

Deploy the 2500 Series Wireless Controller

Contents

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Hardware Specifications](#)

[Additional Features](#)

[Hardware Architecture of the Cisco 2500 Series Wireless Controller](#)

[Basic Configuration of the Cisco 2500 Series Wireless Controller](#)

[Controller Configuration through the CLI](#)

[Configure the Neighbor Switch](#)

[Configure the Cisco 2500 Series Wireless Controller](#)

[Configure the Controller With the Startup Wizard](#)

[License Installation](#)

[Enable DTLS in the Cisco 2500 Series Controller](#)

[Configure the PI and Add the Cisco 2500 Series Wireless Controller](#)

[Cisco 2500 Series Wireless Controller Deployment Scenarios](#)

[Scenario 1](#)

[Internal DHCP Server with DHCP Proxy Enabled](#)

[External DHCP Server with DHCP Proxy Disabled](#)

[External DHCP Server with DHCP Proxy Enabled](#)

[Scenario 2](#)

[Internal DHCP Server with DHCP Proxy Enabled](#)

[External DHCP Server with DHCP Proxy Disabled](#)

[External DHCP Server with DHCP Proxy Enabled](#)

[Scenario 3](#)

[Scenario 4 LAG](#)

[Guidelines to Deploy the Cisco 2500 Wireless Controller](#)

[Web Express Setup](#)

[High Availability](#)

Introduction

This document describes the deployment requirements for the Cisco 2500 Series Wireless Controller.

Background Information

The Cisco 2500 Series Wireless Controller is a cost-effective, systems-wide wireless solution for retail, enterprise branches, and small and medium-sized businesses. The controller can scale in a network as the network grows.

The Cisco 2500 Series Wireless Controller blends into the Cisco Unified Wireless Network (CUWN) and works with both Cisco lightweight access points (LAPs) and the Cisco Wireless Control System (WCS) or Cisco Network Control System (NCS) or Prime Infrastructure (PI) to provide system-wide wireless LAN functions. The Cisco 2500 Series Wireless Controller provides real-time communication between wireless APs and other devices to deliver centralized security policies, guest access, wireless intrusion prevention system (wIPS), context-aware (location), Radio Frequency (RF) management, and quality of services (QoS) for mobility services, such as voice and video, and Office Extend Access Point (OEAP) support for the teleworker solution.

The Cisco 2500 Series Wireless Controller supports a maximum of 50 lightweight APs in increments of 5 AP licenses with a minimum of a 5 AP license, which makes it a cost-effective solution for retail and small and medium-sized businesses. The Cisco 2500 Series Wireless Controller offers robust coverage with 802.11 a/b/g or delivers unprecedented reliability with the use of 802.11n, 802.11ac, and Cisco Next-Generation Wireless Solutions and Cisco Enterprise Wireless Mesh.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco 2500 Series Wireless Controller.

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, ensure that you understand the potential impact of any command.

Hardware Specifications

- Data Ports - 4 x 1 Gigabit Ethernet Ports
- Console Port - 1 x RJ-45
- External 48 VDC Power Supply

Additional Features

- Support for Control and Provisioning of Wireless Access Points (CAPWAP) protocol.
- Encryption on CAPWAP Data Tunnel (DTLS) (optional).
- License-based AP count. AP Counts - 50 (in steps of 5, 25, 50). This was increased to 75 as of Release 7.4 software code.
- Supported Client Count - 500 (In all STATE). This was increased to 1000 as of Release 7.4 software code.
- Supported Tag Count - 500.
- Triple-Play Ready - Supports Data, Voice, and Video.

- 500 Mbps of overall traffic throughput (no matter how many ports are connected). This was increased to 1 Gbps as of Release 7.4 software code.
- Link Aggregation Group (LAG) is available only as of Release 7.4 software code and later.
- In Release 7.4 software code and later, the 2504 can act as a mobility anchor for up to 15 mobility tunnels towards other controllers.
- In Release 7.4, the 2504 started to support directly connected APs in local mode only. Directly connected APs were not supported before that release.
- The 2504 supports new mobility (that is, mobility with converged access controllers such as the 3850/5760) in Release 8.0 and later.
- Bonjour gateway/multicast Domain Name System (mDNS) is not supported anymore on this controller in version 8.0.132 and further 8.0 maintenance release and 8.1.x and later

 **Note:** The 2504 Wireless Access Controller supports neither the wired guest feature before Version 8.0, nor the multicast-unicast feature (only multicast-multicast). It also does not support the Lync SDN and Flexconnect AVC features that were introduced in Version 8.1

 **Note:** For an accurate list of supported features, check the release notes for your specific software release, which contain a Features not supported on WLC 2504 paragraph.



01_2504 WLC Chassis View

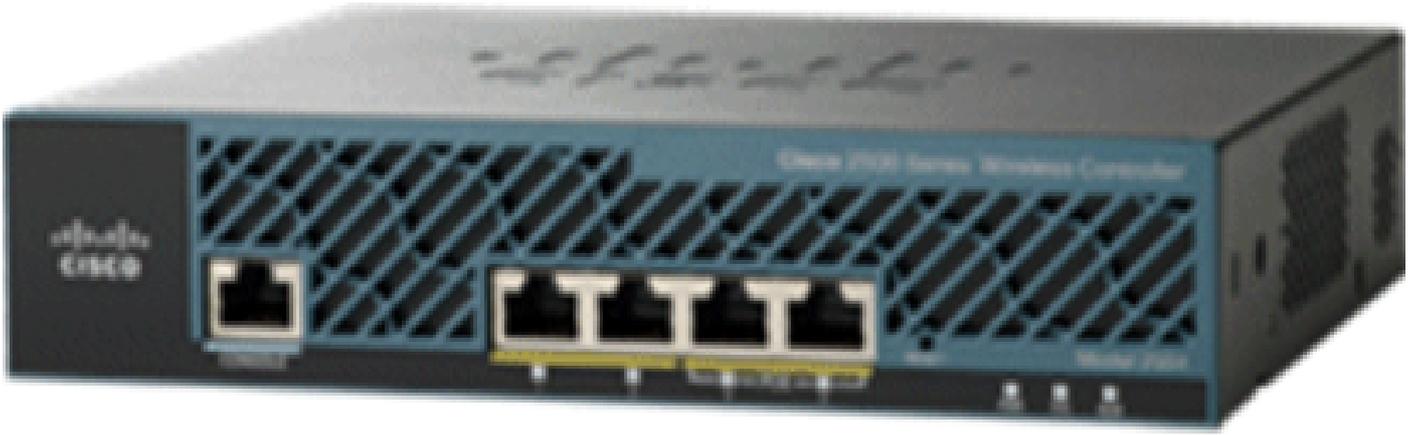
Hardware Architecture of the Cisco 2500 Series Wireless Controller

These sections provide a greater insight into the architecture of the Cisco 2500 Series Wireless Controller.

The Cisco 2500 Series Wireless Controller physically has the same form factor as the Cisco 2106 controller. The CPU on a Cisco 2500 Series Wireless Controller is a multi-core CPU and can handle both data plane and wireless data traffic. The CPU can handle control plane application, which handles all the management traffic needed to control a wireless network.

The Cisco 2500 Series Wireless Controller has 1 GB of system memory. Two types of memory devices are supported to store software images. The boot flash contains the boot code, and the compact flash contains the application code that can store multiple images. The front panel houses four Gigabit Ethernet ports. Two of the ports are 802.3af capable. All ports transfer the traffic to and from the wireless network.

The Cisco 2500 Series Wireless Controller is powered by an external 48 VDC power brick. The power brick can handle power input from 110 VAC to 240 VAC.



02_2500 WLC Chassis View

Basic Configuration of the Cisco 2500 Series Wireless Controller

These tools and information are needed before you can install the controller:

- Wireless Controller hardware:
 - Controller with factory-supplied power cord and hardware required to mount it
 - Network, OS service network, and AP cables as required for the CLI console
 - VT-100 terminal emulator on the CLI console (PC, laptop, or palmtop)
 - Null modem serial cable to connect the CLI console and controller
- Local TFTP server (required in order to download the OS software updates). Cisco uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as the Cisco WCS because Cisco WCS and third-party TFTP servers use the same communication port.

If the controller is brought up for the first time with no prior configuration, it automatically enters into a wizard that asks you a series of configuration information questions. The wizard first prompts for user ID and password. This wizard cannot be bypassed and you must enter all the information requested.

⚠ Caution: Do not connect a Power over Ethernet (PoE) cable to the console port. This action damages the controller.

Controller Configuration through the CLI

Before you can configure the controller for basic operations, connect it to a PC that uses a VT-100 terminal emulator (such as HyperTerminal, ProComm, Minicom, or Tip). Complete these steps to connect the PC to the controller console port:

1. Plug the RJ-45 connector on a null-modem serial cable into the controller console port and the other end of the cable into the PC serial port.
2. Start the PC terminal emulation program.
3. Configure the terminal emulation program for these parameters:

- 9600 baud
- 8 data bits
- No flow control
- 1 stop bit
- No parity

The Cisco 2500 Series Wireless Controller has 4 Gigabit Ethernet ports. Each port is, by default, an 802.1Q VLAN trunk port. The VLAN trunk characteristics of the port are not configurable.

An interface is a logical entity on the controller. An interface has multiple parameters associated with it; which include the IP address, default-gateway (for the IP subnet), primary physical port, secondary physical port, VLAN tag, and DHCP server. Since LAG is not used, each interface is mapped to at least one primary physical port and an optional secondary port. Multiple interfaces can be mapped to a single Wireless Controller port.

There are multiple types of interfaces on the Wireless Controller, four of which are static types that must be present and are configured at setup time:

- Management interface (static and configured at setup time; mandatory)
- AP-manager interface - Not required for the Cisco 2500 Series Wireless Controller
- Virtual interface (static and configured at setup time; mandatory)
- Dynamic interface (user-defined)

The management interface is the default interface for in-band management of the controller and connectivity to enterprise services, such as Authentication, Authorization, and Accounting (AAA) servers. The management interface is also used for communications between the controller and APs. The management interface is the only consistently pingable in-band interface IP address on the controller. The management interface acts like an AP manager interface by default.

The dynamic interface with the **Dynamic AP Management** option enabled on it is used as the tunnel source for packets from the controller to the AP, and as the destination for CAPWAP packets from the AP to the controller. The dynamic interfaces for AP manager must have a unique IP address. Typically, this is configured on the same subnet as the management interface, but this is not necessarily a requirement. In the case of the Cisco 2500 Series Wireless Controller, a single dynamic AP manager can support any number of APs. However, as a best practice, it is suggested to have 4 separate dynamic AP manager interfaces and associate them to the 4 Gigabit interfaces. By default, the management interface acts like an AP manager interface, as well and it is associated to one Gigabit interface. As a result, if you use the management interface, you need to create only 3 more dynamic AP manager interfaces and associate them to the 3 Gigabit interfaces that remains.

