Cisco Unified Wireless Network Design Guide for Nokia Eseries Phones

The purpose of this document is to provide configuration assistance for the Cisco Unified Wireless Network (CUWN) products that support the Nokia Eseries phones. This is a WNBU Technical Marketing document to support the *Nokia Eseries Deployment Guide* provided by IPCBU Technical Marketing. The content includes Wi-Fi coverage design recommendations that are particular to 2.4-GHz radio performance characteristics of the Eseries phone. It also contains configuration examples and recommendations for the wireless LAN controllers (WLC) and the Wireless Control System (WCS).

You should review the *Voice over Wireless LAN Design Guide* and *Enterprise Mobility Design Guide* for comprehensive insight into deploying the Nokia Eseries as a Wi-Fi phone in an enterprise WLAN. Refer to the appendix for links to any documents referenced in this document.

This document primarily focuses on QoS, RF channel coverage, and RF channel capacity because without proper design of the first hop to the wired LAN and the last hop (the wireless shared media of Wi-Fi channels) from the wired LAN, call quality suffers, regardless of the design and configuration of the infrastructure.

The Nokia Eseries Wi-Fi enabled phones have the Wi-Fi Alliance certification for Wi-Fi Multimedia (WMM). The WMM certification is based on the IEEE 802.11e specifications which determine the quality of service (QoS) mechanisms used by packets sent between the Nokia phone and the Cisco access points. When correctly enabled on the client and WLC, the voice packets have priority access to the RF channel and have shorter transmit intervals on the RF channel over video and data packets. This certification is a very important feature in voice over wireless LAN (VoWLAN) support of call quality.

This document contains the following information:

- Designing the Wi-Fi Channel, page 2. The section includes design considerations for trouble spots like elevators.
- Configuring WLC for Access Point Radio and QoS Support, page 7. This section includes the settings for fast roaming and packet security.
- Using WCS Templates for Nokia Wi-Fi Connections, page 19. This section shows how WCS is used to estimate the VoWLAN coverage readiness and how it can audit the VoWLAN WLC configuration.
- Voice Readiness, Auditing, and Reporting, page 26. This section describes what reporting is available on WCS and gives steps for running the reports.
- Symmetric Mobility Tunneling, page 33. This section describes the new Layer 3 functionality for clients to roam seamlessly and maintain IP addressing and session state even across boundaries.

Designing the Wi-Fi Channel

Adding VoWLAN support to an existing WLAN requires a survey audit. When considering the addition of voice over the current WLAN, you must first determine the quality and coverage of the Wi-Fi channels. The items to evaluate include the following:

- required Data Rates
- Channel Capacity at peak periods of usage
- 802.11b/g VoWLAN on 802.11n
- Coverage and Roaming

Doing this evaluation reveals the existing RF conditions. These items must be addressed to produce quality calls. In most cases, moving from a data-only WLAN to a data-and-VoWLAN WLAN requires additional access points. If the same facility is considering the installation of a Wi-Fi based location services application, you should review access point placement documentation for the RFID. The RFID support design can be quite different from a data or voice design.

Channel design must be focused on the phones' signal strength at the access point. The recommendation for the coverage design is a –67 dBm RSSI value on the access point from the edge of the coverage area. In most cases, the data rate should be 11 Mb/s for 802.11b/g and 12 Mb/s for 802.11g. For a good quality link to support a client phone, the client must be heard by the access point. Client phones have limited transmit powers and antenna performance when compared to access points. The RF uplink from the client to the access point causes many quality issues; therefore, to determine if a channel design provides good quality calls, measure the signal of the phone as displayed on the access point when the phone is at the designed cell edge.

Data Rates

The throughput of a 2.4-GHz WLAN RF cell is influenced by the configured data rates. Beacons and other 802.11 management and control packets are transmitted at the lowest required or mandatory data rate. Packets at 1 or 2 Mb/s support first generation clients. In a dense access point deployment, these data rates cause high retry rates because the cell is larger than what the client easily supports from a transmit power perspective. In a dense access point deployment with data rates of 1 or 2 Mb/s, the coverage cell may contain too many clients. In most cases, today's 2.4-GHz client radios support data rates from 1 Mb/s to 54 Mb/s. The 1 Mb/s data rate provides the longest distance of coverage capable from that client radio. But in many locations, long distance coverage in the 2.4-GHz spectrum is not necessarily an advantage and may result in poor cell throughput.

