

# Cisco 4400 Series Wireless LAN Controller (WLC) with Aironet 1100, 1200, 1300 Series APs Configuration and Deployment Guide

SpectraLink's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between NetLink Wireless Telephones and WLAN infrastructure products. The products listed below have been thoroughly tested in SpectraLink labs and have obtained VIEW Certification. This document details how to configure the Cisco 4400 series WLC and Aironet 1100/1200/1300 Series access points (APs) with NetLink Wireless Telephones.

## Certified Product Summary

Manufacturer:	Cisco Systems: <a href="http://www.cisco.com">www.cisco.com</a>	
Approved products:	4400 series WLC with and LWAPP-capable 1130†, 1200, and 1300 series APs	
RF technology:	802.11b/g	
Radio:	2.4 – 2.484 GHz	
Tested security :	WPA-PSK, WPA2-PSK and FSR (Cisco's Fast Secure Roaming method using CCKM)	
AP and WLC software version tested:	4.0.206.0	
NetLink handset models tested:	e340/h340/i640	8000 Series
NetLink handset software tested:	89.134	122.010 or greater
NetLink radio mode:	802.11b	802.11b
Maximum active telephone calls per AP:	10	

† Denotes products directly used in Certification Testing

## Known Limitations

1. WMM must be disabled in order for NetLink Wireless Telephones to work properly.
2. Heavy multicast, broadcast or push-to-talk (PTT) traffic may impair voice quality.
3. The Cisco 1000 series APs are not VIEW certified at this time.
4. Voice and data must be separated onto separate SSIDs to obtain the best voice performance.



This document does not cover the steps involved in converting autonomous APs to LWAPP APs such that they can be controlled by the 4400 WLC. Please contact Cisco's Customer Support at [www.cisco.com](http://www.cisco.com) for instructions on this procedure. Once the APs are converted, this document can be used to provision LWAPP APs.



Subnet roaming was successfully tested, although it is not represented in the network configuration diagram, nor is it covered in the subsequent configuration steps contained in this document. It is important to note that

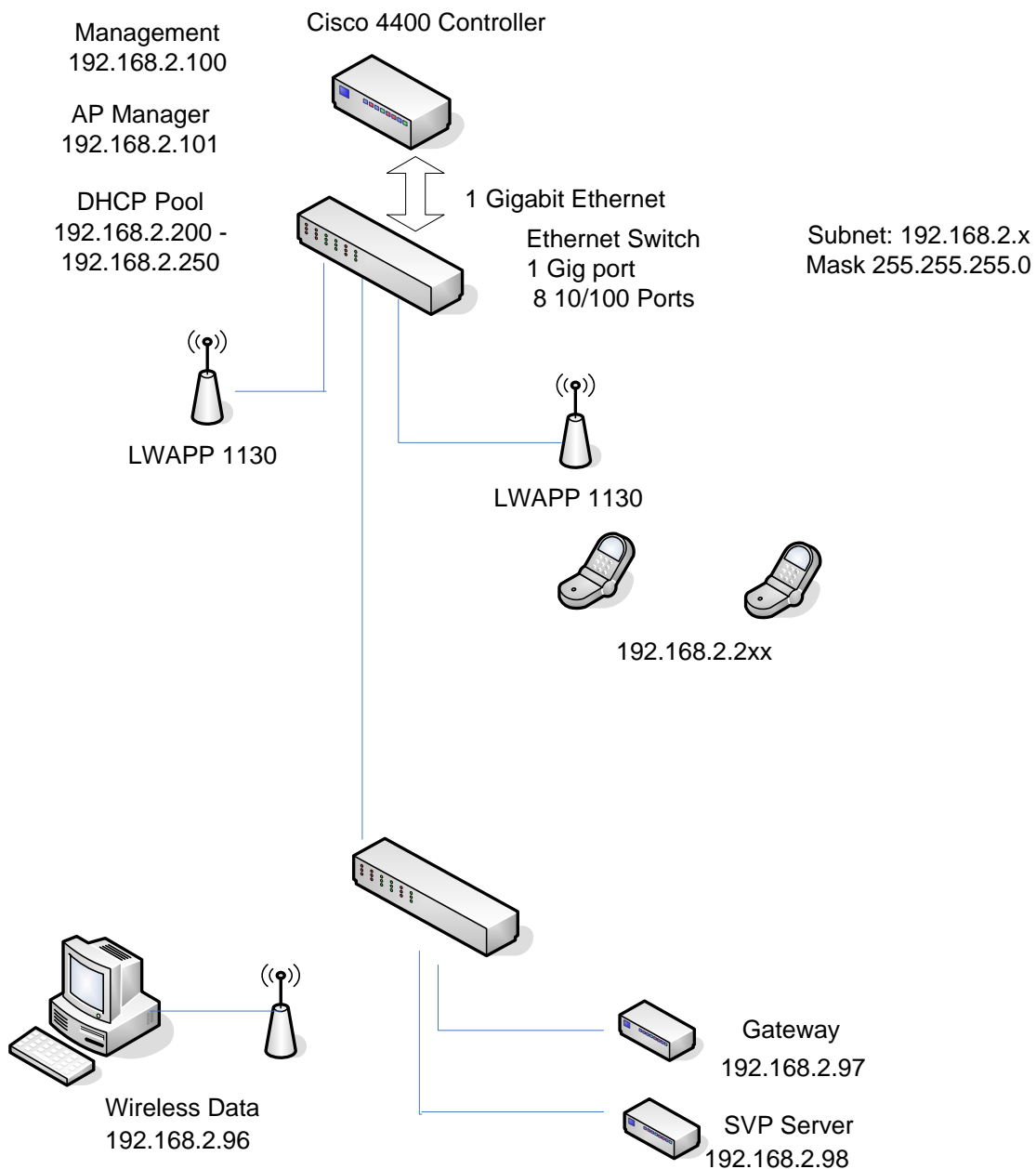
the NetLink Wireless Telephones cannot roam across subnets without the creation of a tunnel between two Cisco WLCs. Please consult the Cisco documentation in order to configure these tunneling mechanisms.