 **Note:** If you use AP manager interfaces, the CAPWAP DISCOVERY packet that is sent initially by the APs to discover the WLC is still sent toward the management interface IP address. The management interface replies with a CAPWAP DISCOVERY RESPONSE to give the list of AP manager interfaces of the WLC. This means that the APs always need UDP 5246 and 5247 reachability to the controller management interface and that the DHCP option 43 must mention only the management interface IP address, not the AP manager IP addresses.

The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security, such as guest web authentication and VPN termination. The virtual interface must be configured with an unassigned and unused gateway IP address. A typical virtual interface is 192.0.2.1. The virtual interface address is not pingable and must not exist in any routing table in your network.

Dynamic interfaces are created by users and are designed to be analogous to VLANs for wireless LAN client device. The Cisco 2500 Series Wireless Controller supports up to 16 dynamic interfaces. Dynamic interfaces must be configured on a unique IP network and VLAN. Each dynamic interface acts as a DHCP relay for wireless clients associated to wireless LANs (WLANs) mapped to the interface. A WLAN associates a Service Set Identifier (SSID) to an interface and is configured with security, QoS, radio policies, and other wireless network parameters. There can be up to 16 WLANs configured per controller. Management servers, such as a RADIUS server and NTP server, must not be in a dynamic interface subnet, but must be either in the management interface subnet or any other subnet not added to the WLC.

 **Note:** LAG is supported on the Cisco 2500 Series Wireless Controller only on Release 7.4 software code and later.

Configure the Neighbor Switch

By default, all four ports on the Cisco 2500 Series Wireless Controller are 802.1Q trunk ports. The controller is always connected to a Gigabit Ethernet port on the neighboring switch. The neighbor switch port is configured as an 802.1Q trunk and only the appropriate VLANs are allowed on the trunk. All other VLANs are pruned. This is not necessary, but is a deployment best practice because when irrelevant VLANs are pruned, the controller only processes relevant frames which optimizes performance.

This is the 802.1Q switchport configuration:

```
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan X
switchport trunk allowed vlan X
switchport mode trunk
end
```

Configure the Cisco 2500 Series Wireless Controller

Configure the Controller With the Startup Wizard

This wizard output is taken from Release 7.4 software, so it can be slightly different in other software releases.

```
<#root>
```

```
(Cisco Controller)
(Cisco Controller)
```

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
```

Would you like to terminate autoinstall? [yes]:
AUTO-INSTALL: starting now...
rc = 0
AUTO-INSTALL:no interfaces registered.
AUTO-INSTALL: process terminated - no configuration loaded

System Name [Cisco_b2:19:c4] (31 characters max):

WLC

Enter Administrative User Name (24 characters max):

admin

Enter Administrative Password (3 to 24 characters):

Re-enter Administrative Password :

Enable Link Aggregation (LAG) [yes][NO]:

no

Management Interface IP Address:

10.48.39.212

Management Interface Netmask:

255.255.255.0

Management Interface Default Router:

10.48.39.5

Management Interface VLAN Identifier (0 = untagged):

0

Management Interface Port Num [1 to 4]:

1

Management Interface DHCP Server IP Address:

10.48.39.5

Virtual Gateway IP Address:

192.0.2.1

Multicast IP Address:

239.1.1.1

Mobility/RF Group Name:

Nico

Network Name (SSID):

none

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]:

BE

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]:

yes

Enter the NTP server's IP address:

10.48.39.33

Enter a polling interval between 3600 and 604800 secs:

3600

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

yes

Configuration saved!
Resetting system with new configuration...

Configuration saved!
Resetting system

 **Note:** The previous configuration is an example. It can vary from one installation to another.

(Cisco Controller) >show sysinfo

```
Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 7.4.121.0
Bootloader Version..... 1.0.20
Field Recovery Image Version..... 7.6.101.1
Firmware Version..... PIC 16.0

Build Type..... DATA + WPS

System Name..... WLC
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.9.1.1279
IP Address..... 10.48.39.212
Last Reset..... Software reset
System Up Time..... 0 days 0 hrs 14 mins 58 secs
System Timezone Location.....
System Stats Realtime Interval..... 5
System Stats Normal Interval..... 180

--More-- or (q)uit
Configured Country..... BE - Belgium
Operating Environment..... Commercial (0 to 40 C)
Internal Temp Alarm Limits..... 0 to 65 C
Internal Temperature..... +31 C
External Temperature..... +35 C
Fan Status..... 4300 rpm
```

```

State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
Number of WLANs..... 1
Number of Active Clients..... 0

Memory Current Usage..... Unknown
Memory Average Usage..... Unknown
CPU Current Usage..... Unknown
CPU Average Usage..... Unknown

Burned-in MAC Address..... 84:78:AC:B2:19:C0
Maximum number of APs supported..... 75

```

License Installation

The Cisco 2500 Series Wireless Controller does not have any licenses installed. Without any installed licenses, the APs cannot join the controller. It is recommended to install appropriate licenses on the Cisco 2500 Series Wireless Controller to work with the controller as you go forward. The Cisco 2500 Series Wireless Controller is shipped with an evaluation license for a period of 60 days (that is, 8 weeks 4 days). The evaluation license is a base license only.

The ordered license can be installed on the controller with either the CLI or the GUI. The license installed can be checked through both the CLI and the GUI. In both cases, there must be a TFTP server that hosts the license files.

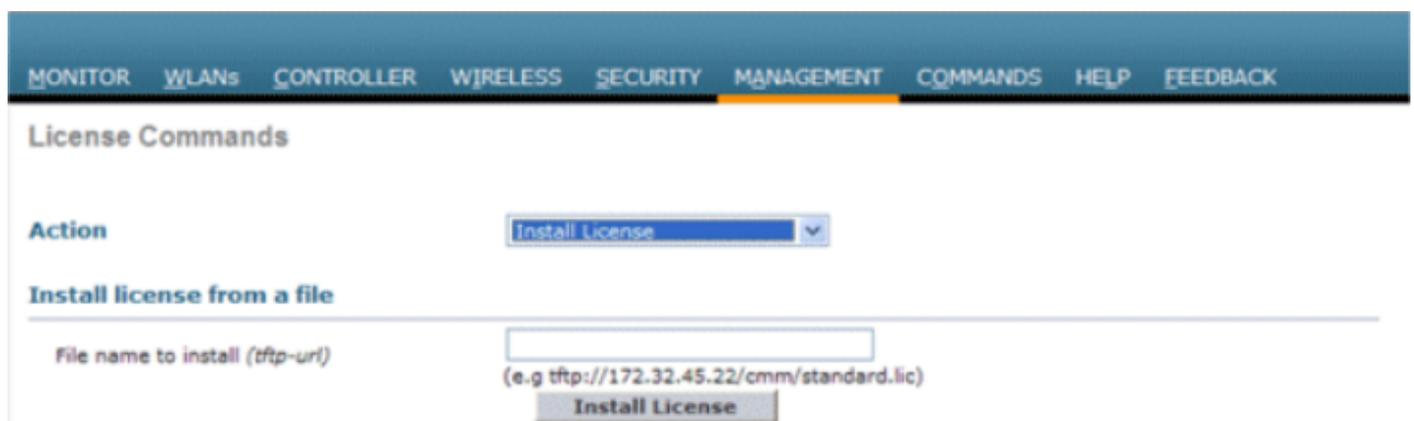
```

<#root>

(Cisco Controller) >
license install ?

<url>          tftp://<server ip>/<path>/<filename>
(Cisco Controller)

```



03_2500 WLC License Installation

The **show license all** command displays the installed licenses.

 **Note:** This license includes a data DTLS functionality.

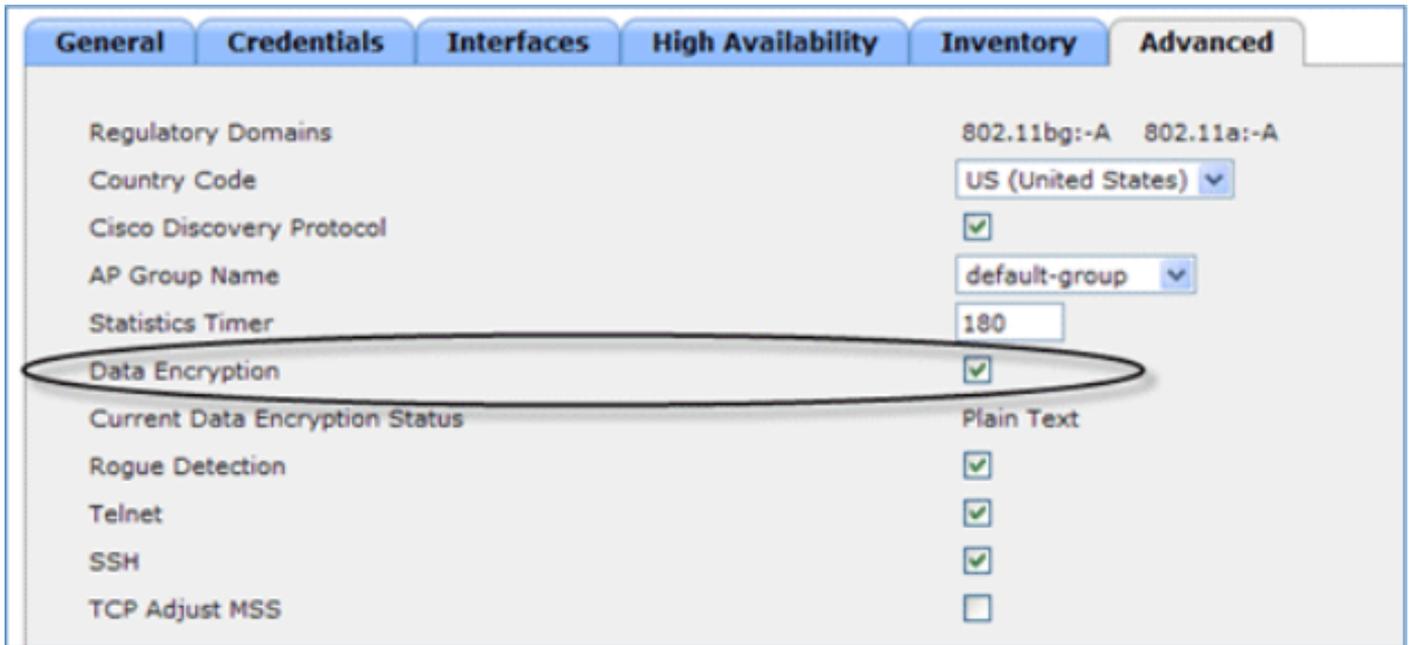
(Cisco Controller) >show license all

