access−technology−independent mobile core networks (specified in RFC 5213). It accommodates various access technologies such as WiFi, WiMAX, 3GPP, and 3GPP2−based access architectures. PMIPv6 enables the same functionality as Mobile IP without any modifications to the host's TCP/IP Protocol stack. With PMIPv6, the host can change its point−of−attachment to the Internet without changing its IP address. This functionality is implemented by the network, which is responsible for tracking the movements of the host and initiating the required mobility signaling on its behalf.

The PMIPv6 architecture defines these functional entities:

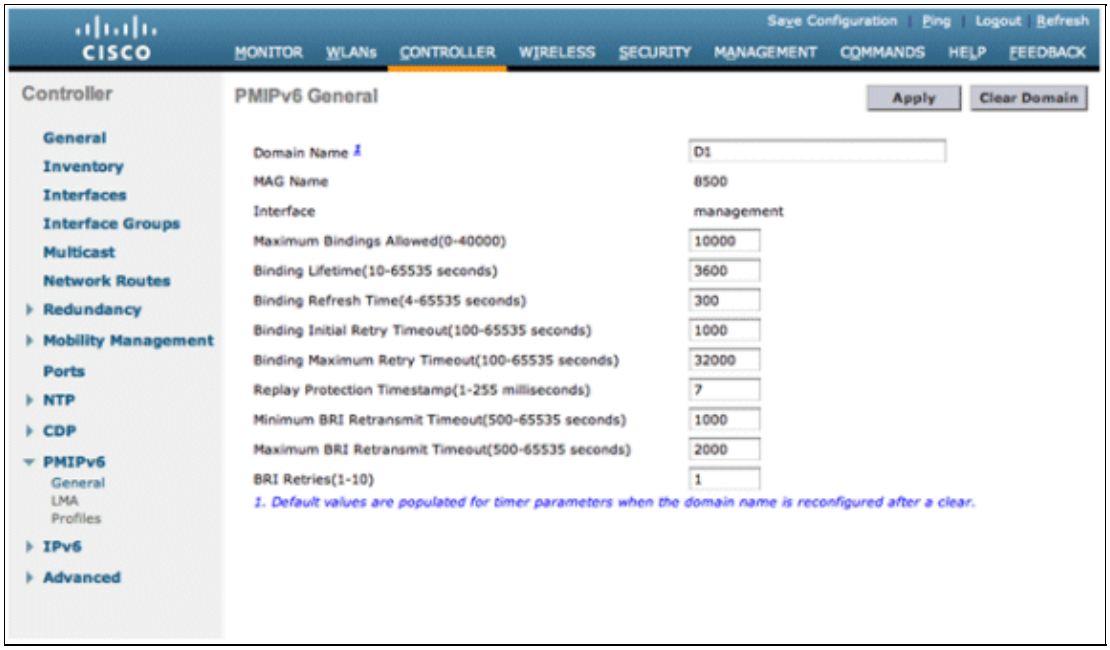
- Local Mobility Anchor (LMA)
- Mobile Access Gateway (MAG)
- Mobile Node (MN)
- Cellular Networks (CN)

The LMA is the central core element of the PMIPv6 architecture. It is the point for assigning and advertising the MN IP addresses. The LMA establishes a bi−directional tunnel to the controller, (running release 7.3 or later) and functions as a PMIPv6 MAG. The MAG (that is, controller) interfaces with the LMA, and performs the mobility management on behalf of the wireless client (MN).

Other device on the network (defined as CN) will be able to reach the wireless client (MN) via its home address through the LMA, which is advertising the reachability for the MN prefix to the CN.

For more information on the PMIPv6 Seamless IP Mobility feature, refer to Cisco Wireless Proxy Mobile IPv6 Configuration Guide.

Here you can see the general PMIPv6 settings screen on an 8500 Controller:



Note: The PMIPv6 MAG functionality is currently only available for the Cisco 8500, 5500, and WiSM−2 Controller platforms.

Note: Release 7.3 supports communication with up to 10 LMAs, and 40,000 PMIPv6 clients.

WiFi Passpoint 1.0 (or HotSpot 2.0)

There are three technology pillars to Passpoint (HotSpot2.0): IEEE 802.11u, WPA2−Enterprise, and EAP−based authentication.

Wi−Fi certified Passpoint (HS2.0) assures simple and secure connection to public Wi−Fi hotspots for offloading cellular data, ensuring lower overall TCO.