## Network Topology

The following configuration was tested during VIEW Certification.



It is important to note that this configuration is not necessarily applicable to all customer environments.



## Configuring a New Controller Starting From Factory Defaults

1. Initial provisioning of the controller is done via the command line interface (CLI). Connect a null modem serial cable between the console port of the controller and the serial port of a PC.
2. Open a terminal program, such as Hyper Terminal, and configure the port settings to 9600 baud, no parity, 8 data bits and 1 stop bit.
3. Power-on the controller. Status of the controller's boot process will appear as the controller is powering up. Once the controller is running, it will prompt you to run the Startup Wizard.
4. The Startup Wizard provides for an easy means to perform initial controller setup and provisioning. Refer to the *Installation and Startup Guide* for the 4400 series controllers found at Cisco's web site. This document contains a detailed explanation of using the Startup Wizard:  
[http://www.cisco.com/en/US/products/ps6366/products\\_quick\\_start\\_chapter09186a008056add1.html](http://www.cisco.com/en/US/products/ps6366/products_quick_start_chapter09186a008056add1.html)
5. Once the controller has been configured via the Startup Wizard, the remaining configuration can be configured through the switch-web interface using a web-browser (Cisco recommends using MS IE 6.0+).
6. If necessary, the controller can be reset to factory defaults. To reset the WLC to factory default, you must reboot, then type **Recover-config** at the CLI. This only works before the first time a user logs in via the console.

## Connecting to the Controller via a Browser

1. Connect to the WLC by pointing your internet browser to the URL:  
https<IP\_Addr> (where <IP\_Addr> is the IP address of the management interface of the WLC).
2. Click on the **Login** prompt. The default User Name and Password is **admin**.
3. Once logged in properly, a page similar to the one below is presented.