```
License Store: Primary License Storage
StoreIndex: 2 Feature: base-ap-count Version: 1.0
  License Type: Permanent
  License State: Active, In Use
  License Count: 50/50/0
  License Priority: Medium
StoreIndex: 3 Feature: data encryption Version: 1.0
  License Type: Permanent
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Medium
License Store: Evaluation License Storage
StoreIndex: 0 Feature: base Version: 1.0
  License Type: Evaluation
  License State: Active, Not in Use, EULA accepted
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 8 weeks 4 days
  License Count: Non-Counted
  License Priority: Low
StoreIndex: 1 Feature: base-ap-count Version: 1.0
  License Type: Evaluation
  License State: Inactive
    Evaluation total period: 8 weeks 4 days
    Evaluation period left: 8 weeks 4 days
  License Count: 50/0/0
  License Priority: None
(Cisco Controller) >
```

Enable DTLS in the Cisco 2500 Series Controller

To enable DTLS on an AP or particularly on a group of APs, make sure a Data Encryption License is installed in the controller. Data Encryption (DTLS) can be enabled on a per AP basis from the **Advanced** tab once the the AP details are selected.

Select an AP, go to the **Advanced** tab, and check the **Data Encryption** check box.



04_2500 Enable Data Encryption

```
(Cisco Controller) >config ap link-encryption enable ?
<Cisco AP> Enter the name of the Cisco AP. all Apply the configuration for
all capable Cisco AP
(Cisco Controller) >config ap link-encryption enable J-3502E
(Cisco Controller) >show ap link-encryption all
```

AP Name	Encryption State	Dnstream Count	Upstream Count	Last Update
J-3502E	En	102	747	22:12
J-1262	Dis	0	0	22:12
J-1040	Dis	0	0	22:13
J-1140	Dis	0	0	22:10

```
(Cisco Controller) >show dtls connections
```

AP Name	Local Port	Peer IP	Peer Port	Ciphersuite
J-3502E	Capwap_Ctrl	10.10.10.116	41066	TLS_RSA_WITH_AES_128_CBC_SHA
J-3502E	Capwap_Data	10.10.10.116	41066	TLS_RSA_WITH_AES_128_CBC_SHA
J-1262	Capwap_Ctrl	10.10.10.120	45543	TLS_RSA_WITH_AES_128_CBC_SHA
J-1040	Capwap_Ctrl	10.10.10.122	65274	TLS_RSA_WITH_AES_128_CBC_SHA
J-1140	Capwap_Ctrl	10.10.10.123	4825	TLS_RSA_WITH_AES_128_CBC_SHA

```
(Cisco Controller) >
```

Configure the PI and Add the Cisco 2500 Series Wireless Controller

PI is the current management software used to manage the Cisco 2500 Series Wireless Controller. Earlier versions were called WCS or NCS. It provides advanced management tools, such as wireless coverage display and location-based services. There is a close relation between the software version of the management system, Prime Infrastructure (PI)/NCS/WCS, and the WLC software version. See the wireless

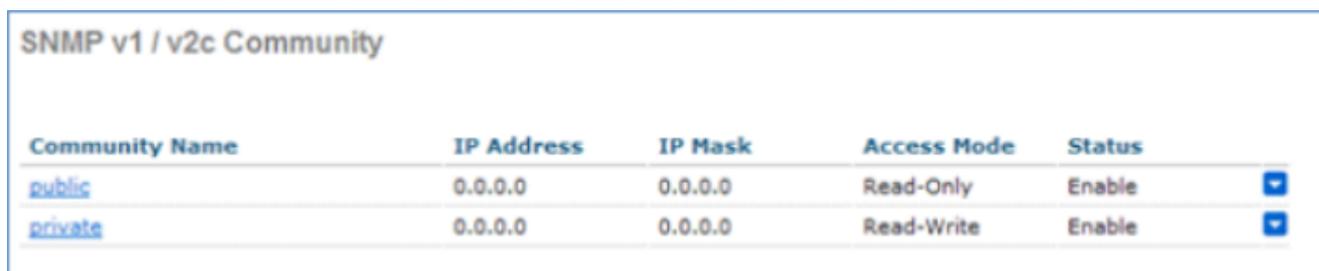
software compatibility matrix, as well as the PI and WLC release notes for supported compatible releases. PI uses SNMP to manage wireless controllers, access points, and client devices. The Cisco 2500 Series Wireless Controller devices need to have SNMP configured correctly.

Complete these steps:

1. Log in to the PI web interface with the URL:

`https://<prime-ip-address>`

2. SNMPv2 is configured on the Cisco 2500 Series Wireless Controller. To configure SNMPv2 through the Controller web interface, navigate to **Management > SNMP > Communities**. The Cisco 2500 Series Wireless Controller defaults are Read-Only community public and Read-Write community private. Add new communities or modify as necessary. For simplicity, the defaults are used.



Community Name	IP Address	IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read-Only	Enable
private	0.0.0.0	0.0.0.0	Read-Write	Enable

05_2500 WLC SNMP Communities

3. In the PI interface, navigate to **Operate > Device work center**. Select **Add device** from the menu bar. This can vary, dependent upon if the classic theme is used from PI or if NCS or WCS is used.

Enter the IP address of the Cisco 2500 Series Wireless Controller management interface and configure the appropriate SNMP parameters. Click **OK**.

Add Device
✕

* Indicates required fields

▼ General Parameters *

IP Address

DNS Name

▼ SNMP Parameters

Version

* Retries

* Timeout (secs)

* Community ?

* Confirm Community

▼ Telnet/SSH Parameters

Protocol

* Timeout (secs)

Username

Password

Confirm Password

06_2500 WLC Management Access Parameters

The controller is added successfully and the Cisco 2500 Series Wireless Controller is ready to be provisioned by PI.

To verify the Cisco 2500 Series Wireless Controller after it is added in PI, check in the device work center to verify it is successfully synced and managed. Wrong SNMP credentials can leave it unmanaged.

Cisco 2500 Series Wireless Controller Deployment Scenarios

The Cisco 2500 Series Wireless Controller provides a cost-effective, unified wireless solution. Although the controller has multiple 10/100/1000 ports, it does not behave like switches or routers. It is not recommended to use different ports as a hub/switch implementation. This fundamental point is a key aspect to get the best performance out of the controller.

The Cisco 2500 Series Wireless Controller supports multiple uplink ports. In Release 7.4 and later, use LAG

to build an etherchannel and treat several ports as just one connection. Or, disable LAG and configure a system where management and dynamic interfaces can be configured on different physical ports, and data traffic can switch back and forth intra network from respective physical ports.

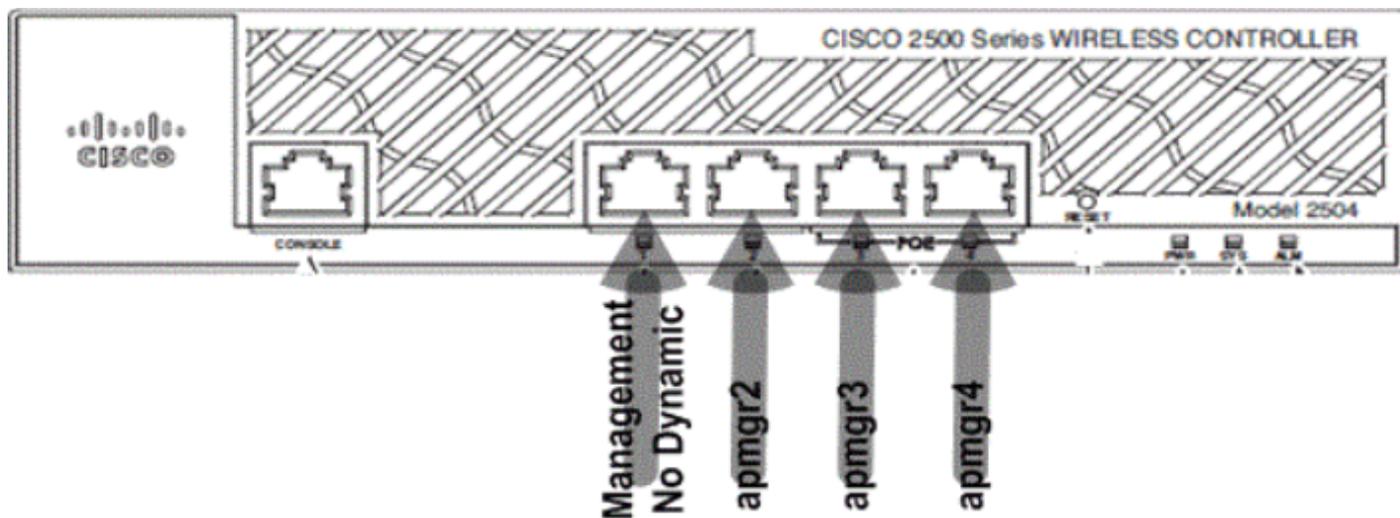
The Cisco 2500 Series Wireless Controller also supports multiple AP managers (for AP Load Balancing) where multiple AP managers can be configured in addition to an AP manager that is bounded with a management interface. In this case, it is recommended to have all AP managers in the same subnet as a management interface.

