



Cisco 4400 Series Wireless LAN Controller (WLC) with 802.1x Authentication for Avaya 3631 Wireless Telephone Configuration and Deployment Guide

This document details how to configure the Cisco 4400 series WLC with 802.1x Authentication for use with Avaya 3631 wireless IP telephones.

Product Summary

Manufacturer: Cisco Systems: www.cisco.com
Products 4400 series WLC with AP 1131 and LWAPP capable 1200 series APs
Cisco 4400 series WLC's Software version: 4.1.185.0
RF technology: Spread spectrum direct sequence (DS)
Radio: 2.4 – 2.484 GHz
Security: 802.1 x
Recommended network topology: Switched Ethernet (required)

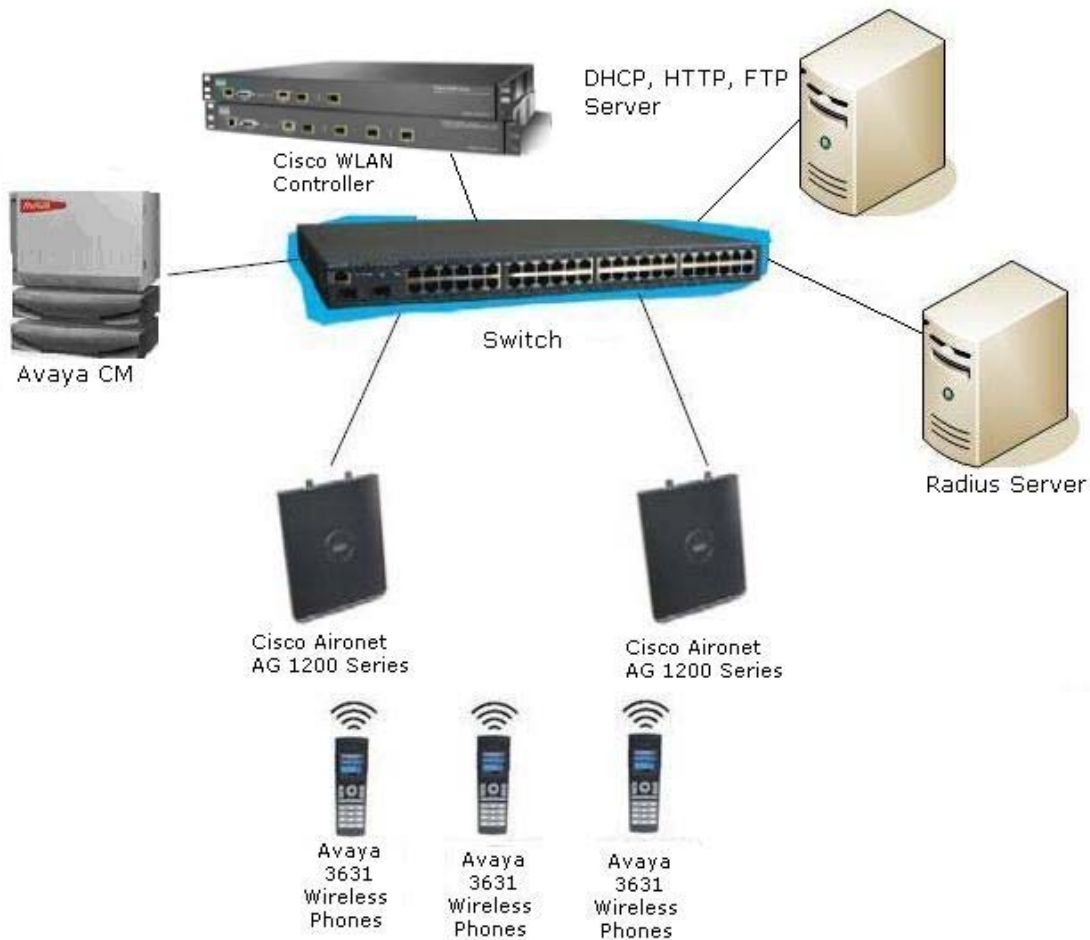
Service Information

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 for instructions on this procedure. Once the APs are converted, this document can be used to provision LWAPP APs.

Note: Cisco's web link to convert the Autonomous AP to LWAPP is provided at the end of this document.

Network Topology

The following topology is an example configuration using a Cisco WLC and Cisco LWAP APs across different subnets. It is important to note that these do not necessarily represent all possible configurations.



The setup indicates that the WLAN Controller, APs and all the servers (Avaya CM, DHCP & Radius Servers) are connected to the switch. Avaya 3631 Wireless IP telephones are connected to the APs.

Known Limitations

No limitations were discovered during testing.



Cisco WLAN Controller (WLC) Configuration Configuring a New Controller Starting From Factory Defaults Connecting to WLC via the Console

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.

Basic Configuration

1. 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.
2. The Configuration Guide provides an easy means to perform initial controller setup and provisioning. Refer to the "*Cisco Wireless LAN Controller Configuration Guide*" found at Cisco's web site. This document contains a detailed explanation of using the Startup Wizard:

<http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ccfig40.html>

3. Once the controller has been configured via the Configuration Guide, the remaining configuration can be configured through the switch-web interface using a web-browser (Cisco recommends using MS IE 6.0+).



Configuration Note

Configuring the Cisco WLAN Controller for use with Avaya 3631 phones

Further configurations of the Cisco WLC can be done both using a Web Browser interface or a Command Line interface. Avaya recommends using the Web Browser interface as described in the following sections.

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:

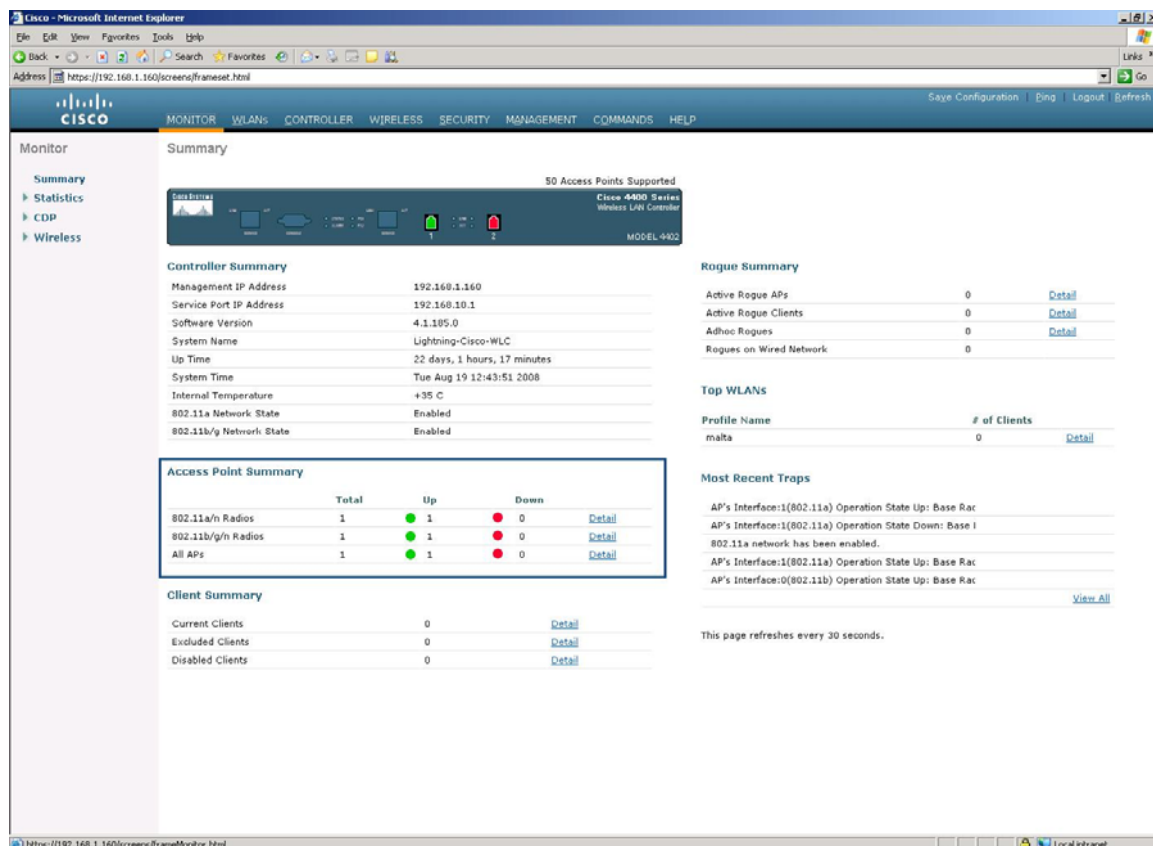


Figure 1: Monitor

4. The highlighted area shows the number of APs connected to the Wireless LAN Controller (Figure 1).



Configuration Note

Installing Software

1. Make sure that the latest 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 **Wireless LAN Controller Software Downloads** 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, preferably IE. 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.