The screenshot displays the Cisco Systems Wireless LAN Controller (WLC) management interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows a tree view with categories like Monitor, Summary, Statistics, Controller, Ports, and Wireless. The main content area is titled 'Summary' and features a '12 Access Points Supported' status bar. Below this, there are three main summary sections: Controller Summary, Access Point Summary, and Client Summary. Each section contains a table of key metrics and their current values. The Controller Summary table lists management IP, service port IP, software version, system name, up time, system time, internal temperature, and network states. The Access Point Summary table shows the status of 802.11a and 802.11b/g radios. The Client Summary table shows the number of current, excluded, and disabled clients. On the right side, there are additional sections for Rogue Summary, Top WLANs, and Most Recent Traps.

**Controller Summary**

Management IP Address	192.168.2.100
Service Port IP Address	0.0.0.0
Software Version	4.0.206.0
System Name	VIEW
Up Time	0 days, 0 hours, 5 minutes
System Time	Tue May 30 11:45:52 2006
Internal Temperature	+41 C
802.11a Network State	Disabled
802.11b/g Network State	Enabled

**Access Point Summary**

	Total	Up	Down	
802.11a Radios	1	0	1	<a href="#">Detail</a>
802.11b/g Radios	1	1	0	<a href="#">Detail</a>
All APs	1	1	0	<a href="#">Detail</a>

**Client Summary**

Current Clients	3	<a href="#">Detail</a>
Excluded Clients	0	<a href="#">Detail</a>
Disabled Clients	0	<a href="#">Detail</a>

**Rogue Summary**

Active Rogue APs	0	<a href="#">Detail</a>
Active Rogue Clients	0	<a href="#">Detail</a>
Adhoc Rogues	0	<a href="#">Detail</a>
Rogues on Wired Network	0	

**Top WLANs**

Profile Name	# of Clients	
Data	1	<a href="#">Detail</a>
Voice	0	<a href="#">Detail</a>

**Most Recent Traps**

- AP's Interface:1(802.11b) Operation State Up: Base Rar
- AP's Interface:0(802.11a) Operation State Down: Base I
- AP Associated. Base Radio MAC: 00:0b:85:58:06:30
- AP Disassociated. Base Radio MAC: 00:0b:85:58:06:30
- AP's Interface:1(802.11b) Operation State Down: Base I

[View All](#)

This page refreshes every 30 seconds.

## Installing Software

1. Make sure that the VIEW Certified version of software is installed on the controller. From the main menu, select **Monitor> Summary**. The heading labeled **Software Version** shows the current software version.
2. Download the appropriate software for your model of controller from the Cisco website.
3. Set up a TFTP server running on a PC to download the file to the controller.
4. Connect to the controller via a Web browser. Select **Commands** from the main menu, and then select **Download File**.
5. For **File Type**, select **Code**. For **TFTP Server**, type in the IP Address of the TFTP Server, Add the **Path** (this is the path in the TFTP server's root directory and not the system path where the TFTP server is located) and **File Name** of the firmware file to download.
6. Allow a few minutes for the download to complete.

Cisco Systems

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | **COMMANDS** | HELP

Save Configuration | Ping | Logout | Refresh

Commands

Download File

Upload File

Reboot

Reset to Factory Default

Set Time

Download file to Controller

File Type: Code

TFTP Server

IP Address: 192.168.2.99

Maximum retries: 10

Timeout (seconds): 6

File Path:

File Name: AIR-WLC4400-K9-4-0-206-0.aes

Clear Download

## Controller Setup

The initial setup of the controller is shown below.



The setup instructions outlined in this document are for the configuration shown in the diagram only. Your configuration may differ, and the appropriate adjustments must be made.



It is not necessary to configure each AP individually. The WLC is capable of provisioning the APs.

1. From the main menu, select **Controller**.
2. Set the **LWAPP Transport Mode** to **Layer 3**. (This setting is for proper communication between the controller and the APs only. It does not enable L3 roaming of Wireless Handsets).
3. Set the **Ethernet Multicast Mode** to **Multicast** and enter a multicast IP address that is currently not being used on your network for the **Multicast Group Address**.
4. Click **Apply** and **Save Configuration**.