The original 802.11 specification supported WLAN radio data rates of 1 Mb/s and 2 Mb/s. The modulation type (CCK) used for those data rates provides the largest distance coverage of any modulation type in an 802.11 specification to date. The highest data rates in the 802.11 specifications use the modulation type known as OFDM. The highest data rates have the smallest distance coverage. These two facts are instrumental in cell design. High data rates have the smallest coverage area but provide the highest throughput cells. Low data rates provide the largest coverage area but have the lowest throughput cells.

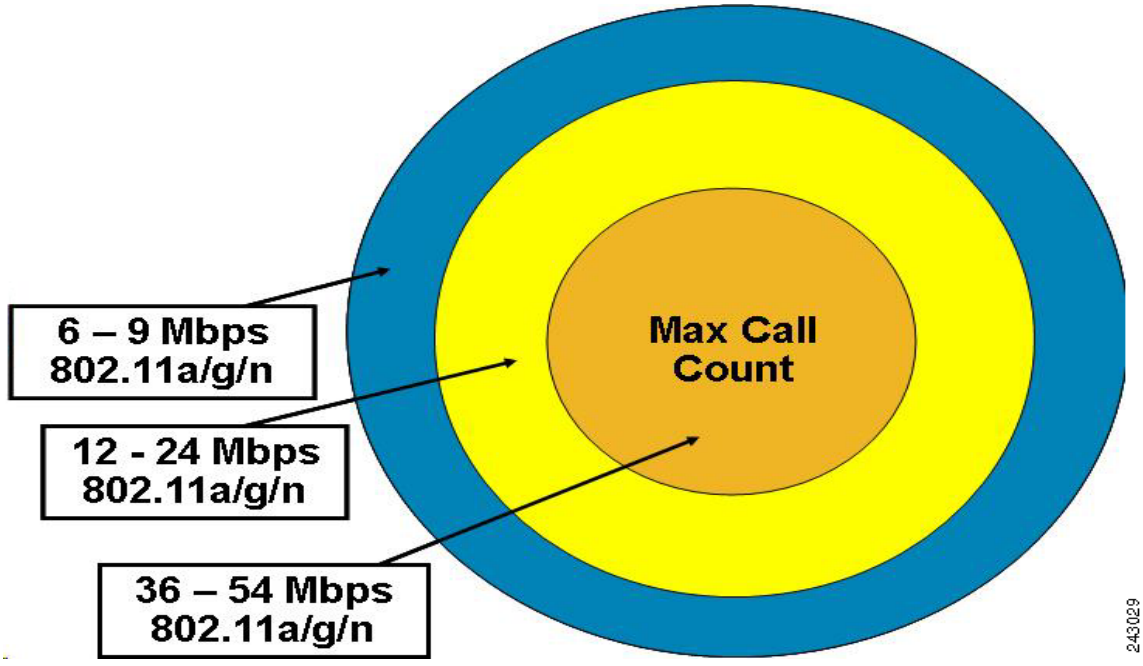
Another disadvantage of larger 2.4GHz cells is the increased size of the RF collision domain and lower signal-to-noise ratios (SNR). The larger the cell, the more RF level interaction between WLAN clients, but also Bluetooth, microwaves, and other RF interferers. Sites that have dense 2.4 GHz access points deployments have shown channel utilization numbers over 30% without any data or voice traffic. The bandwidth of the channel is consumed by 802.11 management and control traffic. When such sites have the data rates of 1 and 2 Mb/s removed, and only 5.5 and 11 Mb/s were required, the channel utilization dropped to 5%.