Configuration Note

Controller Setup

The initial setup of the controller is shown below. Note that 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.

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

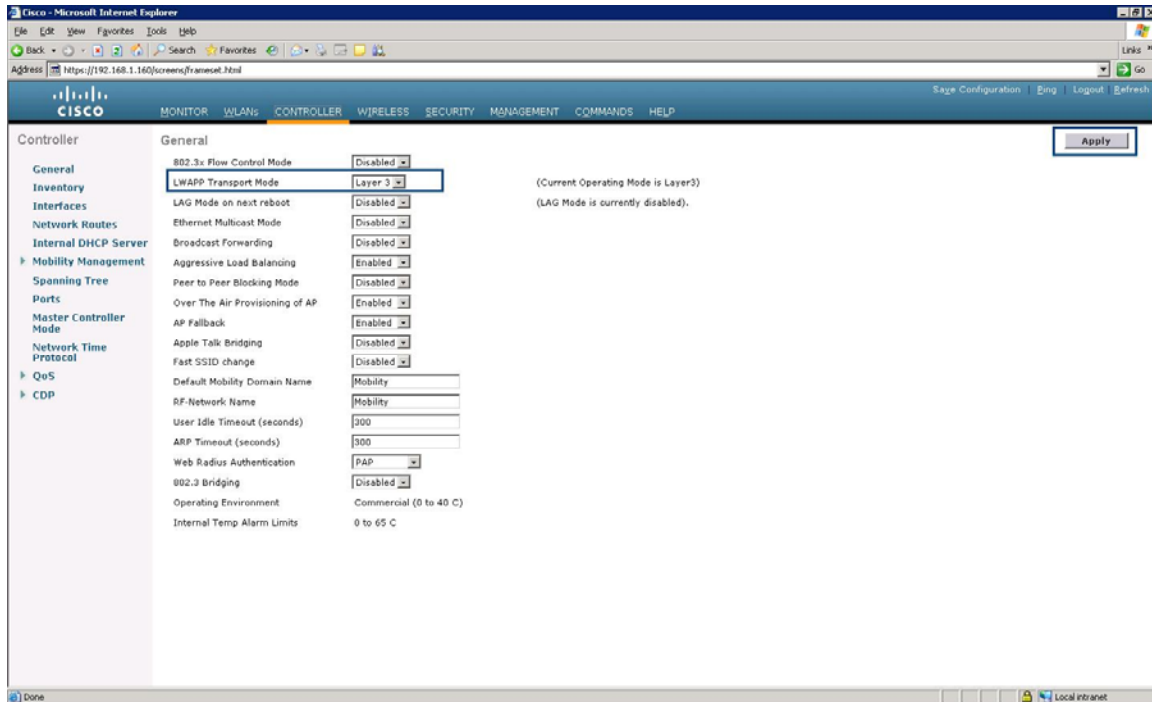


Figure 2: Controller

1. From the main menu, select **Controller** (Figure 2).
2. Set the **LWAPP Transport Mode** to **Layer 3**.
3. Click **Apply** and **Save Configuration**.



Configuration Note

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. In case of APs connected to other subnets than the controller, the LWAPP Discovery Algorithms try to retrieve the controllers AP-Manager IP Address from the DHCP server or from DNS Servers (if available). See "Using DHCP Option 43" and "Using the DNS for Controller Discovery" in the "Cisco WLAN Controller Configuration Guide".

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 hand out leases to the AP). The instructions for doing so are included at the end of this document.

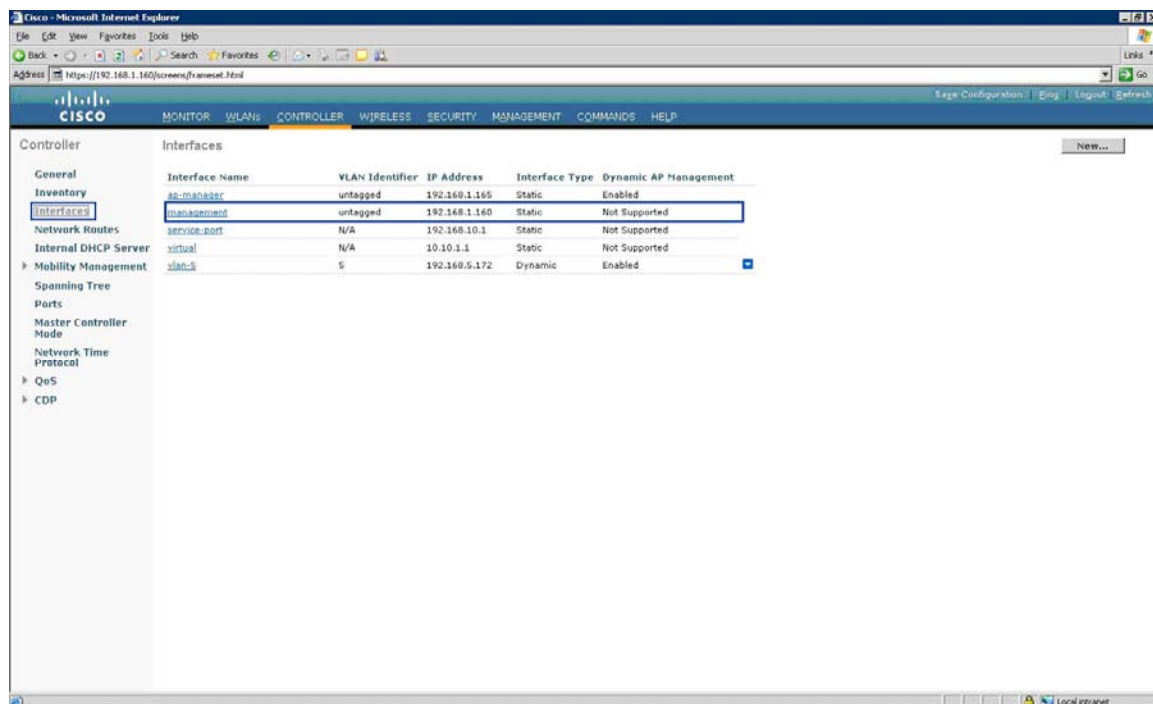


Figure 3: Interfaces

1. From the main menu, select **Controller>Interfaces** (Figure 3). Verify that the proper IP Addresses are assigned to the interfaces.
2. Select the **Management interface**.

The screenshot shows the Cisco WLC configuration page for the 'management' interface. The left sidebar contains a navigation menu with options like General, Inventory, Interfaces, Network Routes, Internal DHCP Server, Mobility Management, Spanning Tree, Ports, Master Controller Mode, Network Time Protocol, QoS, and CDP. The main content area is titled 'Interfaces > Edit' and contains several sections: General Information (Interface Name: management, MAC Address: 00:1b:d4:6b:06:a0), Interface Address (VLAN Identifier: 0, IP Address: 192.168.1.160, Netmask: 255.255.255.0, Gateway: 192.168.1.1), Physical Information (Port Number: 1, Backup Port: 0, Active Port: 1), DHCP Information (Primary DHCP Server: 192.168.5.152, Secondary DHCP Server: 0.0.0.0), and Access Control List (ACL Name: none). A 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.'