Cisco Systems		Save Configuration   Ping   Logout   Refresh	
MONITOR   WLANS   CONTROLLER   WIRELESS   SECURITY   MANAGEMENT   COMMANDS   HELP			
Controller	General	<b>Apply</b>	
General	802.3x Flow Control Mode	Disabled	
Inventory	LWAPP Transport Mode	Layer 3 (Current Operating Mode is Layer3)	
Interfaces	LAG Mode on next reboot	Disabled (LAG Mode is currently disabled).	
Network Routes	Ethernet Multicast Mode	Multicast 224.0.1.100	
Internal DHCP Server	Aggressive Load Balancing	Disabled	
Mobility Management	Peer to Peer Blocking Mode	Disabled	
Mobility Groups	Over The Air Provisioning of AP	Enabled	
Mobility Statistics	AP Fallback	Enabled	
Spanning Tree	Apple Talk Bridging	Disabled	
Ports	Fast SSID change	Disabled	
Master Controller Mode	Default Mobility Domain Name	VIEW	
Network Time Protocol	RF-Network Name	VIEW	
QoS Profiles	User Idle Timeout (seconds)	300	
	ARP Timeout (seconds)	300	
	Web Radius Authentication	PAP	
	Operating Environment	Commercial (0 to 40 C)	
	Internal Temp Alarm Limits	0 to 65 C	

## Connecting APs

As the APs are connected to the network, they should automatically find the controller via the LWAPP Discovery Algorithms. The DHCP server will assign each AP an IP address.



You can configure a DHCP server to run on a remote PC for a small deployment. However, for large-scale deployments, an enterprise-grade DHCP server must be used.

The AP-Manager and Management Interfaces' configuration should include the DHCP server you have configured. Alternately, you can configure the DHCP server internally on the controller to hand out leases to the connected clients (Note: The WLC's DHCP server does not lease addresses to the AP). The instructions for doing so are included at the end of this document.

1. From the main menu, select **Controller>Interfaces**. Verify that the proper IP addresses are assigned to the interfaces.

The screenshot shows the Cisco Systems Controller web interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER (selected), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar lists various configuration options, with 'Interfaces' selected under the 'Controller' section. The main content area displays a table of interfaces:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	192.168.2.101	Static	Enabled
management	untagged	192.168.2.100	Static	Not Supported
service-port	N/A	0.0.0.0	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

Each row has an 'Edit' link next to it. A 'New...' button is located in the top right corner of the table area.

2. Select **Edit** for the **Management** interface. Under **DHCP Information**, enter the IP address of the DHCP server. Repeat this step for the **AP-Manager** interface.

The screenshot shows the Cisco Systems Controller web interface with the configuration page for the 'ap-manager' interface. The top navigation bar is the same as the previous screenshot. The left sidebar shows 'Interfaces' selected. The main content area is titled 'Interfaces > Edit' and includes a '< Back' button and an 'Apply' button. The configuration is organized into several sections:

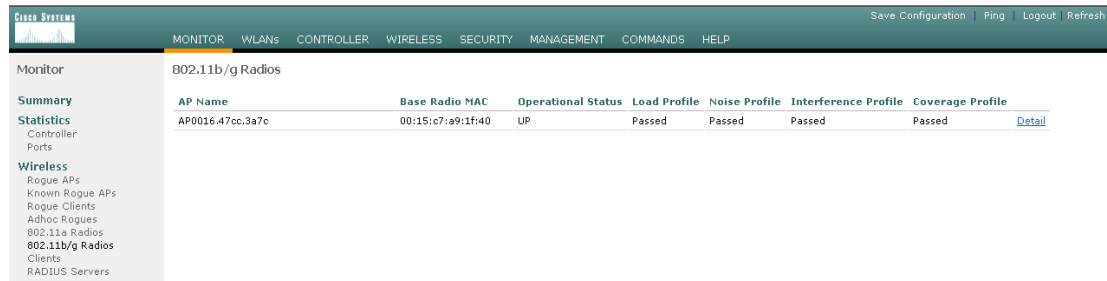
- General Information:** Interface Name is 'ap-manager'.
- Interface Address:**
  - VLAN Identifier: 0
  - IP Address: 192.168.2.101
  - Netmask: 255.255.255.0
  - Gateway: 192.168.2.1
- Physical Information:**
  - Port Number: 1
  - Backup Port: 0
  - Active Port: 1
  - Enable Dynamic AP Management: ☒
- DHCP Information:**
  - Primary DHCP Server: 192.168.2.99
  - Secondary DHCP Server: (empty field)
- Access Control List:**
  - ACL Name: none

A red note at the bottom states: "Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients."