After determining which applications are used by non-phone clients and what data rates are required by those clients, you should remove as many low data rates as possible. A cell without data rates of 1 and 2 Mb/s per second is smaller, but it also has the lowest amount of interference, the highest throughput, and the most calls. A cell without 802.11b data rates of 1, 2, 5.5 and 11 Mb/s supports even more throughput and calls. The 802.11g data rate of 6 Mb/s and 12 Mb/s provides about the same cell coverage area as 802.11b when the transmit power is below 17 dBm. In deployments with a high density of access points, the transmit power in most cases is 15 dBm and lower. When 802.11 and 802.11b rates are disabled, the phones and access points no longer send clear-to-send management packets, and the number of calls in the cell can reach 14 instead of the 7 calls normally associated with 802.11b.

Channel Capacity

Figure 1 shows the data rates and relative cell sizes and which part of the cell achieves the highest number of calls. When an access point is configured with low data rates (such as 6 Mb/s and 9Mb/s), it effectively has a larger cell coverage area than an access point that has those rates disabled. More clients can be active with the access point because of the larger cell size. The larger cell will likely have a higher channel utilization and noise floor and therefore support fewer VoWLAN calls. A cell that supports the data rates of 6 through 54 Mb/s supports fewer calls than a cell that has only 36 to 54 Mb/s enabled. The packets of the clients in the 6Mb/s coverage area of the cell have longer air time than the packets sent at data rates of 12 to 24 Mb/s and longer than those packets sent at 36 to 54Mb/s. The graphic shows a cell with the combination of 54Mb/s and 6Mb/s clients. The 54Mb/s clients are slightly slower because of the lower transmission rates of the 6 Mb/s data rate clients.

Figure 1 Varying Data Rates and Cell Sizes



The data rates and cell sizes are part of the criteria for call planning. The original Cisco guidelines for call planning suggested seven calls per access point. That design logic is no longer valid. With the advent of 802.11e and WMM, the design criteria involves call streams per RF channel. An example of a call stream is a VoWLAN phone calling a wired desk phone. Two call streams would be two VoWLAN phones calling two wired desk phones or those two Nokia VoWLAN clients calling each other. If those

two phones that are calling each other are associated to the same access point, then those two call streams are in the same cell and on the same RF channel. The new call planning criteria is based on the number of call streams on the same RF channel. It is important to remember that RF channels can overlap. Two access points in near proximity of each other can be sharing the same RF channel; therefore, the number of quality call streams is related to the channel and not to the number of access points.

802.11b/g VoWLAN on 802.11n

The 2.4 GHz spectrum is used by four 802.11 specifications and four 802.11 modulation types. The specifications are 802.11, 802.11b, 802.11g, and 802.11n. The 802.11n specification also includes 5 GHz. The Wi-Fi alliance has decided to not include a certification for 40 Mhz wide channels on the 2.4 GHz spectrum. Cisco supports this view but current 802.11n Aironet access points are capable of 40 Mhz 2.4 GHz channels. The Nokia Eseries Wi-Fi phones have successfully been tested with Cisco Aironet 802.11n access points. The Nokia phones perform with equal call quality on 802.11n whether the access point is in 20 Mhz or 40 Mhz channel mode; therefore, running the access point in 40GHz mode has no call quality advantage.

The 802.11n specification, like the 802.11g specification, requires the use of CTS control packets if the access point is configured to support 802.11b. The data rates for 802.11n and 802.11g are maintained. The throughput of the cell is reduced because of the CTS protection mechanism. You should disable all 802.11b data rates if support for 802.11 is not required. With 802.11b disabled, the CTS protection mechanism is turned off. The 802.11g and 802.11n 2.4 GHz clients seamlessly interoperate with each other because they both use the OFDM modulation type.

The 802.11n carries expectations to improve cell throughput, capacity, and coverage. Although this is true, an 802.11b client is still an 802.11b client even when the client is associated to an 802.11n-enabled access point. The 802.11b client still has a maximum data rate of 11 Mb/s per second and a maximum throughput of about 7.1 Mb/s. The coverage is improved by the access points because of increased receiver sensitivity and increased transmit powers, but it is unlikely to improve more than 10% for 802.11b/g clients. In a noisy environment with high multipaths, the throughput is better because the MIMO antenna technology on the access point minimizes retries.