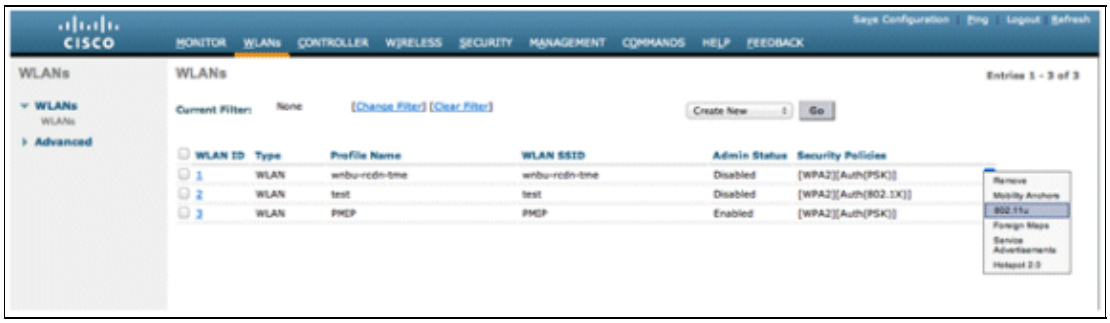
HS2.0 support is available on these AP modes of operation:

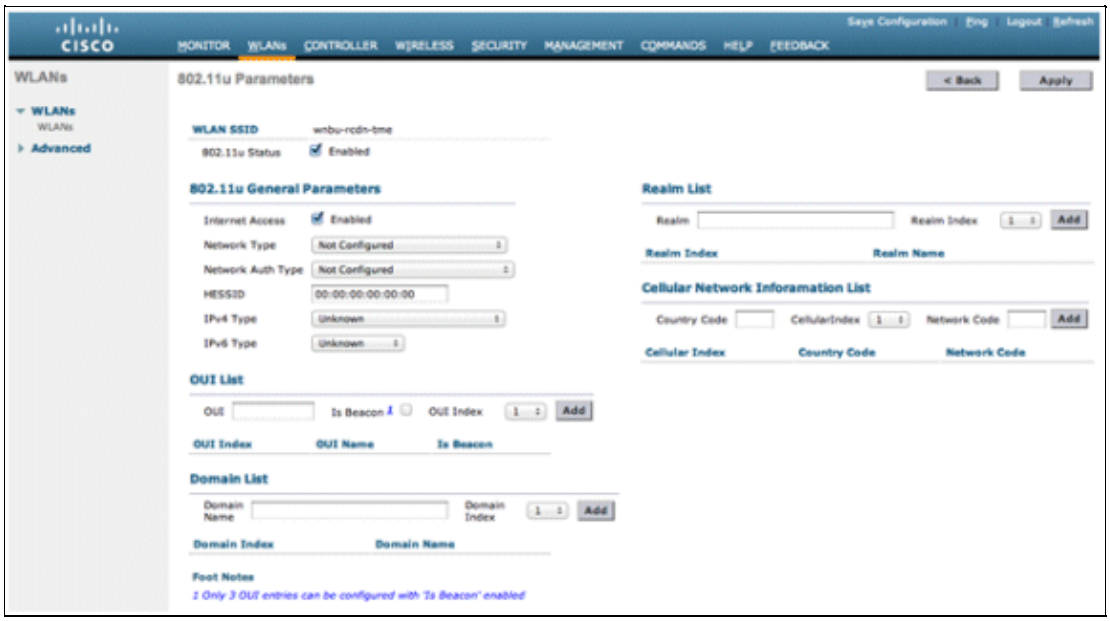
- Local mode AP
- Bridge mode AP (Root AP only)
- FlexConnect; both Central Switch and Local Switching mode

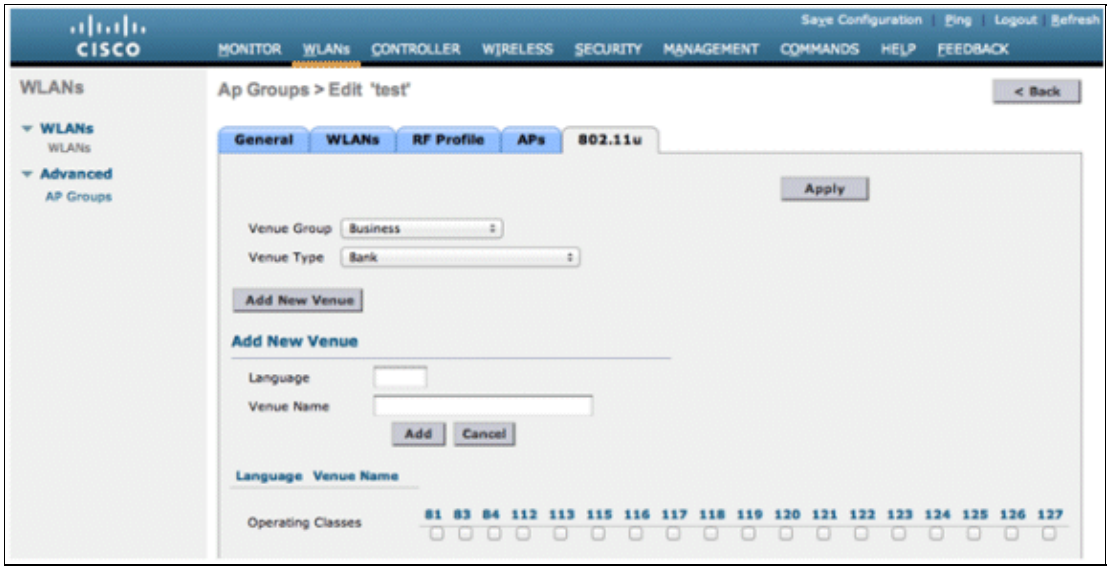
Note: The Passpoint features are available in software release 7.3 for all controller platforms and CAPWAP APs which are capable of running the 7.2 release (except the Office Extend AP600).