3. Click **Apply** and save the changes.

## AP Configuration

1. Power-on and connect the APs to the network. Wait a few minutes for the APs to find the controller.
2. Verify the APs are associated to the WLC. From the main menu, select **Monitor**-> **802.11b/g Radios**. All the APs that are connected should be listed, showing their **Operational Status** as **UP**.



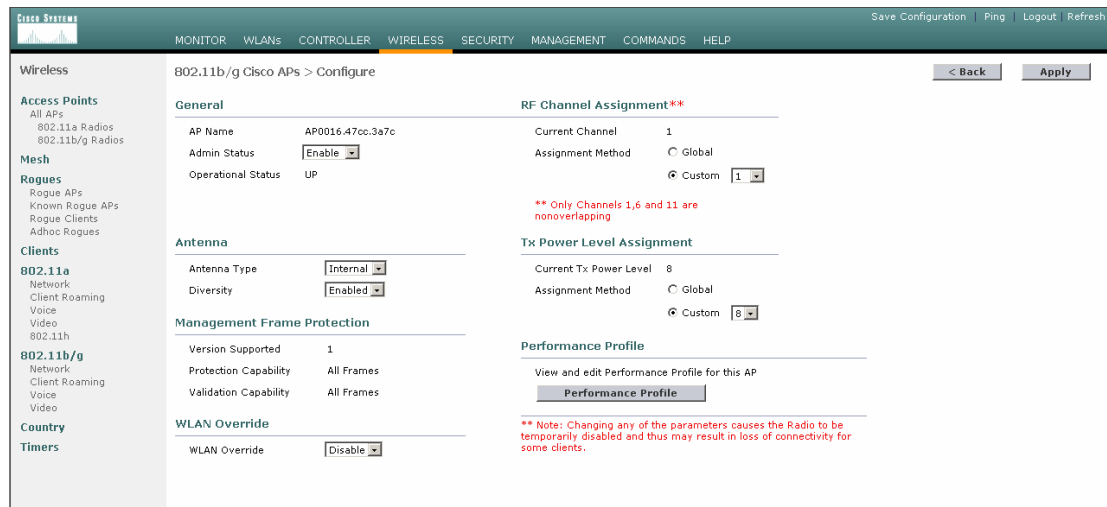
AP Name	Base Radio MAC	Operational Status	Load Profile	Noise Profile	Interference Profile	Coverage Profile
AP0016.47cc.3a7c	00:15:c7:a9:1f:40	UP	Passed	Passed	Passed	Passed

3. From the main menu, select **Wireless**. Under **Access Points**, select **802.11b/g Radios**.



Global settings for **RF Channel Assignment** and **TX Power Level Assignment** were not tested in VIEW certification. For **Custom Power** and **Channel** settings please consult your facilities RF site survey—optimized for wireless voice traffic—to determine correct power and channel settings for each AP using only channels 1, 6 and 11.

4. Set **Admin Status** to **Enable**.
5. Configure any other settings that might be relevant to your deployment as needed.
6. Click **Apply** to save all changes.



**Wireless** 802.11b/g Cisco APs > Configure

**General**

AP Name: AP0016.47cc.3a7c  
 Admin Status: ☒ Enable  
 Operational Status: UP

**Antenna**

Antenna Type: ☒ Internal  
 Diversity: ☒ Enabled

**Management Frame Protection**

Version Supported: 1  
 Protection Capability: All Frames  
 Validation Capability: All Frames

**WLAN Override**

WLAN Override: ☒ Disable

**RF Channel Assignment\*\***

Current Channel: 1  
 Assignment Method: ☐ Global ☒ Custom [1]

**\*\* Only Channels 1,6 and 11 are nonoverlapping**

**Tx Power Level Assignment**

Current Tx Power Level: 8  
 Assignment Method: ☐ Global ☒ Custom [8]