```
<CISCO2504> >show interface summary
```

Interface Name	Port	Vlan Id	IP Address	Type	Ap Mgr	Guest
apmgr2	2	10	10.10.10.12	Dynamic	Yes	No
apmgr3	3	10	10.10.10.13	Dynamic	Yes	No
apmgr4	4	10	10.10.10.14	Dynamic	Yes	No
management	1	10	10.10.10.10	Static	Yes	No
virtual	N/A	N/A	192.0.2.1	Static	No	No

```
<CISCO2504> >
```

Note: Configuration of interfaces on different ports that are in the same VLAN is not supported and breaks connectivity as per Cisco bug ID [CSCux75436](#). It only works in this example when an AP manager is present on each of those ports. If the interface created is not an AP manager and is in the same VLAN as another port, routing issues occur.



07_2500 WLC Front Panel Layout 1

In this output, the management interface and AP manager are bounded together to port 1. Three more AP managers are created on other physical ports (2, 3, and 4) in the same subnet as management interfaces.

APs that join the controller are load balanced, such that each port on the controller shares the load of the 50 APs. Each port in the previous configuration allows 13 APs to join the controller.

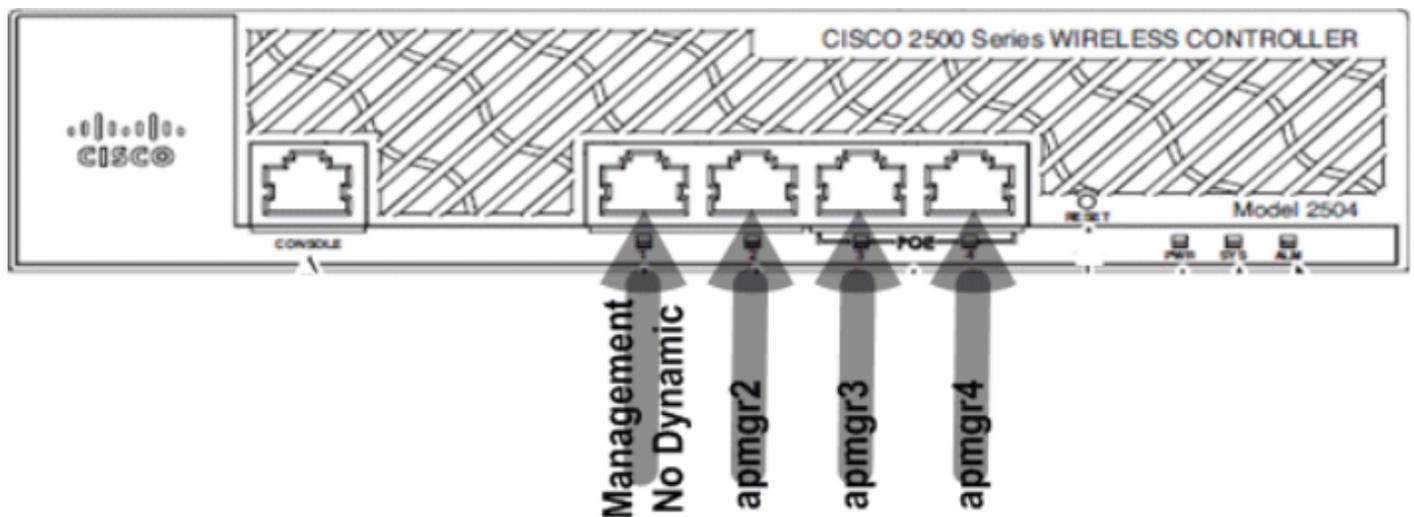
It is also possible to have multiple AP managers in a different subnet than the management interface.

However, in this case, it is recommended to disable the AP manager from the management interface and create another AP manager interface on different physical ports in a different subnet than the management interface. All multiple AP managers in this scenario must be in the same subnet.

```
<CISCO2504> >show interface summary
```

Interface Name	Port	Vlan Id	IP Address	Type	Ap Mgr	Guest
apmgr2	2	11	10.10.11.12	Dynamic	Yes	No
apmgr3	3	11	10.10.11.13	Dynamic	Yes	No
apmgr4	4	11	10.10.11.14	Dynamic	Yes	No
management	1	10	10.10.10.10	Static	No	No
virtual	N/A	N/A	192.0.2.1	Static	No	No

```
<CISCO2504> >
```



08_2500 WLC Front Ports Layout 2

In the previous output, management and the AP manager are not bounded. In this scenario, multiple AP managers can be created in a different subnet from the management interface and mapped to different physical ports.

 **Note:** The internal DHCP server only works (for wireless clients) with DHCP proxy enabled.

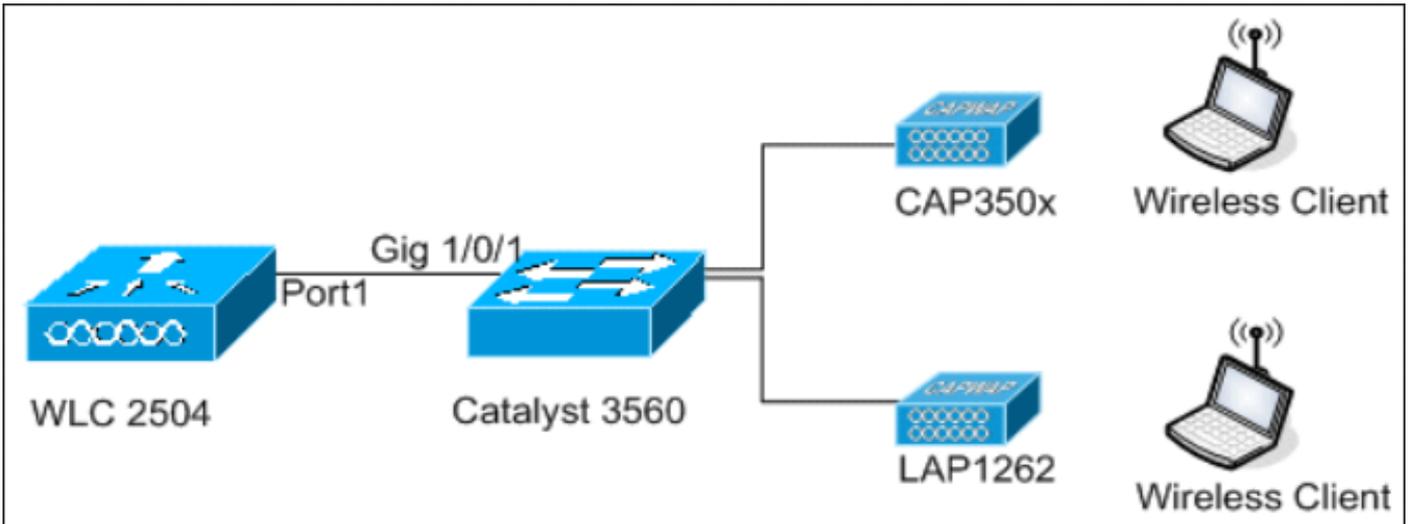
Some of the scenarios supported by the Cisco 2500 Series Wireless Controller are described here with sample configurations.

Scenario 1

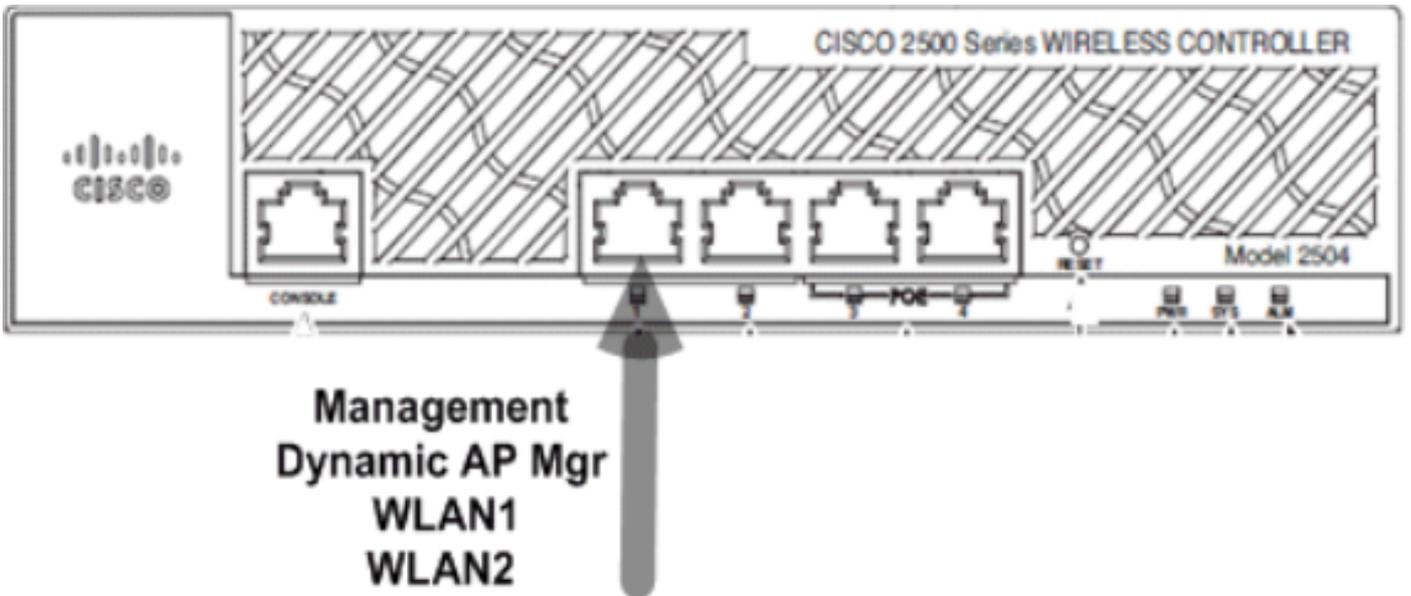
The management interface with an embedded AP manager is configured on Port 1. Two WLANs are configured on the controller. WLAN 1 and WLAN 2 are mapped to the management interface.

A simple topology has the Cisco 2500 Series Wireless Controller connected to a Catalyst 3560 switch.

Gigabit Ethernet port 1 on the controller is connected to Gigabit Ethernet port 1/0/1 on the switch.



09_2500 WLC Topology View 1



10_2500 WLC Single Cable Connected

```
Switch#sh run int gig 1/0/1
Building configuration...
```

```
Current configuration : 123 bytes
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
end
```

```
Switch#
```

The management interface configuration on the Cisco 2500 Series Wireless Controller is straightforward and has dynamic AP management enabled.

Interfaces > Edit

General Information

Interface Name	management
MAC Address	00:22:bd:d9:52:80

Configuration

Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	<input type="text" value="0"/>

NAT Address

Enable NAT Address	<input type="checkbox"/>
--------------------	--------------------------

Interface Address

VLAN Identifier	<input type="text" value="10"/>
IP Address	<input type="text" value="10.10.10.10"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="10.10.10.1"/>

Physical Information

Port Number	<input type="text" value="1"/>
Backup Port	<input type="text" value="0"/>
Active Port	1
Enable Dynamic AP Management	<input checked="" type="checkbox"/>

DHCP Information

Primary DHCP Server	<input type="text" value="10.10.10.10"/>
Secondary DHCP Server	<input type="text" value="0.0.0.0"/>

Two WLANs are configured. WLAN1 and WLAN2 are mapped to the management interface and service clients.

```
<CISCO2504> >show wlan summ
```

```
Number of WLANs..... 2
```

WLAN ID	WLAN Profile Name / SSID	Status	Interface Name
1	WLAN1 / WLAN1	Enabled	management
2	WLAN2 / WLAN2	Enabled	management

```
<CISCO2504> >
```

Internal DHCP Server with DHCP Proxy Enabled

The DHCP server TestVlan10 is configured on the controller and this scope services APs and clients. The DHCP server configuration on the controller is simple.