For more information on configuring these features, refer to the Cisco Wireless LAN Controller Configuration Guide, Release 7.3.

These images display various 802.11u configuration options:







4k VLAN Support at the Controller

In order to Address Service Provider s scalability requirements, the 7.3 software release extends the number of supported VLANs to 4096.

This enables location−based service per Interface/VLAN as the number of maximum interfaces has also been increased from 512 to 4096 (4095 + management interface) and associated VLANs.

Note: The 4k VLAN is supported only on the 8500 and Flex7500 Controllers.

Dual−redundant DC Power

In order to accommodate Service Provider DC power requirements, the 8500 can be ordered in a Dual−redundant −48V DC power supply configuration.

Input voltage range: Minimum: −40VDC and Maximum: −75VDC

Note: The DC powered 8510 controller does not ship with any of the country specific power cords. For the DC powered units, you should use your own 12G wire and connect to the DC power supply.

Other Important Service Provider Oriented Features

These other important Service Provider oriented features were introduced in the Cisco WLCs with the 7.3 code:

- Central DHCP for FlexConnect local switching
- VLAN Tagging on CAPWAP management (no CAPWAP restriction to native VLAN)
- RADIUS Accounting Enhancements
- MAC Authentication Failover to 802.1x Authentication
- FlexConnect with 802.11u/hotspot for Mobile Network offload
- Standards based 802.11r fast roaming
- Bi−Directional Rate Limiting (per−user throughput limits with higher granularity)
- VideoStream for rich media flows (in Local Mode)
- FlexConnect VLAN Based Central Switching
- FlexConnect Split Tunneling
- FlexConnect WGB/UWGB Support
- PPPoE client at an AP
- NAT/PAT support at an AP

Some of the new Service Provider related features integrated into the 7.4 code:

- LAG support (Sub−second link failover)
- Added 6 more options for the sent Called−Station−ID RADIUS attribute:
    - ♦ ap−group−name
    - ♦ ap−location
    - ♦ ap−name
    - ♦ ap−name−ssid
    - ♦ flex−group−name
    - ♦ vlan−id
- Added six (6) more choices for the Option−82 sent to a DHCP server:
    - ♦ ap−group−name
    - ♦ ap−location
    - ♦ apname−vlan−id
    - ♦ ap−ethmac−ssid
    - ♦ flex−group−name
    - ♦ apmac−vlan−id
- Configurable Primary and Secondary RADIUS servers at the FlexConnect Group level; with a limit of up to 2x the number of FlexGroups supported on the platform (i.e. up to 4000 RADIUS servers on an 8500 controller)
- Several Controller management enhancements (Faster HA upgrade process, SFTP file transfers, Service port HA enhancement, Granular TACACS+ control)
- Upstream QOS (bi−dir client rate limiting)
- AP client Load Balance using AP Ethernet utilization
- DHCP proxy mode per VLAN interface
- WLC ordered with HA−SKU, can be used as a secondary in an "N+1" failover scenario (supporting the full platform capacity)
- AP radio can be set to accept only 802.11n clients ("Not" to be confused with "Green Field")