**Performance Profile**

View and edit Performance Profile for this AP

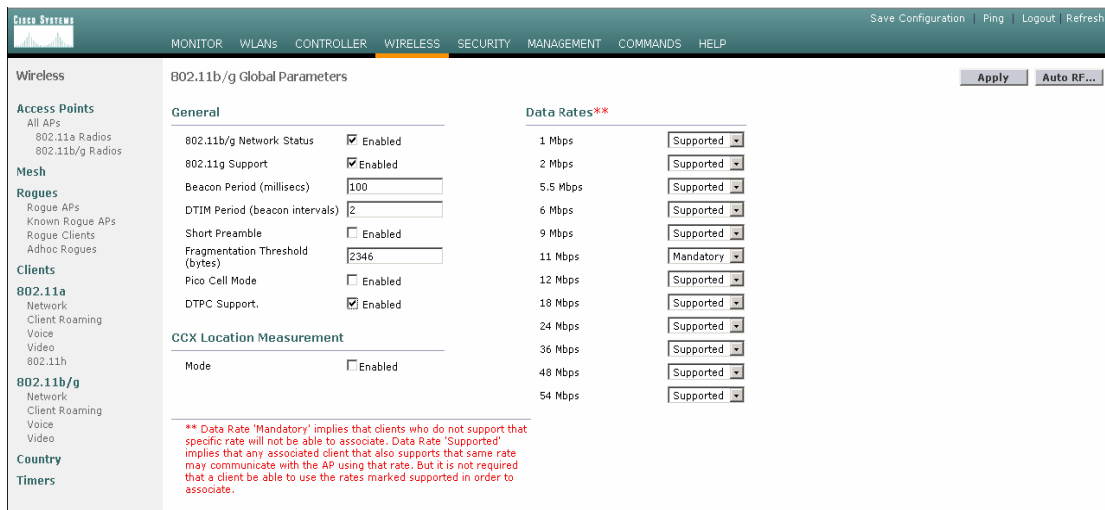
**\*\* Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.**

7. Under **802.11b/g**, select **Network**.
8. Enable **802.11b/g Network Status** and **802.11g Support**, if g clients are present.
9. For setting up the **Data Rates**, to optimize throughput the data rates should be configured as **Supported** for 1.0, 2.0, and 5.5 Mb/sec with 11 Mb/sec set as



**Mandatory.** To support this data rate set, signal strength of -60 dBm or stronger is required wherever the wireless telephones are to be used. To optimize range, the data rates should be configured as **Supported** for 2.0, 5.5 and 11 Mb/s with 1 Mb/s set as **Mandatory**. To support this data rate set, signal strength of -70 dBm or stronger is required wherever the handset is to be used. The screen capture below is set to optimize throughput. All 802.11g rates must be set as **Supported** or **Disabled** for NetLink handsets to operate.

10. Use the default **Fragmentation Threshold** (2346 bytes).
11. Set the **Beacon Period** to **100**.
12. Set the **DTIM Interval** to **2**. (this is to ensure the best PTT performance)
13. Do not enable **Short Preamble**.
14. NetLink handsets do not support dynamic power and will not utilize the information element that is set when **DTPC support** is enabled. NetLink handset power should be configured to match the highest transmit power of the APs.
15. Click **Apply** to save the settings.



**Wireless** 802.11b/g Global Parameters Apply Auto RF...

**Access Points**  
All APs  
802.11a Radios  
802.11b/g Radios

**Mesh**

**Rogues**  
Rogue APs  
Known Rogue APs  
Rogue Clients  
Adhoc Rogues

**Clients**

**802.11a**  
Network  
Client Roaming  
Voice  
Video  
802.11h

**802.11b/g**  
Network  
Client Roaming  
Voice  
Video

**Country**

**Timers**

**General**

802.11b/g Network Status ☒ Enabled

802.11g Support ☒ Enabled

Beacon Period (milliseconds)

DTIM Period (beacon intervals)

Short Preamble ☐ Enabled

Fragmentation Threshold (bytes)