When Nokia phones were tested with Cisco Aironet 802.11g and 802.11n access points in the cell coverage area edge of the 802.11g access points, the average mean opinion score (MOS) value improved by half a point. The number of call streams increased by one call. Two additional call streams did reduce the average MOS value.

Coverage and Roaming

The proper coverage for voice suggests a 15 to 20 percent cell overlap. The WLAN data design guidelines do not require this level of overlap. The optimal VoWLAN cell boundary recommendation is –67 dBm, and the separation of cell is 19 dBm to provide quick roams at the RF median level. However, roam times and therefore call quality during roams are affected by the time it takes to re-authenticate the roaming phone that roamed to the access point. The new link to the roamed-to access point requires a new unique encryption key. To accomplish fast and secure roaming, Cisco recommends Cisco Centralized Key Management (CCKM) with TKIP encryption.

The Eseries configurations for EAP-based 802.1X security mode with CCKM support are as follows:

- CCKM with WEP —CCKM Key Management (EAP-based authentication) with dynamic WEP encryption
- CCKM with TKIP —CCKM Key Management (EAP-based authentication) with TKIP encryption

- NOT SUPPORTED!! CCKM with AES —CCKM Key Management (EAP-based authentication) with AES encryption

Follow these steps to configure CCKM on the WLC configuration.

Step 1 Choose **WLANs** and click an SSID.

Step 2 On the WLANs > Edit window, click the **Security** tab.

Step 3 In the Layer 2 Security tab, choose **WPA+WPA2** from the drop-down menu.

Step 4 Check the **WPA Policy** check box to enable.

Step 5 Check the **TKIP** check box to enable and leave the **AES** check box unchecked to disable. (These check boxes appear after you enable WPA Policy.)

Step 6 Ensure that the **WPA2 Policy** check box is unchecked.

Step 7 From the Auth Key Mgmt drop-down menu, choose **CCKM**.

The complete WLC configuration is shown in chapter 2. For more information see the *Cisco Wireless LAN Controller Configuration Guide*. The document link is in the appendix.

Roaming Coverage with Elevators

Elevators and elevator shafts are highly reflective of Wi-Fi signals. Reflected signals create multipath, which means multiple copies of the transmitted signal are traveling in slightly different paths and time. Multipath is likely to cause RF level retry rates of 20% to 50% for signals transmitted at higher data rates. The method used to improve call quality in high multipath areas is to disable the higher data rates and enable the lowest data rates. The lowest data rates have the best delay spread performance which in turn reduces the retries. However, this is a trade off because the throughput of the cell near the elevator is reduced (along with a reduction of multipath and retries) while the call's quality is improved. OFDM modulation is effective for multipath phenomenons, but increasing the delay spread best addresses the retry problems in high multipath areas. The lower the data rate the better the delay spread. Because simultaneous calls are unlikely in an elevator, dropping the call, and not bandwidth, is the issue. The undesirable side effect of enabling the low data rates and disabling the high data rates is the increased collision domain of nearby cells on the same channel. Also, RRM does not adjust data rates and is not multipath aware. Data rates are a global setting per controller.

No standard foolproof method ensures coverage in elevators since there are many variables to consider. As such, you should follow a series of recommendations and best practices until an approach that provides a satisfactory level of service is found for a set of wireless clients in a unique environment.

When the elevator is in motion, the wireless client is unpredictable as it reacts to the rapid crossing of cells. Roaming is the responsibility of the WLAN clients and not the access points or supporting infrastructure. As such, wireless client roaming behavior is strongly influenced by the roaming algorithm implemented in the wireless driver supplied by the vendor. You cannot expect stable connectivity in elevators because of the unique and differing environmental and wireless client characteristics.