Figure 4: DHCP Information

3. Under **DHCP Information** (Figure 4), enter the IP address of the DHCP server. Repeat this step for the **AP-Manager** interface.
4. Click **Apply** and save the changes.
5. Power-on and connect the APs to the network. Wait a few minutes for the APs to find the controller.
6. 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 Configuration

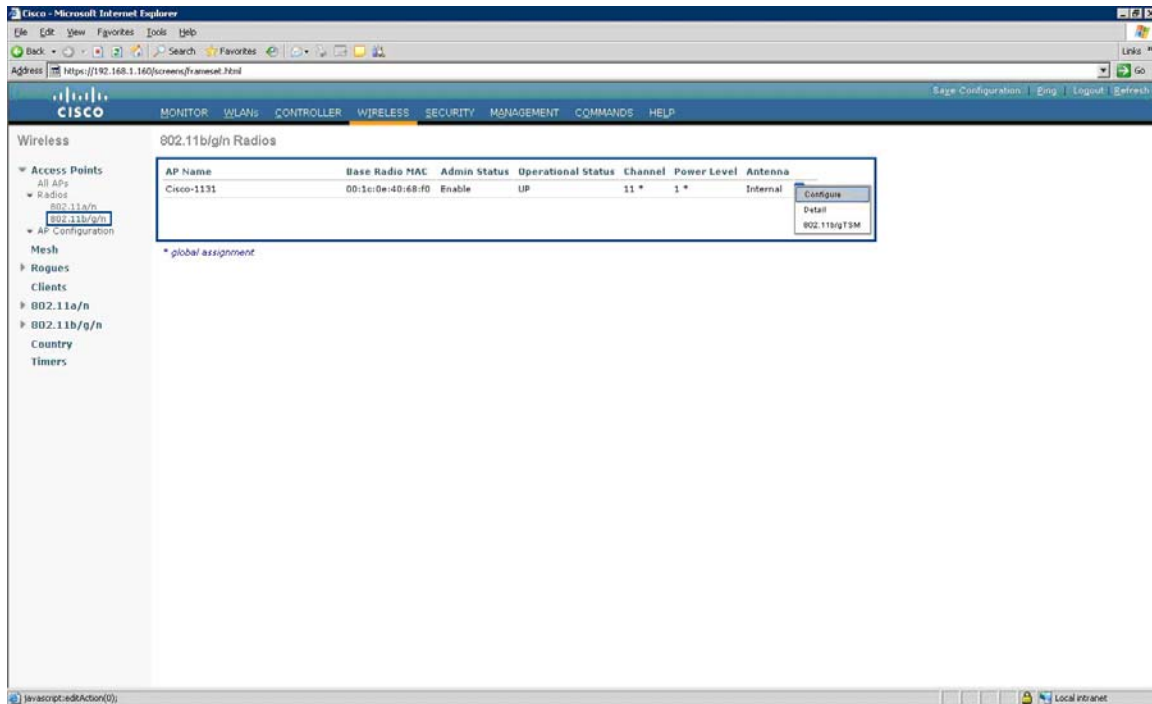


Figure 5: 802.11 b/g/n Radios

1. From the main menu, select **Wireless**. Under **Access Points**, select **802.11b/g/n Radios** (Figure 5).
2. Press the **Down Arrow** and Click the **Configure** option.

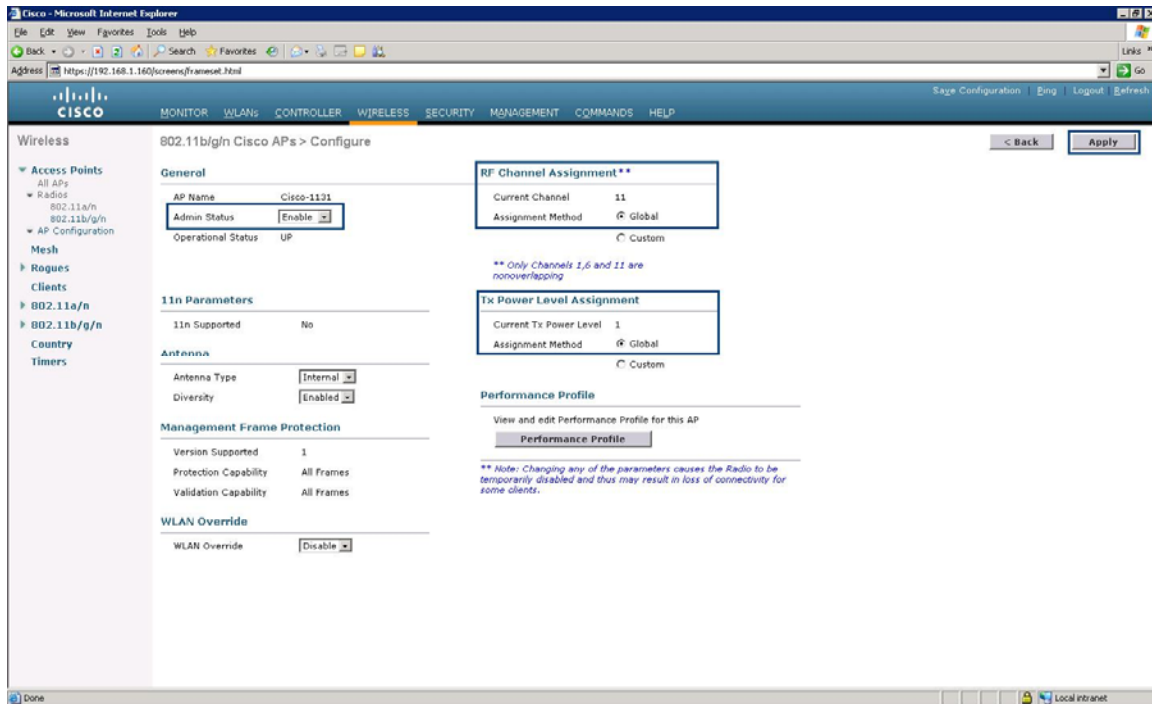


Figure 6: Configuring 802.11b/g/n Cisco APs

3. Set both the **RF Channel Assignment** and **Tx Power Level Assignment** to **Global** (Figure 6). This will force the APs to use only channels 1, 6, or 11 and to select the proper power level dynamically as needed to avoid interference and noise.
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.