Pico Cell Mode ☐ Enabled

DTPC Support ☒ Enabled

**CCX Location Measurement**

Mode ☐ Enabled

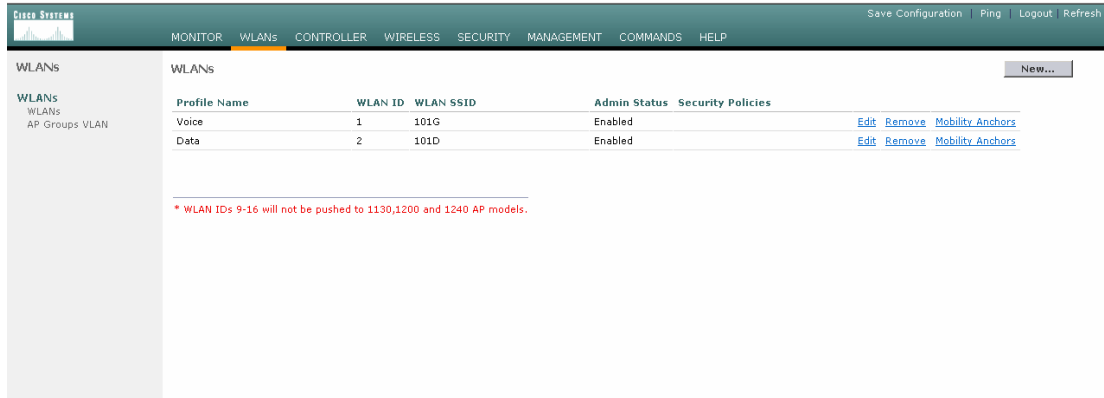
**Data Rates\*\***

1 Mbps	Supported
2 Mbps	Supported
5.5 Mbps	Supported
6 Mbps	Supported
9 Mbps	Supported
11 Mbps	Mandatory
12 Mbps	Supported
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

\*\* Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate.

## Setting up the SSID

It is required for voice and data to be on separate SSIDs to prioritize voice traffic. The voice SSID must be set to **Platinum** for **Quality of Service** and the data SSID must be set to **Silver** for **Quality of Service**.



1. Select **WLANS** from the main menu.
2. Enter a name for the **WLAN SSID**.
3. Set the **Radio Policy** to **802.11b/g**.
4. Enable **Admin Status**.
5. Set **Session Timeout** to **0**.
6. Set **Quality of Service** to **Platinum** (Note: This is the required setting for voice traffic).
7. Set **WMM Policy** to **Disabled**. (Note: This is required for usage with NetLink handsets.)
8. Under **Security Policies**, select desired security policy (either **WPA** or **WPA2**) and enter all required options.
9. Click **Apply** to save all changes.

Cisco Systems

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Save Configuration Ping Logout Refresh

WLANS

WLANS  
AP Groups VLAN

WLANS > Edit

WLAN ID 1

Profile Name Voice

WLAN SSID 101G

General Policies

Radio Policy 802.11b/g only

Admin Status ☒ Enabled

Session Timeout (secs) 0

Quality of Service (QoS) Platinum (voice)

WMM Policy Disabled

7920 Phone Support ☐ Client CAC Limit ☐ AP CAC Limit

Broadcast SSID ☒ Enabled

Aironet IE ☐ Enabled

Allow AAA Override ☐ Enabled

Client Exclusion ☐ Enabled \*\*

DHCP Server ☒ Override 192.168.2.99  
DHCP Server IP Addr

DHCP Addr. Assignment ☐ Required

Interface Name management

MFP Version Required 1

MFP Signature Generation ☒ (Global MFP Disabled)

H-REAP Local Switching ☐

\* H-REAP Local Switching not supported with IPSEC, CRANITE and FORTRESS authentications.

Security Policies

IPv6 Enable ☐

Layer 2 Security WPA1+WPA2

☐ MAC Filtering

Layer 3 Security None

☐ Web Policy \*

\* Web Policy cannot be used in combination with IPsec.  
\*\* When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)  
\*\*\* CKIP is not supported by 10xx APs

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	none	<input checked="" type="checkbox"/> Enabled none
Server 2	none	none
Server 3	none	none

WPA1+WPA2 Parameters



WEP was not tested during VIEW Certification. WEP is supported by both the LWAPPs and the NetLink Wireless Telephones.