```
<CISCO2504> >show dhcp summary
```

Scope Name	Enabled	Address Range
TestVlan10	Yes	10.10.10.100 -> 10.10.10.200

```
<CISCO2504> >show dhcp detailed TestVlan10
```

```
Scope: TestVlan10
```

```
Enabled..... Yes
Lease Time..... 36400 <10 hours 6 minutes 40 seconds>
Pool Start..... 10.10.10.100
Pool End..... 10.10.10.200
Network..... 10.10.10.0
Netmask..... 255.255.255.0
Default Routers..... 10.10.10.10 0.0.0.0 0.0.0.0
DNS Domain.....
DNS..... 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers..... 0.0.0.0 0.0.0.0 0.0.0.0
```

```
<CISCO2504> >
```

This is the DHCP configuration capture from the GUI of the Cisco 2500 Series Wireless Controller:

DHCP Scope > Edit

Scope Name	TestVlan10		
Pool Start Address	<input type="text" value="10.10.10.100"/>		
Pool End Address	<input type="text" value="10.10.10.200"/>		
Network	<input type="text" value="10.10.10.0"/>		
Netmask	<input type="text" value="255.255.255.0"/>		
Lease Time (seconds)	<input type="text" value="36400"/>		
Default Routers	<input type="text" value="10.10.10.10"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
DNS Domain Name	<input type="text"/>		
DNS Servers	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Netbios Name Servers	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Status	<input type="button" value="Enabled"/> ▼		

12_2500 WLC DHCP Scope

The DHCP proxy is enabled on all Cisco controllers by default.

DHCP Parameters

Enable DHCP Proxy	<input checked="" type="checkbox"/>
DHCP Option 82 Remote Id field format	<input type="text" value="AP-MAC"/> ▼
DHCP Timeout (5 - 120 seconds)	<input type="text" value="120"/>

13_2500 WLC DHCP Parameters

In the all of the previous configurations, VLAN10 is not tagged on the switch. All traffic from the switch is sourced to Port 1 on the controller. APs and client traffic are forwarded to the controller untagged.

APs are connected to the Catalyst switch with these switchport configurations. The switchport can either be

trunked or configured to be an access port.

```
Switch#sh run int gig 1/0/9
Building configuration...
```

Current configuration : 132 bytes

```
!
interface GigabitEthernet1/0/9
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 10
  switchport mode trunk
end
```

```
Switch#sh run int gig 1/0/10
Building configuration...
```

Current configuration : 66 bytes

```
!
interface GigabitEthernet1/0/10
  switchport access vlan 10
end
```

Switch#

The AP can join the controller and the status of the AP can be verified on the controller. There are two APs that have joined the controller and can be confirmed by the status in this capture:

```
<CISCO2504> >show ap join stats summary all
```

Number of APs..... 2

Base Mac	AP EthernetMac	AP Name	IP Address	Status
00:22:90:96:69:00	00:22:90:90:ab:d3	AP0022.9090.abd3	10.10.10.103	Joined
ec:44:76:b9:7d:c0	c4:7d:4f:3a:e3:78	APc47d.4f3a.e378	10.10.10.105	Joined

```
<CISCO2504> >show ap summary
```

Number of APs..... 2

Global AP User Name..... Not Configured
Global AP Dot1x User Name..... Not Configured

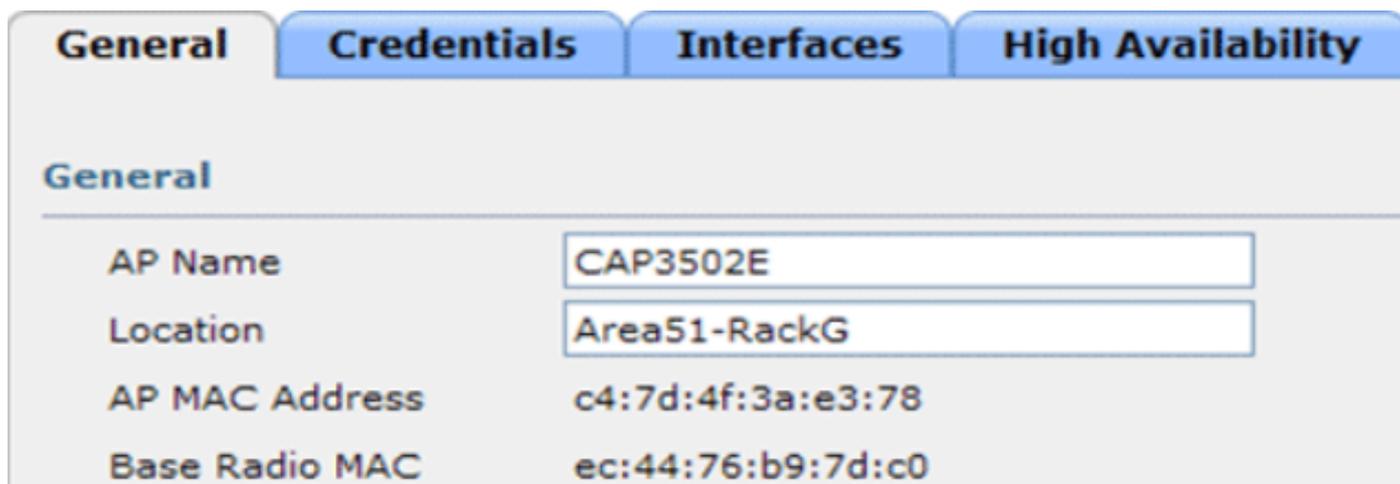
AP Name	Slots	AP Model	Ethernet MAC	Location
AP0022.9090.abd3	2	AIR-LAP1142N-A-K9	00:22:90:90:ab:d3	default location
APc47d.4f3a.e378	2	AIR-CAP3502E-A-K9	c4:7d:4f:3a:e3:78	default location

Port Country Priority

```
-----
1      US      1
1      US      1
```

The APs that have joined the controller can also be verified by the AP summary on the controller. Configure

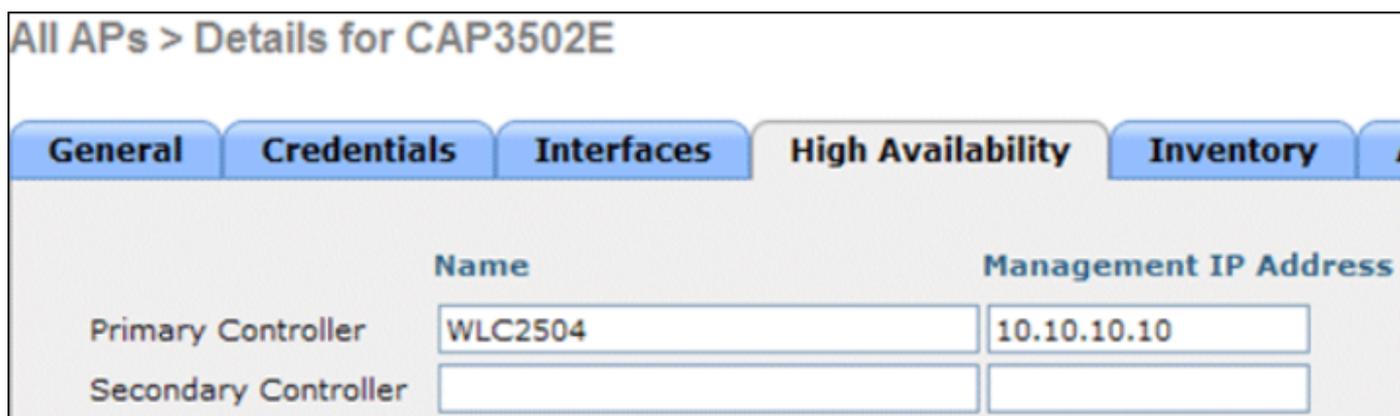
both the AP name and the location of the AP install.



General	
AP Name	CAP3502E
Location	Area51-RackG
AP MAC Address	c4:7d:4f:3a:e3:78
Base Radio MAC	ec:44:76:b9:7d:c0

14_2500 WLC AP General Settings

Configure the controller name and IP address under High Availability to prime the AP.



All APs > Details for CAP3502E		
High Availability		
	Name	Management IP Address
Primary Controller	WLC2504	10.10.10.10
Secondary Controller		

15_2500 WLC AP High Availability Settings

With this configuration, the AP joins the configured controller as the first preference.

External DHCP Server with DHCP Proxy Disabled

This is a general setup that has been in practice for all Cisco controllers for some deployments. The configurations are almost the same as noted previously, but have the DHCP proxy disabled.

DHCP Parameters

Enable DHCP Proxy

DHCP Option 82 Remote Id field format

AP-MAC

DHCP Timeout (5 - 120 seconds)

120

16_2500 WLC Disable DHCP Proxy

The AP manager interfaces in this scenario point to an external DHCP server.

 **Note:** It is recommended to enable either an internal DHCP server or an external DHCP server.