One common technique to provide wireless coverage in elevators is to place a diversity omni antenna directly outside of the doors of the elevators. The antenna should be mounted below the ceiling tiles. For hospitals that are deploying new 2.4- and 5-GHz WLANs, the Cisco AIR-AP1131AG has been a popular choice because of its design and the integrated diversity antenna which radiates the signal in a downward direction. The AIR-AP1242AG is also another good choice when specific external antennas are required or when access point enclosures are required. When external antennas are used, the AIR-ANT5959 2.4 GHz and AIR-ANT5145-R for 5 GHz are recommended for mounting below the ceiling tiles. These antennas are colored to match ceiling tiles and provide low gain diversity omni-directional radiators.

Many wireless installations are using the 802.11n AIR-AP1250 which provides backward compatibility to 802.11a/b/g wireless clients while providing 802.11n and MIMO. The new MIMO antenna technology combined with the newer radios performs better than compared to non-MIMO technologies in areas with high multipath. Many areas of a hospital are prone to high levels of multipath interference due to the construction techniques as well as RF shielding in some areas of the building. Recommendations for MIMO-based ceiling mount antennas are the AIR-ANT2430V-R for 2.4 GHz and AIR-ANT5140V-R for 5 GHz.

In many cases, but dependent on elevator design, a closed elevator door reduces the signal inside by 7 to 10 dB or more. This necessitates that the access point and antenna are positioned just a few feet in front of the elevator doors. To provide fast secure roaming between floors, put the access points that service elevators on the same controller and ensure that they are part of the same access point group. The design of the WLANs mobility groups and access point groups is essential for mobility design. Use the links in the appendix for the *Cisco Wireless LAN Controller Configuration Guide* and the *Enterprise Mobility Design Guide*. Symmetric Mobility Tunneling is crucial to prevent a dropped call as the wireless phone rapidly associates between access points on different floors. Refer to the "Symmetric Mobility Tunneling" section on page 33. Symmetric Mobility is not enabled by default and must be enabled for Layer 3 mobility.

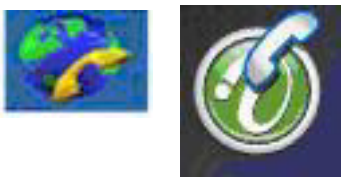
Note With 5.1, Symmetric Mobility Tunneling is enabled by default. When you upgrade from 5.0 or previous versions, the 5.1 code still continues with the configuration of the previous version; therefore, verify the Symmetric Mobility Tunneling setting after you upgrade to 5.0.

Configuring WLC for Access Point Radio and QoS Support

This section describes how to configure WLC for Nokia Eseries WMM certified phones.

The phones supported by this controller configuration are the Eseries running the Nokia Intellisync Internet telephone program. When that application is installed, one of the following icons appears on the menu (see Figure 2).

Figure 2 Intellisync Icons



VoWLAN calls with clients that are WMM certified and associated to an SSID (which is configured to support the WMM specification) have QoS priority over the air. The WMM specification defines eight user priorities and four access categories, each defined by 802.11e.

The 802.11e Enhanced Distributed Channel Access (EDCA) mechanism uses 802.1d user priority (DiffServ tags) to classify the traffic categories as follows:

- Voice: Priority 7 or 6 for toll-quality VoWLAN calls requiring low latency
- Video: Priority 5 or 4 for SDTV or HDTV video streams
- Best Effort: Priority 3 or 0 for latency-insensitive, interactive applications
- Background: Priority 2 or 1 for batch data transfer applications

In the 802.11e specification, traffic for clients not using WMM is referred to as a non-QoS station and is classified as best effort.

Clients that are incapable of using WMM QoS to the access points (because of firmware or driver limitations) can be assigned SSIDs that have a voice access category. The performance of the cell is enhanced when the client is configured to associate to an access point QoS SSID. The traffic or packet sent from the access point to the client fall into one of four access categories marked with one of eight user priorities. Refer to Figure 43 in the appendix for the marking of a voice packet transitioning from the phone to the WLAPP controller and back.