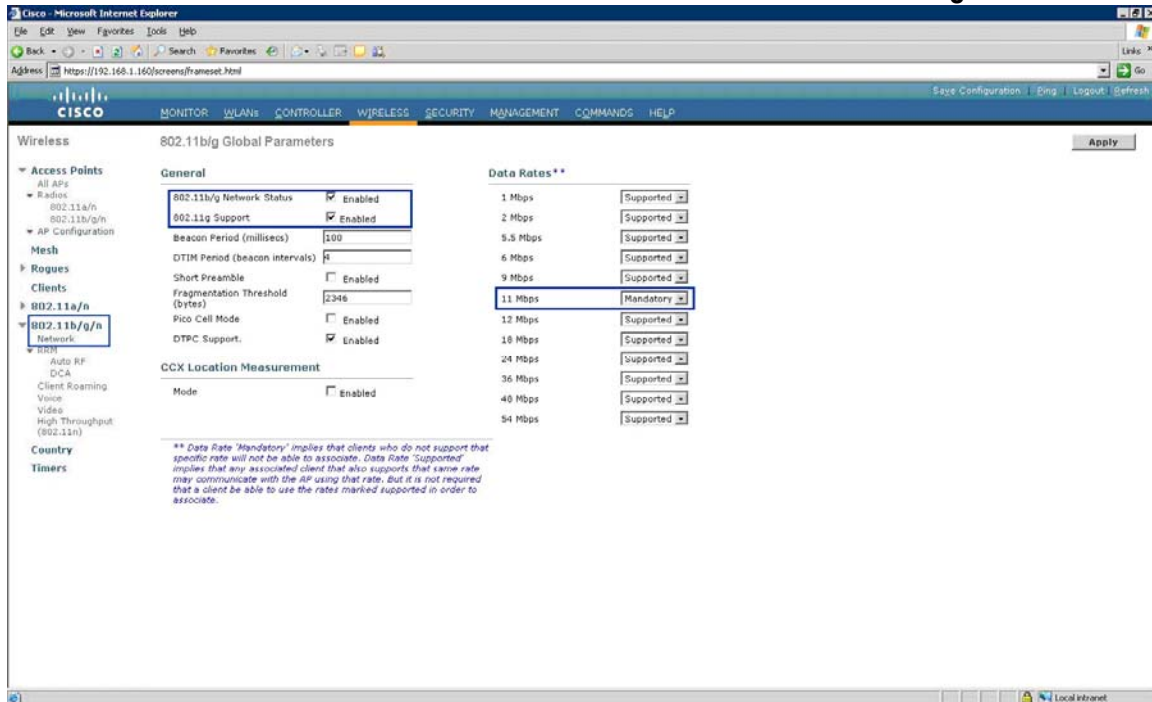


Figure 7: 802.11b/g Global Parameters

6. Under **802.11b/g/n**, select **Network** (Figure 7).
7. Enable **802.11b/g Network Status** and **802.11g Support**.
8. Set **11Mbps** to **Mandatory**. Set all other data rates to **Supported**.
9. Use the default **Fragmentation Threshold** (2346 bytes).
10. Set the **Beacon Period** to 100ms.
11. Set the **DTIM Interval** to 4.
12. Do not enable **Short Preamble**.
13. Enable **DTPC Support**.
14. Click **Apply** to save the settings.



Radius Server Configuration

Configuration Note

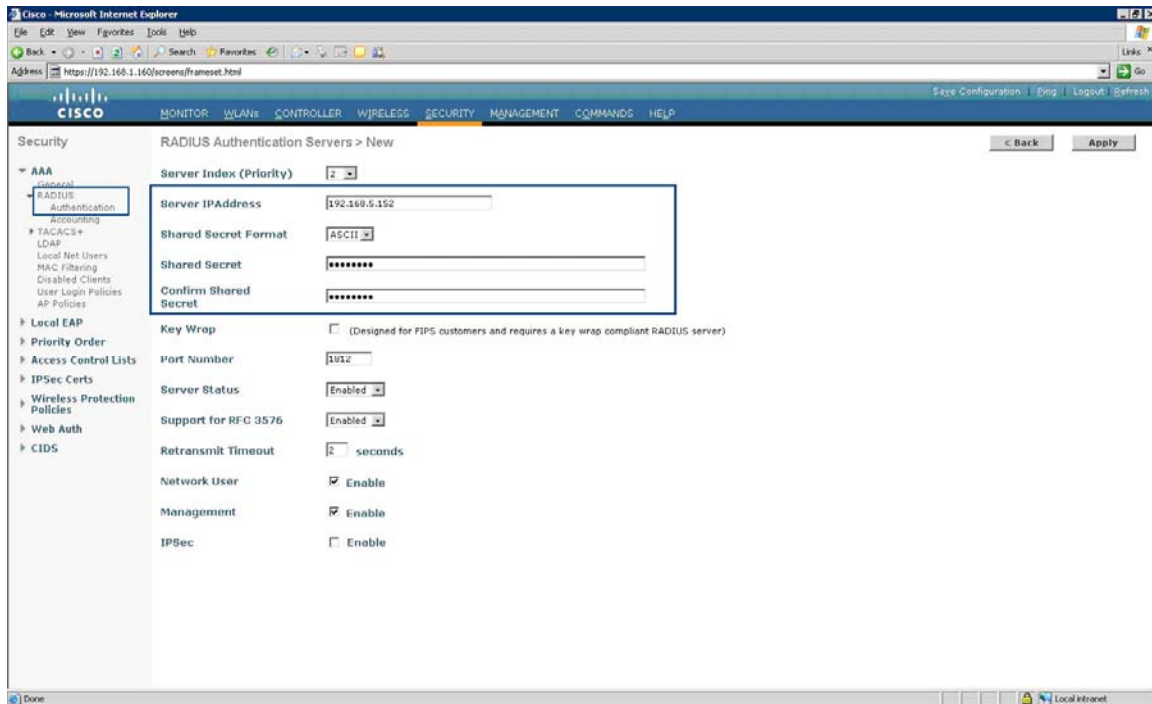


Figure 8: New Radius Authentication Servers

1. From the main menu, select **Security** and Click the **New** Button to add the Radius Server (Figure 8).
2. Enter the **Server IP Address** and **Shared Secret** (ex: avaya123). The shared secret should match with the secret key on the Radius Server. (Radius Server Configuration is out of the scope of this document).
3. Enable **Server Status**, **Network User** and **Management**.
4. Click **Apply** to save the settings.

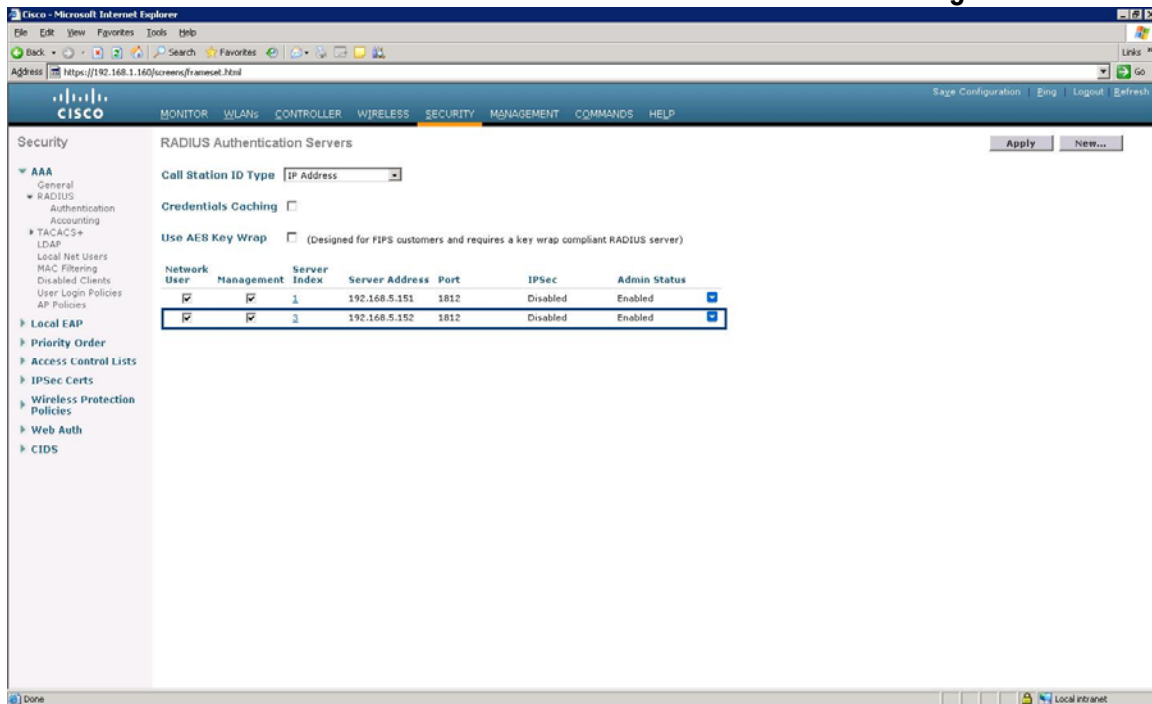


Figure 9: Radius Authentication Servers

5. The entry for the **Radius Server** will be seen under **Security** Tab (Figure 9). More Radius Servers can be added as per the network design.



Configuration Note

Setting up the SSID

Setting up a separate SSID for your 3631 phones allows better optimization of your WLAN configuration, e.g. regarding security policy and quality of service. In combination with setting up dynamic interfaces (**Controller > Interfaces**) the clients of different SSIDs can also be assigned to different VLANs (not scope of this document). When using a common SSID, the settings must be sufficient for all clients which might cause some changes to the following.