```
ip dhcp excluded-address 10.10.11.1 10.10.11.150
!  
ip dhcp pool VLAN11  
  network 10.10.11.0 255.255.255.0  
  default-router 10.10.11.1  
!
```

External DHCP Server with DHCP Proxy Enabled

This is a general setup that is one of the best practices for all Cisco controllers. The configurations are almost the same as noted in the previous with DHCP proxy enabled.

DHCP Parameters

Enable DHCP Proxy

DHCP Option 82 Remote Id field format

AP-MAC

DHCP Timeout (5 - 120 seconds)

120

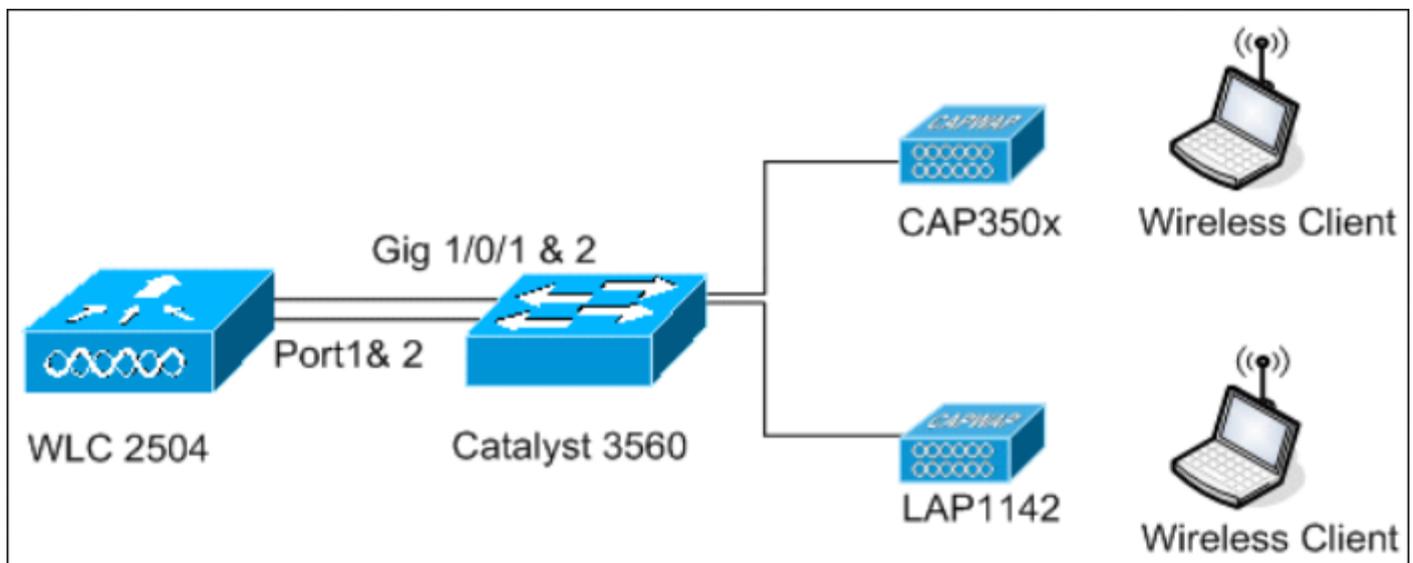
17_2500 WLC Enable DHCP Proxy

The management interface in this scenario is always directed to an external DHCP server.

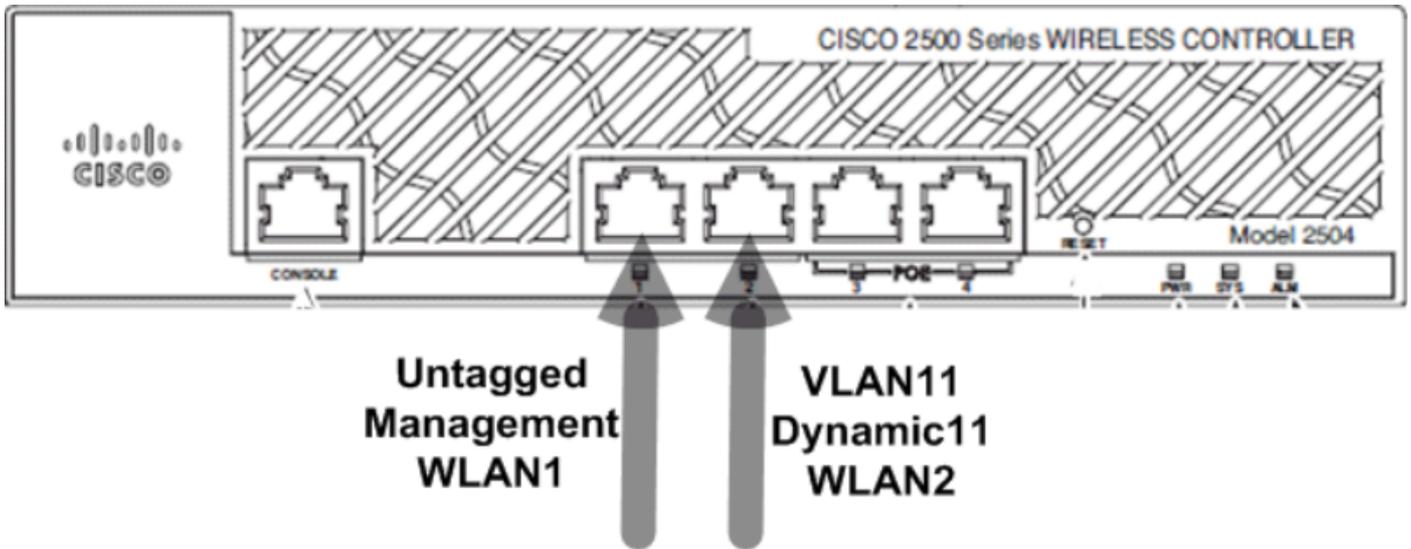
```
ip dhcp excluded-address 10.10.11.1 10.10.11.150
!  
ip dhcp pool VLAN11  
  network 10.10.11.0 255.255.255.0  
  default-router 10.10.11.1  
!
```

Scenario 2

The management interface with AP manager enabled is mapped to port 1. Dynamic interface dynamic11 is mapped to another physical interface (port 2) for data traffic. WLAN 1 is mapped to the management interface and WLAN 2 is mapped to the dynamic interface.



18_2500 WLC Topology View 2



19_Two Cables Connected

One more DHCP scope is configured on the controller. This configured DHCP Scope TestVlan11 is mapped to the dynamic interface configured on the controller.

```
<CISCO2504> >show dhcp summary
```

Scope Name	Enabled	Address Range
TestVlan10	Yes	10.10.10.100 -> 10.10.10.200
TestVlan11	Yes	10.10.11.100 -> 10.10.11.200

```
<CISCO2504> >show dhcp detailed TestVlan11
```

```
Scope: TestVlan10
```

```
Enabled..... Yes
Lease Time..... 36400 <10 hours 6 minutes 40 seconds>
Pool Start..... 10.10.11.100
Pool End..... 10.10.11.200
Network..... 10.10.11.0
Netmask..... 255.255.255.0
Default Routers..... 10.10.11.10 0.0.0.0 0.0.0.0
DNS Domain.....
DNS..... 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers..... 0.0.0.0 0.0.0.0 0.0.0.0
```

```
<CISCO2504> >
```

Internal DHCP Server with DHCP Proxy Enabled

By default, the DHCP proxy is enabled on the controller, as seen in one of the previous captures. Dynamic interface dynamic11 is configured and is mapped to VLAN11. The interface is also mapped to the configured internal DHCP server. The dynamic interface is not enabled for dynamic AP management.

General Information

Interface Name	dynamic11
MAC Address	00:22:bd:d9:52:85

Configuration

Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	<input type="text" value="0"/>

Physical Information

Port Number	<input type="text" value="2"/>
Backup Port	<input type="text" value="0"/>
Active Port	2
Enable Dynamic AP Management	<input type="checkbox"/>

Interface Address

VLAN Identifier	<input type="text" value="11"/>
IP Address	<input type="text" value="10.10.11.10"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="10.10.11.1"/>

DHCP Information

Primary DHCP Server	<input type="text" value="10.10.10.10"/>
---------------------	--

20_2500 WLC Physical and Interface Information

One of the configured WLANs is mapped to the management interface and the second WLAN is mapped to the configured dynamic interface dynamic11. The primary DHCP server is a necessity for configuration in this scenario, but must be pointed to the management interface.

General	Security	QoS	Advanced
Profile Name	WLAN2		
Type	WLAN		
SSID	WLAN2		
Status	<input checked="" type="checkbox"/> Enabled		
Security Policies	None (Modifications done under security tab)		
Radio Policy	All		
Interface/Interface Group(G)	dynamic11		
Multicast Vlan Feature	<input type="checkbox"/> Enabled		
Broadcast SSID	<input checked="" type="checkbox"/> Enabled		

21_2500 WLC General Tab Information

External DHCP Server with DHCP Proxy Disabled

DHCP Parameters

Enable DHCP Proxy

DHCP Option 82 Remote Id field format

DHCP Timeout (5 - 120 seconds)

22_2500 WLC DHCP Parameters Proxy Disabled

Clients successfully get IP addresses from the configured external DHCP server. Therefore, verify the status of the internal DHCP server and make sure the internal DHCP server is disabled.

DHCP Scopes				New...
Scope Name	Address Pool	Lease Time	Status	
TestVlan10	10.10.10.100 - 10.10.10.200	10 h 6 m 40 s	Enabled	▼
TestVlan11	10.10.11.100 - 10.10.11.200	10 h 6 m 40 s	Disabled	▼

23_2500 WLC DHCP Scopes

External DHCP Server with DHCP Proxy Enabled

DHCP Parameters

Enable DHCP Proxy

DHCP Option 82 Remote Id field format AP-MAC ▼

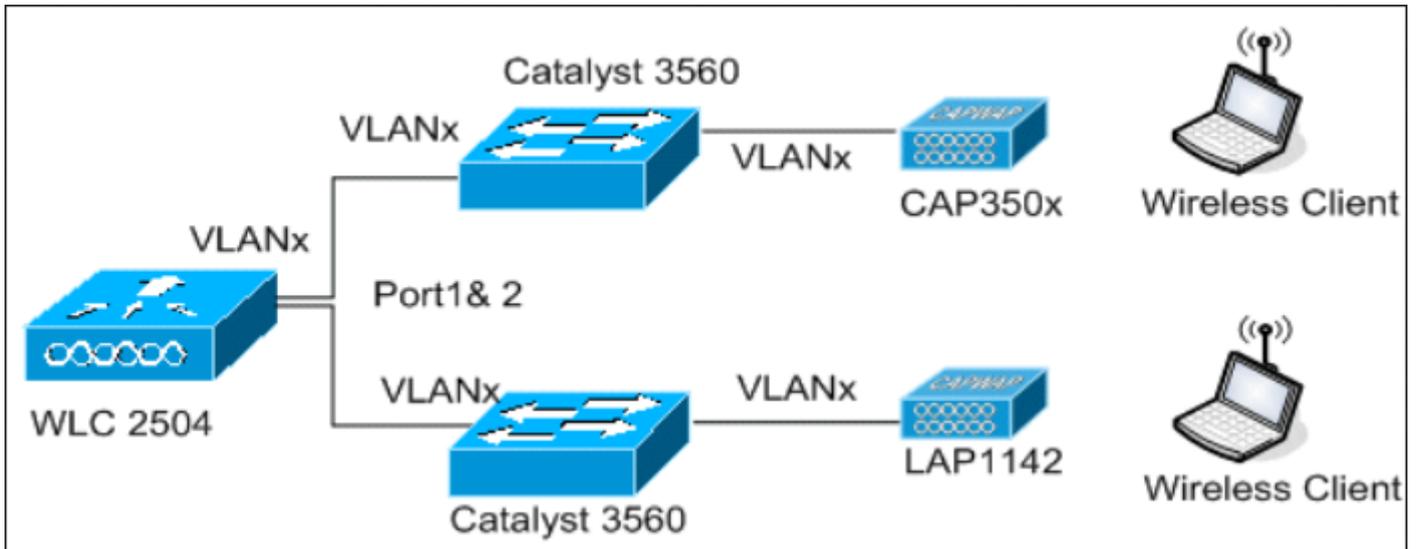
DHCP Timeout (5 - 120 seconds) 120

24_2500 WLC DHCP Parameters Proxy Enabled

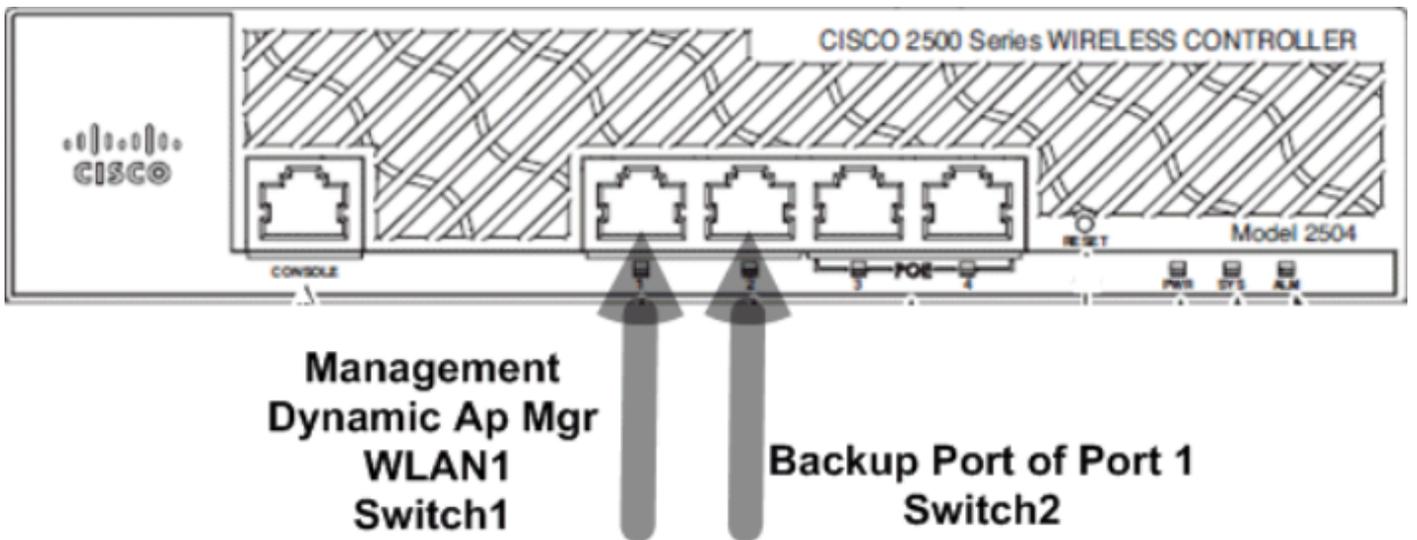
Clients successfully get IP addresses from the configured external DHCP server.

Scenario 3

The management interface with the AP manager enabled is mapped to port 1. Port 2 is configured to be a backport. WLAN 1 is mapped to the management interface.



25_2500 WLC Topology View 2



26_2500 WLC Two Cables Connected

In this scenario the management and dynamic interfaces are configured on Port 1 with either the internal DHCP server or the external DHCP server. Ports 1 and 2 are connected to two different switches. This provides redundancy to the Layer 2 and Layer 3 switch network, as shown in this topology and interface captures.

Interfaces > Edit

General Information

Interface Name	management
MAC Address	00:22:bd:d9:52:80

Configuration

Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	<input type="text" value="0"/>

NAT Address

Enable NAT Address	<input type="checkbox"/>
--------------------	--------------------------

Interface Address

VLAN Identifier	<input type="text" value="0"/>
IP Address	<input type="text" value="10.10.10.10"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="10.10.10.1"/>

Physical Information

Port Number	<input type="text" value="1"/>
Backup Port	<input type="text" value="2"/>
Active Port	1
Enable Dynamic AP Management	<input checked="" type="checkbox"/>

DHCP Information

Primary DHCP Server	<input type="text" value="10.10.10.10"/>
Secondary DHCP Server	<input type="text" value="0.0.0.0"/>

Pr	Type	STP Stat	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	POE
1	Normal	Forw	Enable	Auto	1000 Full	Up	Enable	N/A
2	Normal	Forw	Enable	Auto	1000 Full	Up	Enable	N/A
3	Normal	Disa	Enable	Auto	Auto	Down	Enable	N/A
4	Normal	Disa	Enable	Auto	Auto	Down	Enable	N/A

(Cisco Controller) >show lag summary

LAG Enabled

(Cisco Controller) >show interface summary

Number of Interfaces..... 2

Interface Name	Port	Vlan Id	IP Address	Type	Ap Mgr	Guest
management	LAG	untagged	10.48.39.212	Static	Yes	No
virtual	N/A	N/A	192.0.2.1	Static	No	No

(Cisco Controller) >show interface detailed management