Using the WLAN GUI

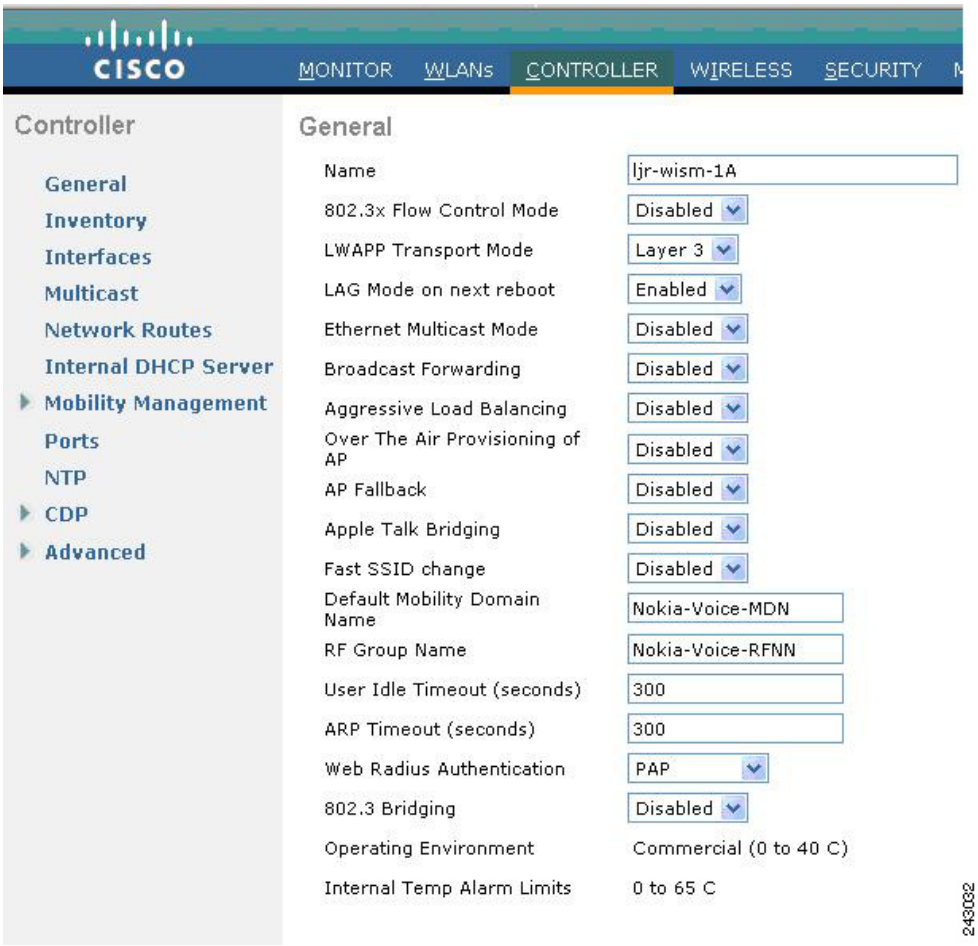
Follow these steps to open the Controller Summary page.

Step 1 Browse to the WLAN controller using your Management Interface address (beginning with https://).

Step 2 When the Security Alert window appears, choose **Yes**. The Login screen appears.

Step 3 Click **Login** to access the controller. The main menu is displayed (see Figure 3).

Figure 3 WLC Main Menu



Step 4 Ensure that LWAPP Transport Mode is set to Layer 3.

Note On software release 5.0 or later, this step is not necessary. The LWAPP Transport Mode parameter is removed because the controllers can only operate in Layer 3.

Step 5 Ensure that Aggressive Load Balancing is disabled.

Note This option is required for any clients that maintain their own access point neighbor lists (which Nokia does).

Step 6 Click **Apply**.

Step 7 Choose **WLANs**.

Step 8 Choose a WLAN from the Profile Name column.

Step 9 Choose the **Advanced** tab.

Step 10 Ensure that P2P Blocking Action is set to Disabled.

Note Phones that are associated to the same access point can then call each other.

Step 11 Click **Apply**.

Creating a Voice Interface

Follow these steps to create a voice interface.

Step 1 From the WLC Main Menu (shown in Figure 3), click **Interfaces** in the left sidebar menu. The VLAN Identifier and IP Address should match your network.