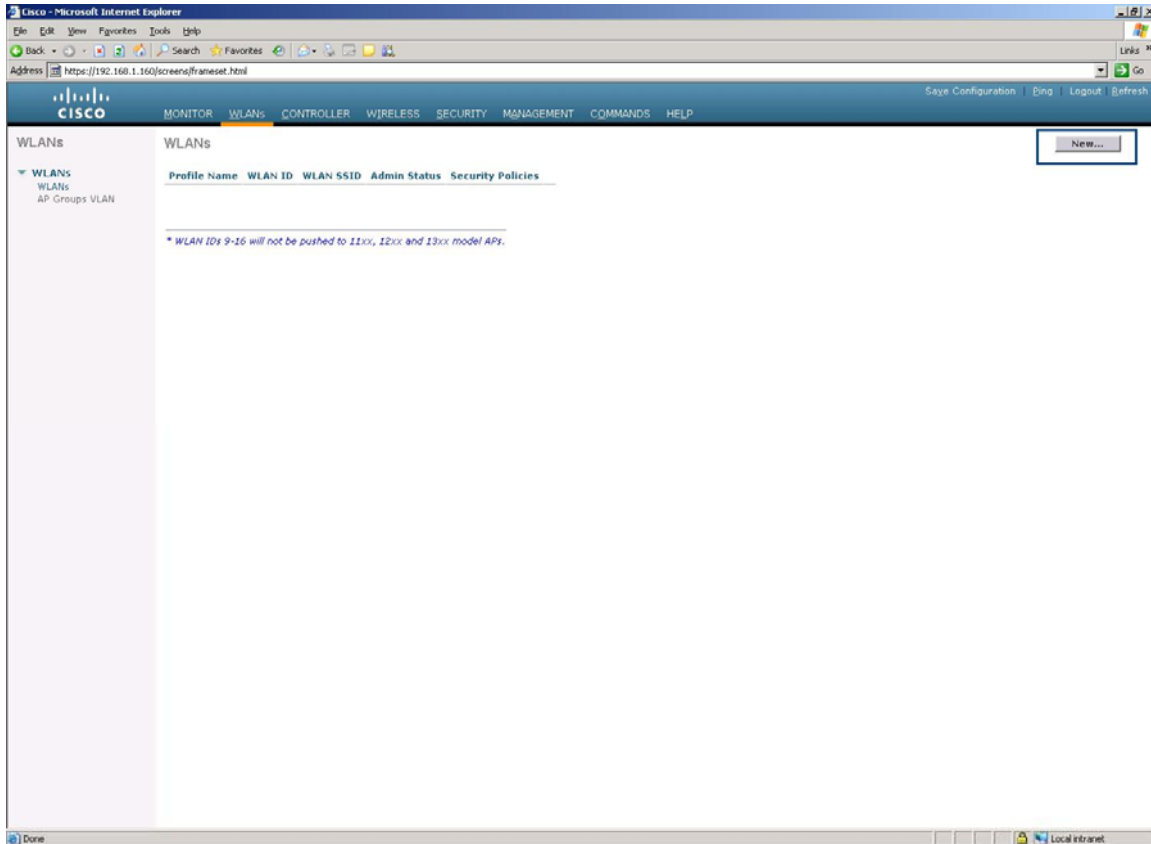


Figure 10: WLAN

1. Select **WLANs** from the main menu. Click on **New** to create a new SSID (Figure 10).

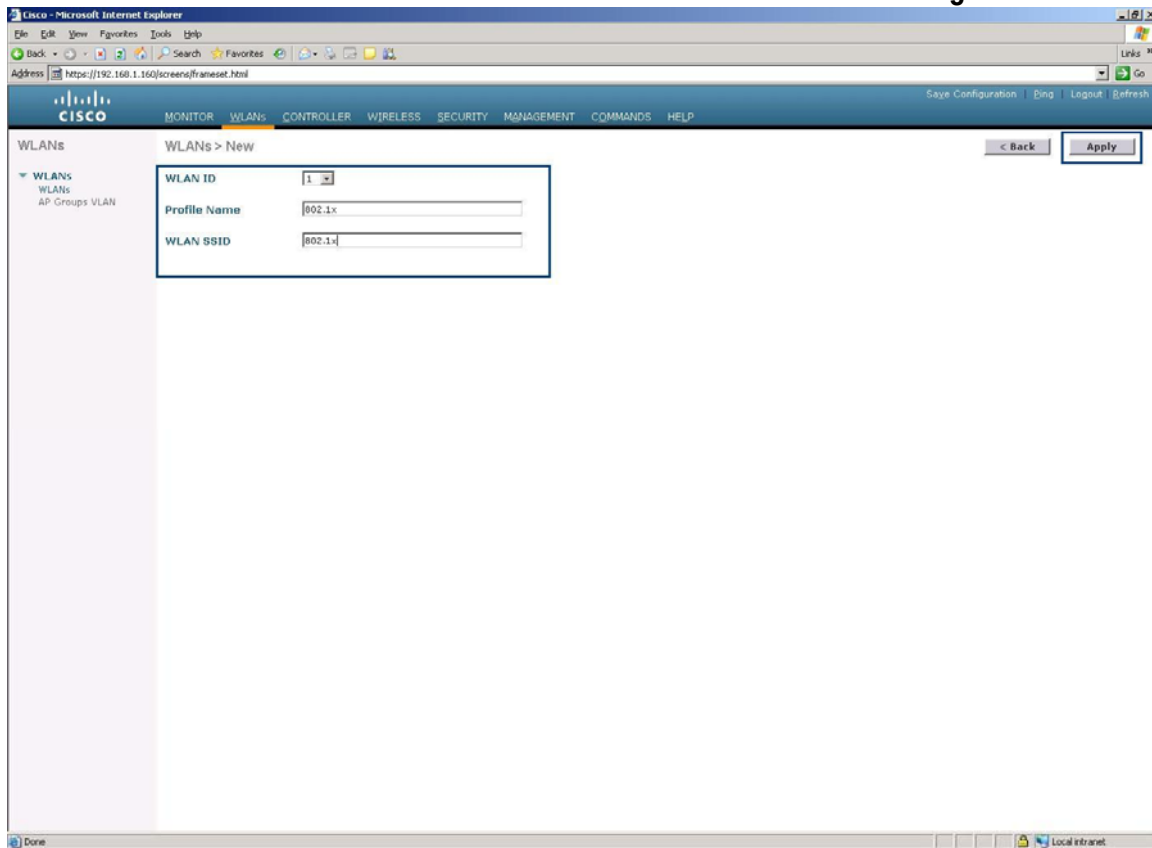


Figure 11: New WLAN Profile

2. Enter the **Profile Name** and a name for the **WLAN SSID** (Figure 11). Click **Apply** to save the settings.

Note: "802.1X" is only an example name.