```

Interface Name..... management
MAC Address..... 84:78:ac:b2:19:cf
IP Address..... 10.48.39.212
IP Netmask..... 255.255.255.0
IP Gateway..... 10.48.39.5
External NAT IP State..... Disabled
External NAT IP Address..... 0.0.0.0
VLAN..... untagged
Quarantine-vlan..... 0
Active Physical Port..... LAG (13)
Primary Physical Port..... LAG (13)
Backup Physical Port..... Unconfigured
DHCP Proxy Mode..... Global
Primary DHCP Server..... 10.48.39.5
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
mDNS Profile Name..... Unconfigured
AP Manager..... Yes
Guest Interface..... No
L2 Multicast..... Enabled

```

Now, it is impossible to select ports for interfaces on the WLC because they are all attached to the LAG port bundle (which always shows as number 13).

On the switch, all ports that participate in the bundle must have the exact same configuration (especially trunk native VLAN and allowed VLANs). In this example, allowed VLANs were limited to what is used on the WLC, which is a best practice.

Once the interfaces are bundled together with the command `channel-group X mode on`, a port channel interface of number X is created. Any further change of the configuration must be completed on the port channel interface and not on the individual ports anymore.

```
Nico3560C#show run int g0/8
Building configuration...
```

```
Current configuration : 208 bytes
!
interface GigabitEthernet0/8
 switchport access vlan 33
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,30-39
 switchport mode trunk
 mls qos trust dscp
 channel-group 1 mode on
end
```

```
Nico3560C#show run int g0/10
Building configuration...
```

```
Current configuration : 182 bytes
!
interface GigabitEthernet0/10
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,30-39
 switchport mode trunk
 mls qos trust dscp
 channel-group 1 mode on
end
```

```
Nico3560C#show etherchannel 1 summ
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator

       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
```

```
Number of channel-groups in use: 1
Number of aggregators:          1
```

Group	Port-channel	Protocol	Ports
1	Po1(SU)	-	Gi0/8(P) Gi0/10(P)