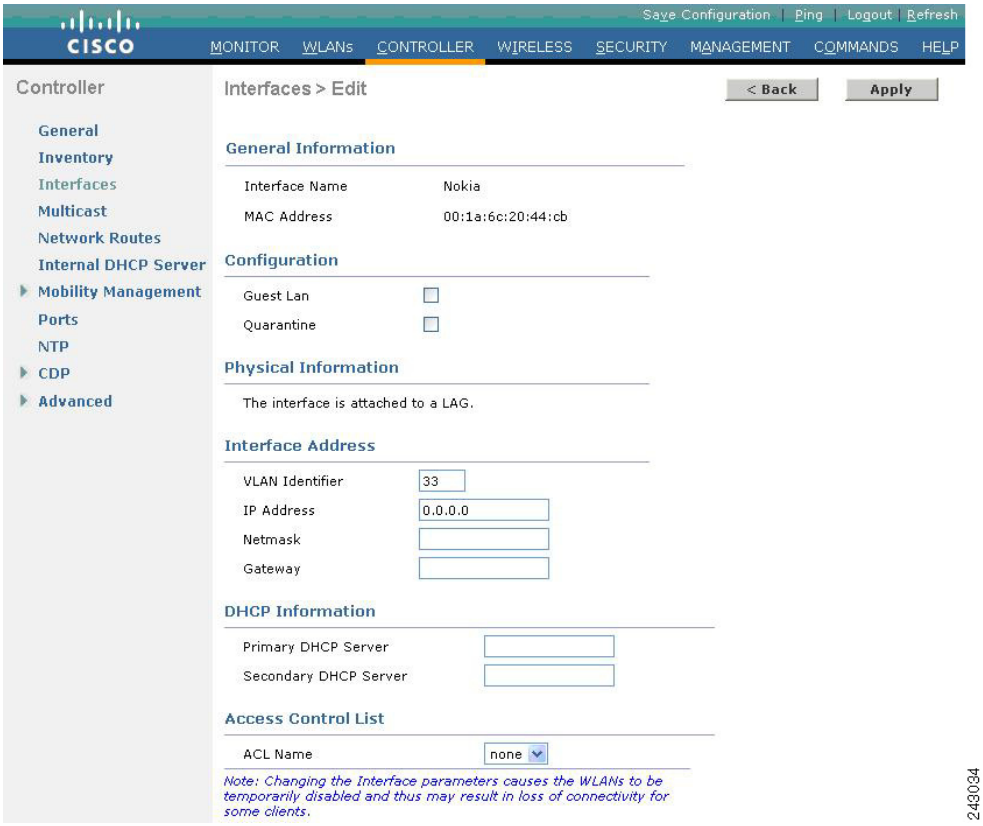
Step 2 Click **New**. The Interfaces window appears (see Figure 4).

Figure 4 Interfaces > New

Step 3 Enter a voice interface name and VLAN ID.

Step 4 Click **Apply**. The Interfaces > Edit window appears (see Figure 5).

Figure 5 Interfaces > Edit



Step 5 Enter the IP Address, Netmask, and Gateway for the voice interface port uplink of the controller.

Step 6 Enter the DHCP server information if required by infrastructure design.

Step 7 Click **Apply**.