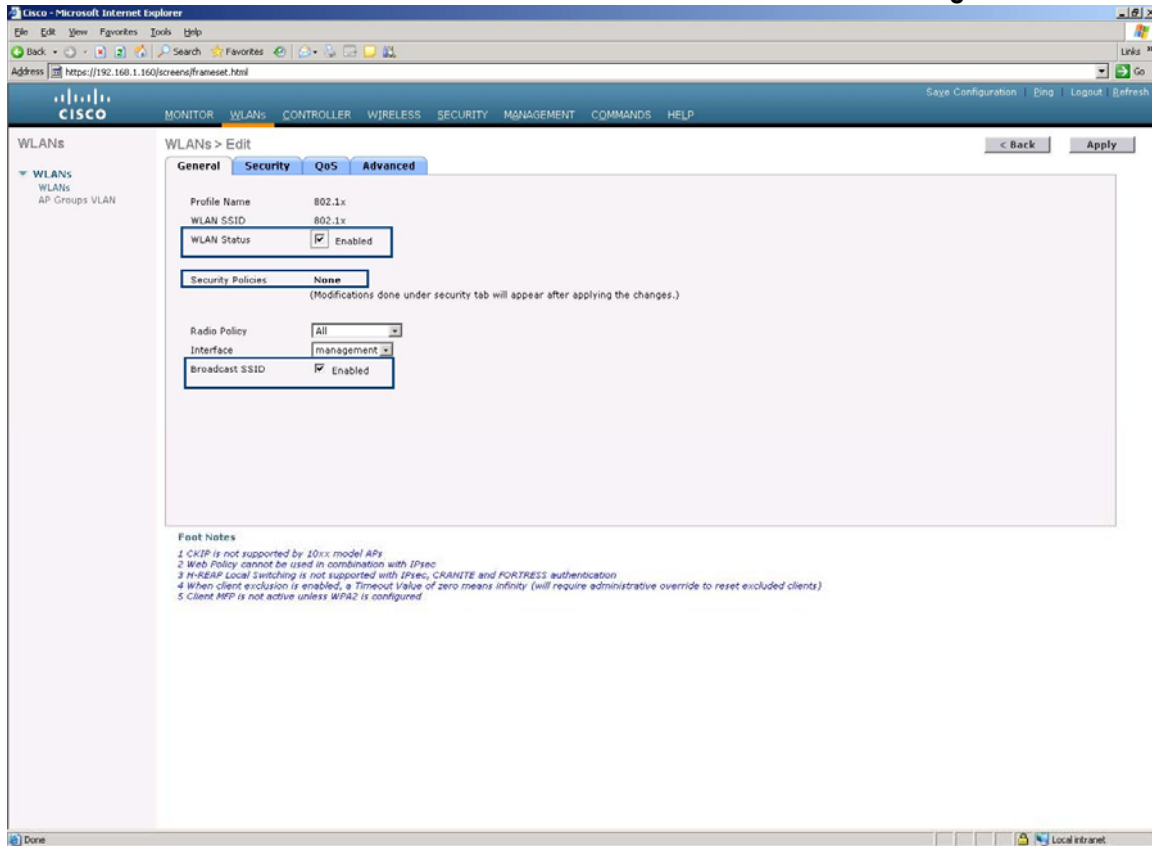


Figure 12: Editing WLAN Profile

3. Under **General** Tab (Figure 12), Enable **WLAN Status** and **Broadcast SSID**.

4. Click the **Security** tab.

Note: Security Policies is "None" by default. Select the appropriate Security as required, by clicking on the security tab.

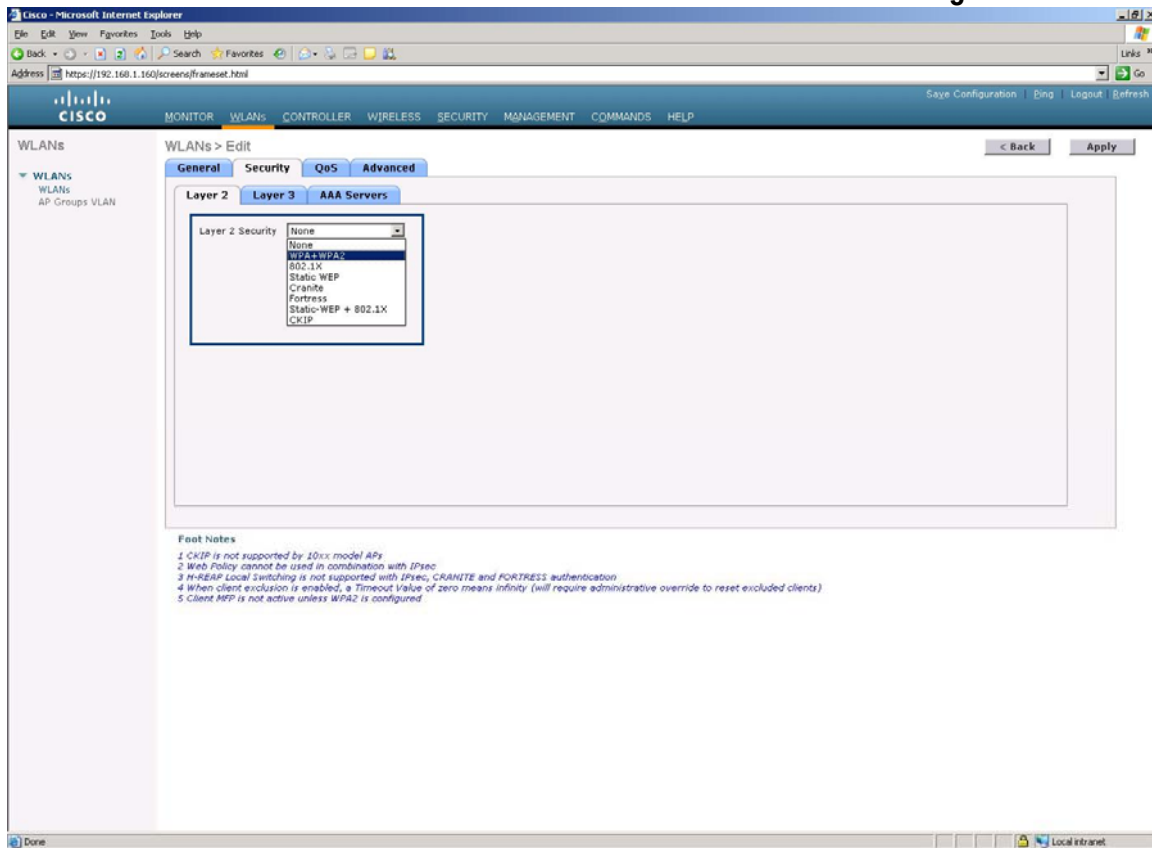


Figure 13: Security

5. Under **Security Tab** → **Layer 2 Sub Tab** (Figure 13), Select **WPA + WPA2**.

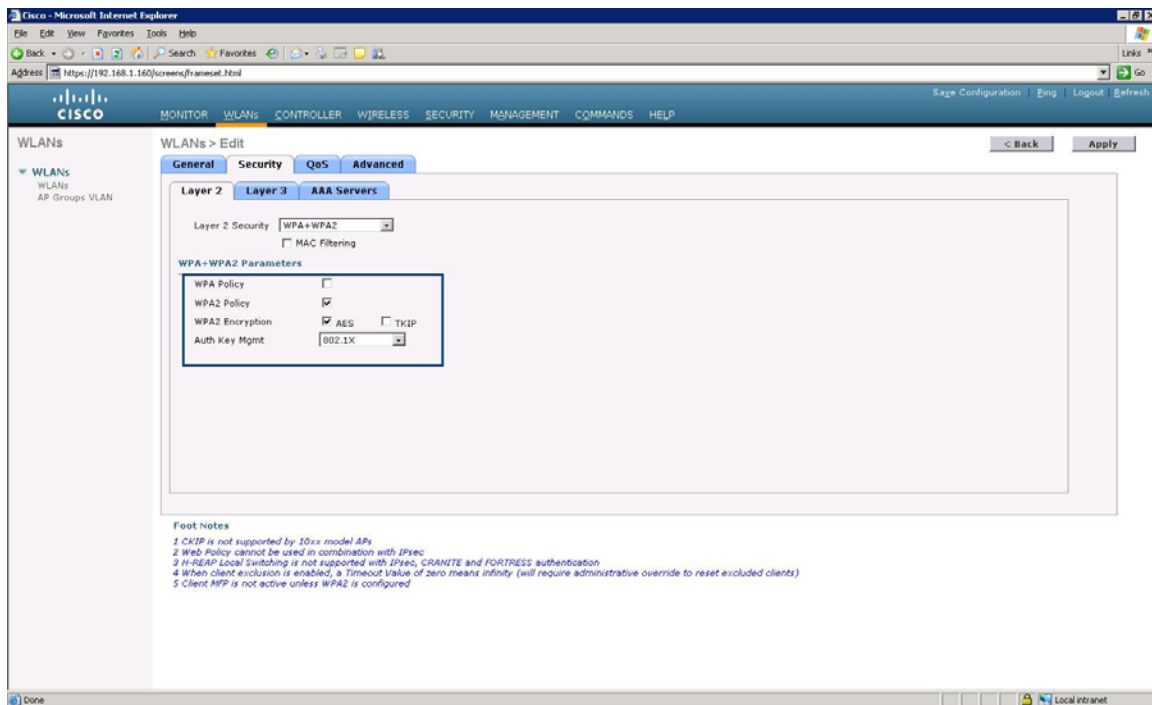


Figure 14: Security



Configuration Note

6. Select **WPA Policy and TKIP** or **WPA2 Policy and AES** (Figure 14).
7. **MAC Filtering** may be enabled for further improvement of security. Use **Security** → **MAC Filtering** to enter the MAC addresses of your phones if you enabled MAC Filtering.