Design Considerations

Multicast

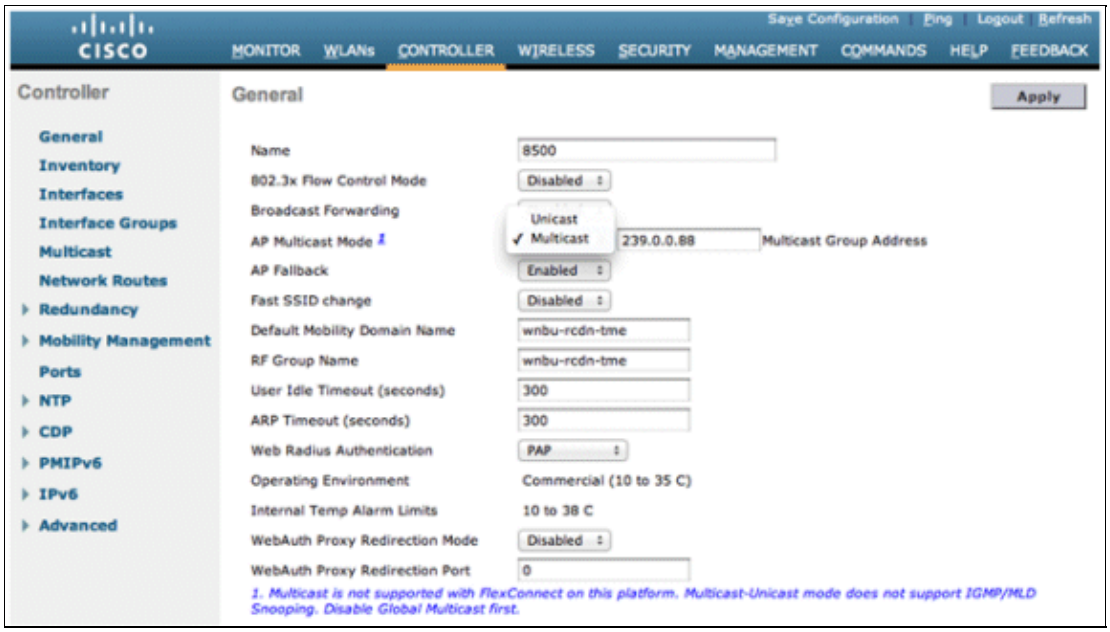
Multicast support is enabled in the Cisco 8500 Controller, and its operation is comparable to that of the Cisco 5500 Series Controllers, but with these restrictions:

1. If all APs on the 8500 Controller are configured in Local mode, Multicast−Multicast will be the default mode and all features are supported (for example, VideoStream). This scenario is identical to a 5500 Controller.
2. If the APs are configured as a mix of Local mode and FlexConnect mode:

    - ♦ If IPv6 is required on the FlexConnect APs:

        a. Disable Global Multicast Mode and change to Multicast−Unicast mode.
        b. IPv6/GARP will work on FlexConnect and Local mode APs, but Multicast data and the VideoStream feature will be disabled.
    - ♦ IPv6/GARP is not required on FlexConnect APs:

        a. Change the mode to Multicast−Multicast and Enable Global Multicast Mode and IGMP/MLD snooping.
        b. IPv6, GARP, Multicast Data, and VideoStream are supported on local mode APs.



Note: Multicast−Unicast is required for IPv6 operation on FlexConnect APs (for RA and NS packet delivery).

Inter−Platform Mobility

In most networks, support for heterogeneous Wireless Controllers in a mobility group is usually required. These can be instances of upgrade, migration, or backup with such a heterogeneous configuration. In these cases, the number of supported Fast Secure Roaming (FSR) clients should be considered in the network design. For example, consider a large wireless network composed of a mix of the following WLC platforms, all configured in the same mobility group:

- 8500 (supports FSR for 64,000 clients)
- 7500 (supports FSR for 64,000 clients)
- WiSM2 (supports FSR for 30,000 clients)
- 5500 (supports FSR for 14,000 clients)

In this scenario:

1. 64,000 authenticated clients can seamlessly roam back and forth between the 7500s and the 8500s.
2. 30,000 authenticated clients can seamlessly roam back and forth between multiple WiSM2 controllers, or between a WiSM2 to 8500 or 7500 controllers.
3. 14,000 authenticated clients can seamlessly roam back and forth between multiple 5500 controllers, or between a 5500 to a WiSM2, 8500, or 7500 controllers.

Wireless clients exceeding those limits will require a rejoin after session timeout.

Local EAP Authentication

The Local EAP authentication database does not scale to the supported 64,000 Clients on the 8500 Controller. Although the feature to have the 8500 act as an Authentication Sever has not been disabled in the user interface, its purpose is solely to support test setup, and **not** for production deployment.

Link Aggregation (LAG)

LAG across the 2x10G interfaces is supported in software versions 7.4 and later. The LAG configuration allows for an active−active link operation with fast failover link redundancy.

Note: The additional active 10G link does not change the total controller network throughput.

Related Information

- **Service Provider Wi−Fi Solution Overview**
- **Cisco Prime Infrastructure 1.2**
- **CUWN Software Release 7.3**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jun 26, 2015 Document ID: 113695