```
Nico3560C#
```

```
Nico3560C#show run int po1
Building configuration...
```

```
Current configuration : 131 bytes
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,30-39
 switchport mode trunk
end
```

The command `eterchannel load-balance src-dst-ip` is also required on the switch globally for this to work.

These are just a few designs implemented by clients to leverage the wireless service to their client devices with CUWN.

Guidelines to Deploy the Cisco 2500 Wireless Controller

Ethernet ports on the Cisco 2500 Series Wireless Controllers do not work as switch ports (that is, two machines directly connected to these ports cannot communicate with each other). Do not connect servers, such as DHCP, TFTP, and so on, on these ports and expect Wireless Clients and APs to receive an IP address from this DHCP server.

Ethernet ports on the Cisco 2500 Series Wireless Controller must only be used to connect/uplink to an infrastructure network configured as a data interface (management interface and dynamic interfaces) or an AP managers interface.

If multiple Ethernet ports on a Cisco 2500 Series Wireless Controller are uplinked to an infrastructure switch, make sure data interfaces (management or dynamic interfaces) or AP managers interfaces are configured for these uplinked physical ports. Physical Ethernet ports, which are used as an uplink to an infrastructure switch, must not be left unconfigured. If not, this can result in unexpected behaviors.

Multicast unicast is not a supported configuration on the Cisco 2500 Series Wireless Controller. As a result, Hybrid Remote Edge Access Point (H-REAP)/Flexconnect APs cannot receive multicast traffic because H-REAP/Flexconnect APs only work with multicast unicast.

If APs are directly connected to any of the physical Ethernet ports on the Cisco 2500 controller, then no interfaces must be configured on those physical ports. Physical ports connected to APs must be left unconfigured.

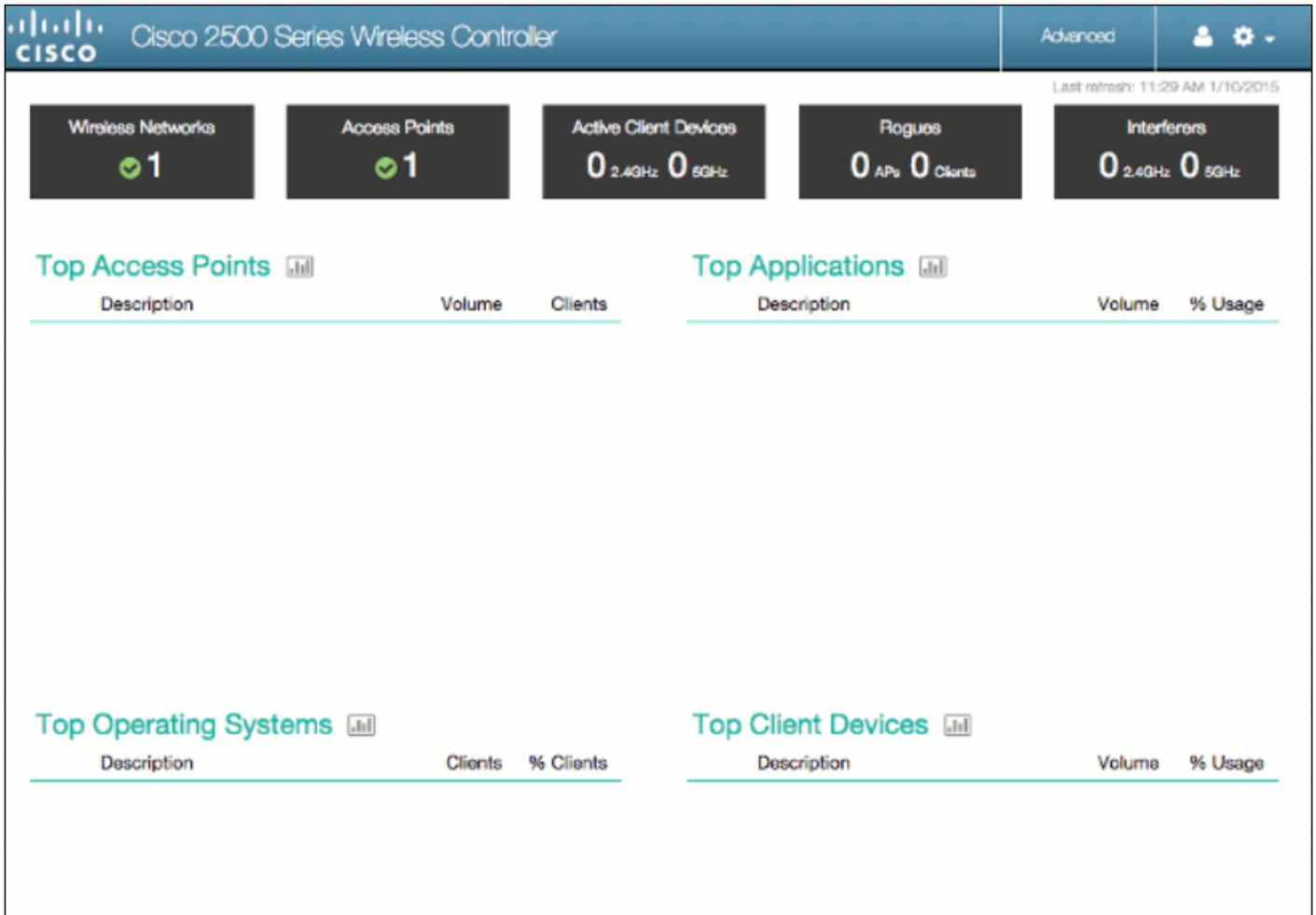
Direct connected APs get an IP address from the AP manager subnet. If there are multiple AP managers, the controller uses the AP manager that is first in the index as the relay interface. AP managers are sorted on the basis of their configured names (numbers and characters) where the lowest one is arranged first in the index.

DHCP proxy must be enabled on controllers for direct connect APs to get an IP address from the internal DHCP server (Controller itself configured as DHCP server). If DHCP proxy is disabled, direct connect APs do not get an IP address from the internal DHCP server. In this case, external DHCP servers must work and direct connect APs can get an IP address.

Web Express Setup

In Version 7.6.130 and later, the WLC offers an Express version of the GUI. It is a way to configure the WLC by the GUI, but is also a simplified monitor dashboard that displays the first time you connect.

On the first GUI connection, you see this:

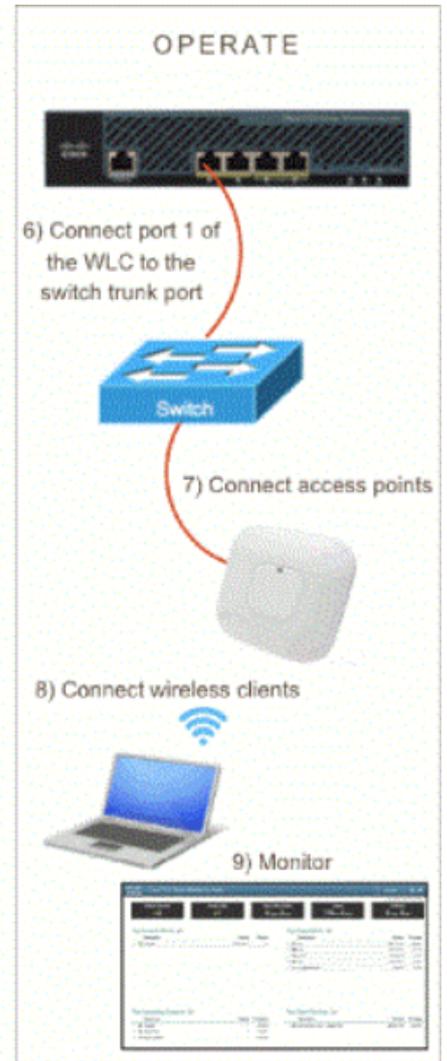
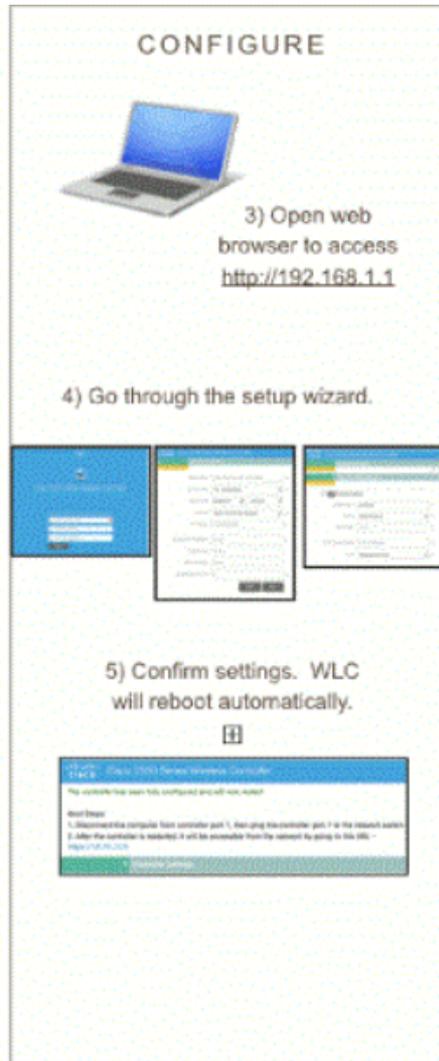
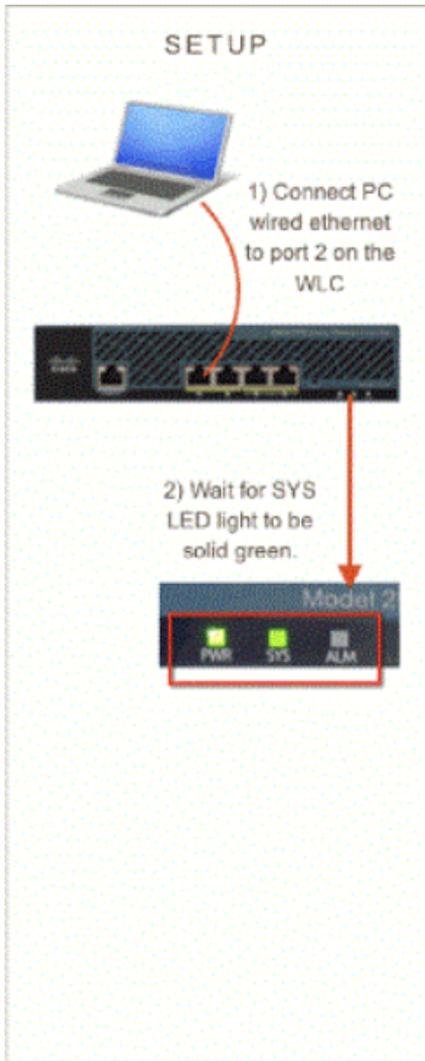


28_2500 WLC First GUI Connection

This page shows all monitoring data in an easy and accessible manner. To reach the old and complete GUI, click **Advanced** in the upper right corner. Once you are in Advanced mode, you cannot go back to the express GUI unless you configured the WLC. As a benefit of the Express Setup GUI, there is a home button on the upper right corner of the WLC page to return to the Express monitoring page.

To configure the 2504 WLC by the Express Setup GUI, connect a PC to port 2, wait for the SYS LED to turn green, and then browse to 192.168.1.1 in the browser. This only works on port 2, which allows connection of port 1 on the WLC for network connectivity.

Configuration of the controller by the Express Setup GUI also changes various default settings to better match small businesses deployments.



29_2500 WLC Express Setup GUI

A special wizard appears for configuration:



Cisco 2500 Series Wireless Controller

Welcome! Please start by creating an admin account.

Start



Cisco 2500 Series Wireless Controller

1 Set Up Your Controller



System Name	<input type="text" value="WLC-30"/>	?
Country	<input type="text" value="United States (US)"/>	?
Date & Time	<input type="text" value="04/23/2014"/>  <input type="text" value="11:35:19"/>	
Timezone	<input type="text" value="Eastern Time (US and Canada)"/>	?
NTP Server	<input type="text" value="0.0.0.0 (optional)"/>	?
Management IP Address	<input type="text" value="172.31.255.30"/>	?
Subnet Mask	<input type="text" value="255.255.255.0"/>	
Default Gateway	<input type="text" value="172.31.255.1"/>	
Management VLAN ID	<input type="text" value="31"/>	?

Back

Next

2 Create Your Wireless Networks



31_2500 WLC Controller Setup

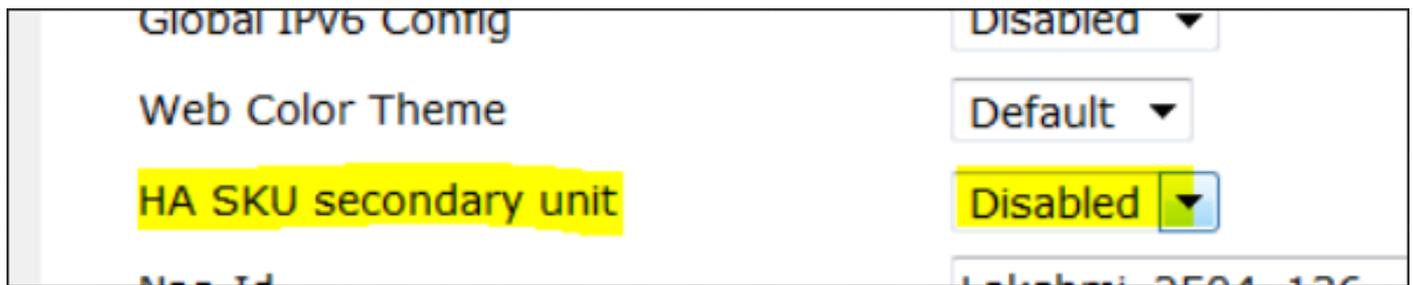
 **Note:** The express GUI setup wizard (Day 0 interface) can be accessed through either a wired connected client or a wireless client. The easy GUI setup wizard on a wired connection only appears when a wired client is plugged in and there are no access points to the controller. If you plug in an access point that starts to broadcast the CiscoAirprovision SSID, the wired GUI wizard is no longer accessible and the easy GUI setup configuration can be completed only through a wireless client connected on the SSID. Therefore, it is either wired or wireless, but the GUI wizard does not work on both simultaneously.

High Availability

In Release 7.5 software code and later, the Cisco 2500 Series Wireless Controllers can be purchased as HA-SKU. This means the 2504 Wireless Controller can then act as N+1 WLC. It still does not support AP SSO.

The HA SKU WLC does not require a license and stands by in case any other WLC of its mobility group fails. It can then support a maximum AP count license for 90 days, which starts when the original WLC failed and when APS started to join the HA-SKU. There is no configuration replication in N+1 redundancy. Check the High Availability deployment guide for more information on HA.

It is also possible to turn a non-HA SKU WLC into an HA SKU when you enable the HA SKU secondary unit :



32_2500 WLC HA SKU Enabled