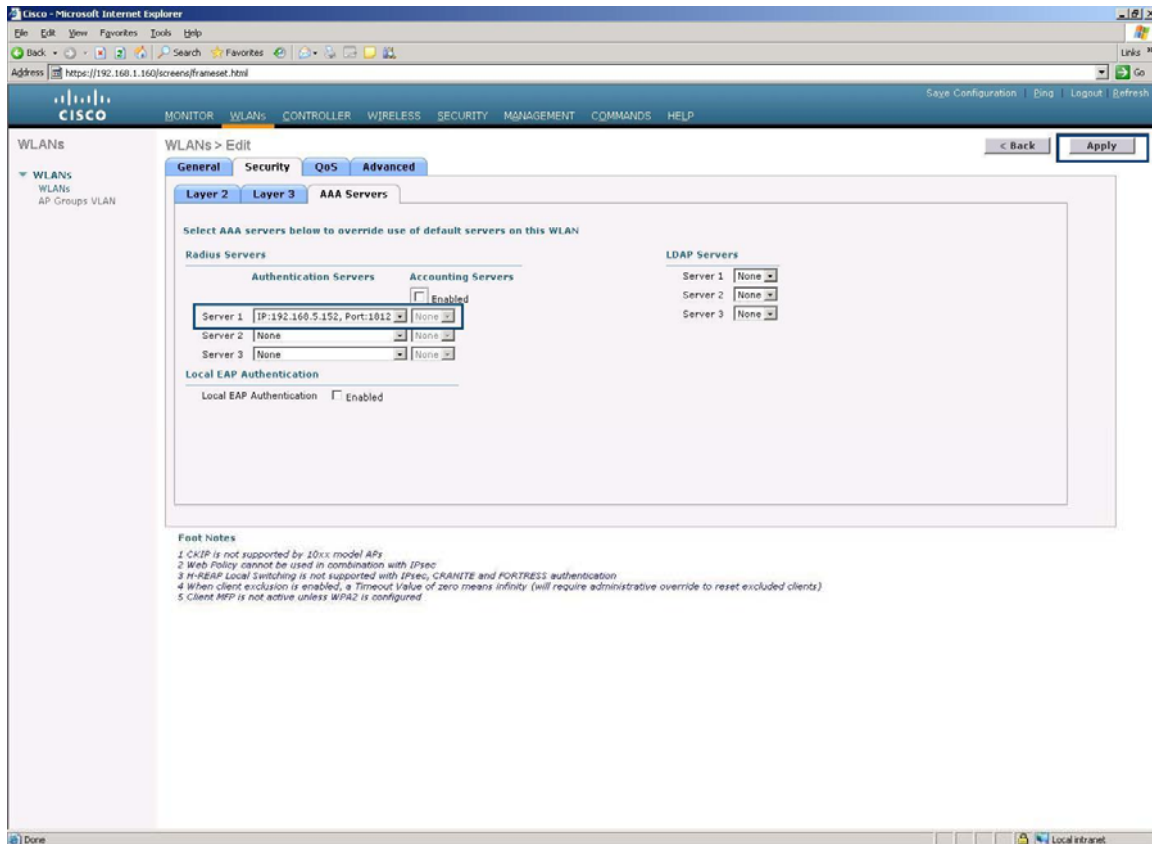


Figure 15: AAA Servers

8. Go to **AAA Servers** Sub tab (Figure 15), select the Server 1 as per the requirement of the network.
- Note: "AAA" server is just another word for "RADIUS".
9. Click **Apply** to save the settings.

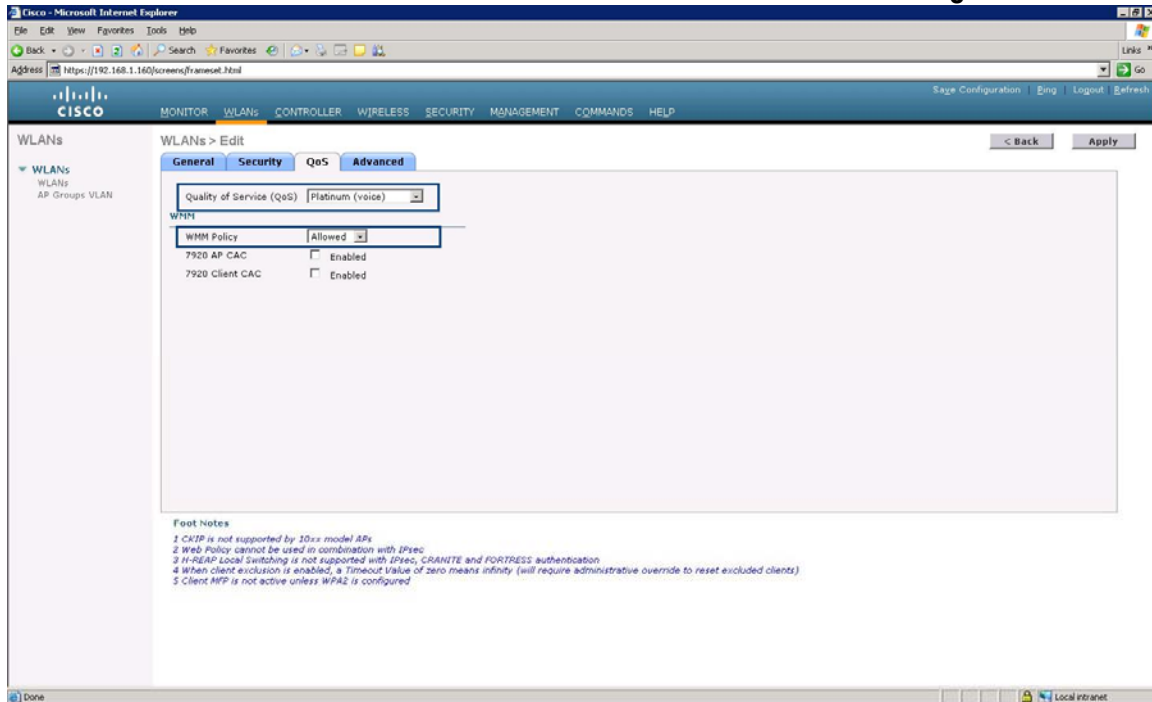


Figure 16: QoS

10. Set Quality of Service to Platinum (recommended setting for voice traffic) (Figure 16).
 11. Set WMM Policy to Required (requires all clients of this SSID to use WMM) or to Allowed.
- Note: It is important to enable WMM on the 3631 Wireless IP Phones.