## Enabling SVP (SpectraLink Voice Priority) on the Controller and Access Points

SpectraLink packets must be given priority in order to enable SVP on the controller.

1. Use a console cable to access the Command Line Interface. In admin mode enter **config advanced edca-parameters svp-voice**. This command will enable QoS for SpectraLink packets.
2. To bring the priority change into effect, the radios on the APs will need to be disabled and re-enabled. Accomplish this through the GUI configuration interface of the controller.
3. From the main menu select **Wireless**, under **802.11b/g** select **Network**.
4. Disable the **802.11b/g Network Status** and click **Apply**.
5. Re-enable the **802.11b/g Network Status** and click **Apply**.
6. To verify the QoS change has taken effect, use the console cable to connect to the APs. Enter “show controllers d0” to show the edca-parameters for the 802.11b/g radio. The output should display the following if the SVP edca-parameters are enabled:

```
Back: cw-min 4 cw-max 10 fixed-slot 7 admission-control Off txop 0
Best: cw-min 4 cw-max 6 fixed-slot 3 admission-control Off txop 0
Video: cw-min 3 cw-max 4 fixed-slot 3 admission-control Off txop 3008
Voice: cw-min 0 cw-max 3 fixed-slot 2 admission-control Off txop 1504
```

**802.11b/g Global Parameters**

**General**

- 802.11b/g Network Status: ☒ Enabled
- 802.11g Support: ☒ Enabled
- Beacon Period (milliseconds):
- DTIM Period (beacon intervals):
- Short Preamble: ☐ Enabled
- Fragmentation Threshold (bytes):
- Pico Cell Mode: ☐ Enabled
- DTPC Support: ☒ Enabled

**Data Rates\*\***

1 Mbps	Supported
2 Mbps	Supported
5.5 Mbps	Supported
6 Mbps	Supported
9 Mbps	Supported
11 Mbps	Mandatory
12 Mbps	Supported
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

**CCX Location Measurement**

- Mode: ☐ Enabled

\*\* Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate.

7. From the GUI interface, go to **Controller**.
8. Select **QoS Profiles**.
9. Select **Platinum**.
10. Change **Wired QoS Protocol** to **802.1p**, set the **802.1p Tag** to **7** and click **Apply**.

Cisco Systems

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Save Configuration Ping Logout Refresh

Controller

General Inventory Interfaces Network Routes Internal DHCP Server Mobility Management Mobility Groups Mobility Statistics Spanning Tree Ports Master Controller Mode Network Time Protocol QoS Profiles

Edit QoS Profile

QoS Profile Name platinum

Description For Voice Applications

Per-User Bandwidth Contracts (k) \*

Average Data Rate 0

Burst Data Rate 0

Average Real-Time Rate 0

Burst Real-Time Rate 0

Over the Air QoS

Maximum RF usage per AP (%) 100

Queue Depth 100

Wired QoS Protocol

Protocol Type 802.1p

802.1p Tag 7

\* The value zero (0) indicates the feature is disabled

## Further Assistance

1. An installation and configuration guide for the 4400 WLC can be found on Cisco's website:  
[http://www.cisco.com/en/US/products/ps6366/products\\_quick\\_start\\_chapter09186a008056add1.html](http://www.cisco.com/en/US/products/ps6366/products_quick_start_chapter09186a008056add1.html).
2. To convert the 1200 Series autonomous AP to an LWAPP, go to:  
[http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_technical\\_reference09186a00804fc3dc.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00804fc3dc.html)
3. For more information on the LWAPP-Enabled APs, see *Quick Start Guide LWAPP-Enabled Cisco Aironet Access Points* at:  
[http://www.cisco.com/en/US/products/hw/wireless/ps430/products\\_quick\\_start09186a00805100f5.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/products_quick_start09186a00805100f5.html)
4. For other assistance, contact either Cisco or SpectraLink's customer service at:  
[www.cisco.com](http://www.cisco.com)  
<http://www.spectralink.com/consumer/index.jsp>