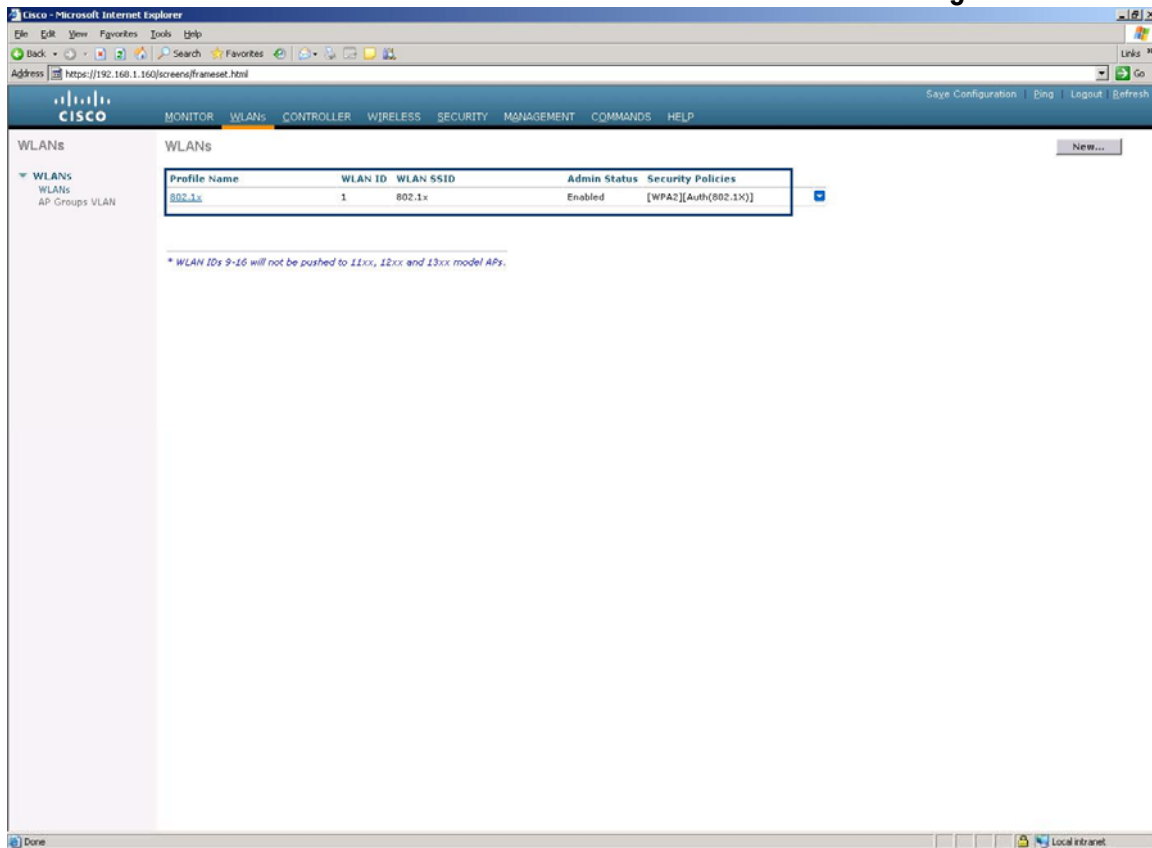


Figure 17: WLANs

12. The entry for the new SSID appears under the WLAN tab (Figure 17).
13. Click Save Configuration to save your configuration in case of a controller restart.



Configuration Note

Setting Up the Internal DHCP Server (Optional)

The internal DHCP server can be used for Avaya wireless handsets 3631. The setup is shown below. Please note that this DHCP Server is used exclusively by the WLAN clients connected to your Cisco WLAN controller. It can not be used by APs, the controller itself or any other LAN devices.

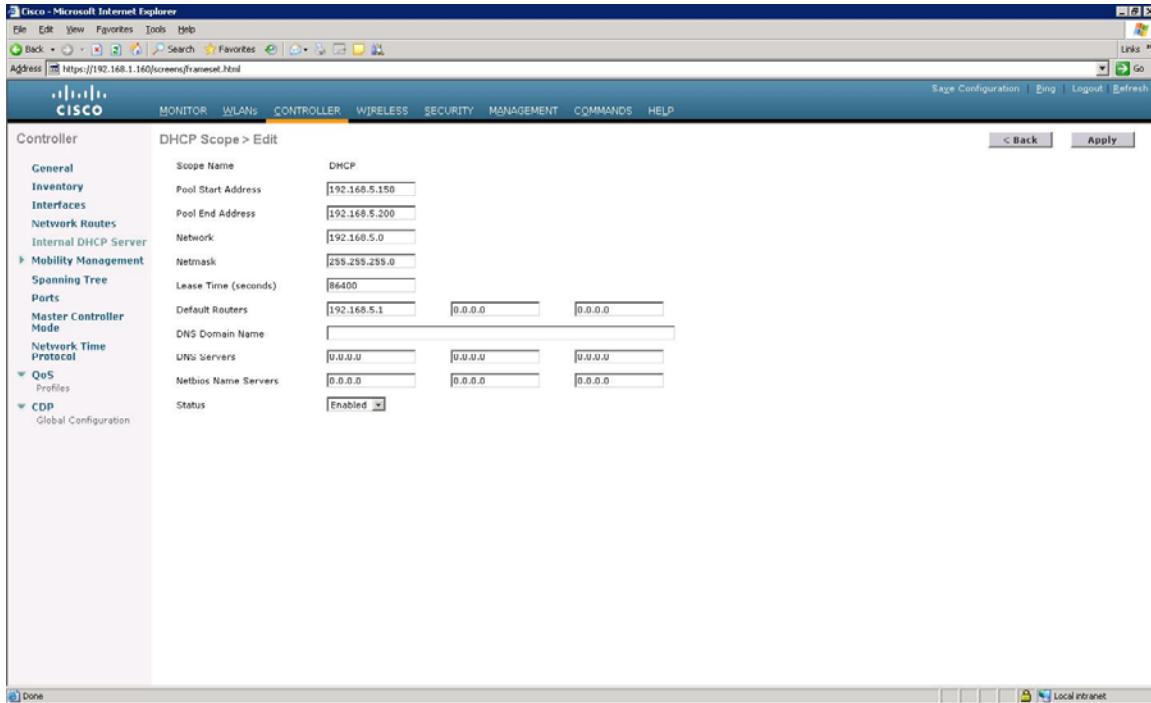


Figure 18: Editing DHCP Scope

1. From the main menu, select **Controller** and **Internal DHCP Server** (Figure 18).
2. Select **New** and enter a **Scope Name**. Click Apply to return to the previous menu.
3. Click on the **Scope Name** to configure the DHCP server.
4. Enter the Starting and Ending addresses for the address pool.
5. Enter the Network and the Netmask.
6. Set a Lease Time.
7. Set any other parameters as required according to your configuration.
8. Set Status to Enabled.
9. Click Apply to save all changes.



Configuration Note

Security Settings on Kimchi Phone

From the A Menu → Advanced → Admin Mode (Enter Admin Password) → Access Profile → Profile 1

Profile Name:	Enter any Profile Name (ex: WLAN1)
SSID:	802.1x (As set in the WLC)
WMM Mode:	ON
Power Save Mode:	ON
Security Type:	WPA2-802.1x or WPA-802.1x
Encryption Type:	AES (if Security type is WPA2-802.1x) or TKIP (if Security type is WPA-802.1x)
Encryption Key:	Leave it blank
WEP Key Index:	Not required for 802.1x
EAP Type:	(Any method as per your Radius Server configuration) e.g PEAP-MsCHAPv2...
EAP Identity:	kimchi (User created on your Active Directory/ Local user created in the Radius Server).
EAP Username:	kimchi (User created on your Active Directory/ Local user created in the Radius Server).
EAP Password:	kimchi123 (password specified for the above user in Active Directory or in the Radius Server).
Use DHCP:	ON/OFF (as per your network setup)

Note: For more information regarding WPA-802.1x/WPA2-802.1x Setup on Avaya 3631 Phone, Certificate generation and uploading the certificate on the phone, refer to the document from the link below:

http://support.avaya.com/elmodocs2/3600/Avaya_3631_Wireless_Security_Configuration_Guide.pdf



Configuration Note

Further Assistance

1. A Quick Start guide for the 4400 WLC can be found on Cisco's website:
<http://www.cisco.com/en/US/docs/wireless/controller/4400/quick/guide/ctrlv32.html>
 2. To convert the 1200 Series autonomous AP to an LWAPP, go to:
http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html
 3. For more information on the LWAPP-Enabled APs, see Quick Start Guide: Cisco Aironet 1000 Series Lightweight Access Points at:
http://www.cisco.com/en/US/docs/wireless/access_point/1000/quick/guide/ap1000qs.html
 4. For other assistance, contact Avaya's customer service at:
<http://support.avaya.com>
-