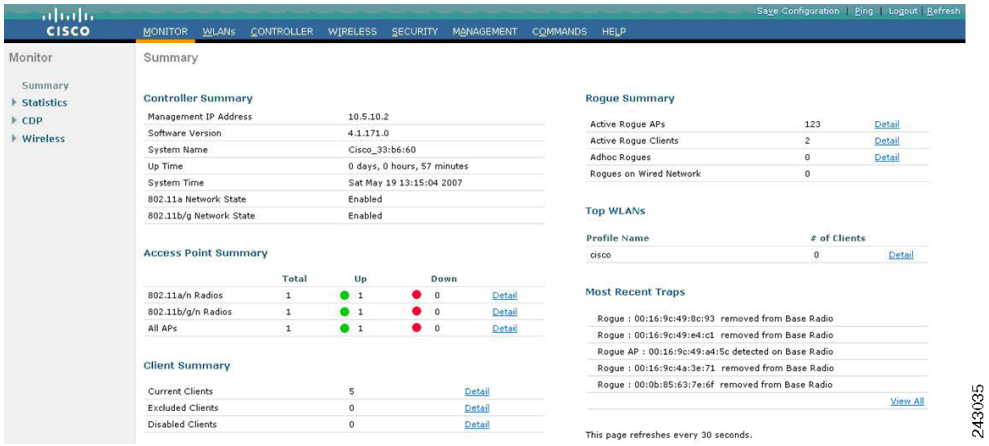
Configuring the 802.11b/g Radio

Follow these steps to configure the 802.11b/g radio.

Step 1 Choose **Monitor > Summary**.

Step 2 In the Access Point Summary section, click the **Detail** link in the 802.11b/g/n Radios row. The 802.11b/g/n Radios window appears (see Figure 6).

Figure 6 802.11b/g/n Radios



Step 3 Choose **Configure** (as shown in Figure 6). The 802.11b/g/n Cisco APs > Configure window appears (see Figure 7).

Figure 7 802.11b/g/n Cisco APs > Configure

Step 4 Ensure that Admin Status is set to **Enable**.

Step 5 Choose the Antenna Type.

Step 6 Ensure that Diversity is set to **Enabled**.

Step 7 In the RF Channel Assignment section of the window, choose **Custom** as the Assignment Method if the site survey design requires it.

Step 8 From the drop-down menu, choose a non-overlapping RF channel.

Note Only Channels 1, 6, and 11 are non-overlapping.

Step 9 In the Tx Power Level Assignment section of the window, choose **Custom** as the Assignment Method if the site survey design requires it.

Configuring the 802.11b/g Global Parameters

Follow these steps to configure the 802.11b/g global parameters.

Step 1 Choose **Wireless**.

Step 2 From the left sidebar menu, choose **802.11b/g/n > Network**.

Step 3 Ensure that Short Preamble and DTPC Support are enabled. This is supported by the Eseries phones.

Step 4 Click the **Enabled** check box under CCX Location Measurement.

Note Leave the Interval parameter at the default value.

Step 5 Choose the data rate that matches the coverage design. The options are as follows for the varying Mb/s (1, 2, 5.5, and 11 Mb/s):

- Disabled
- Supported—Any associated client supporting the same rate may communicate with the access point using this rate.
- Mandatory—Clients that do not support the rate specified cannot associate.

Note The client is not required to use the rates marked *Supported* to associate.

Note Before starting the site survey or WCS voice readiness test, you should disable the 1 and 2 Mb/s data rates on sites with dense access point placements. Only a limited number of legacy client cards and devices still use these original 802.11 specifications. When you disable these rates, channel utilization is significantly improved, and the collision domain is significantly reduced. For the Eseries phones, the data rates of 1, 2, and 5.5 are probably not necessary.

Step 6 Click **Apply**.

Note For WLC software release 4.0.206 to 4.2.x, you should disable network arpunicast. Use the **show network summary** CLI command and see how the ARP Unicast Mode parameter is set. If it is not already set to Disabled, run **config network arpunicast disable**.

Setting Call Admission Control on 802.11b/g

If your Nokia phone supports call admission control (CAC), Cisco recommends the following setup.

Note As of March 2008, no Nokia phones support CAC.

Step 1 Choose **Wireless**.

Step 2 From the left sidebar menu, choose **802.11b/g/n** and then **Network**.

Step 3 Ensure that the 802.11b/g/n Network Status is unchecked (disabled).

Step 4 Click **Apply**.

Step 5 Click **Voice** in the left sidebar menu under 802.11b/g/n. The 802.11b > Voice Parameters window appears (see Figure 8).

Figure 8 802.11b > Voice Parameters

Step 6 Check the **Enabled** check box to enable Admission Control.

Step 7 Set the Load-based AC to enabled.

Step 8 Leave the RF bandwidth percentage at the default.

Step 9 Leave the reserved roaming bandwidth percentage at the default.

Step 10 Click the check box to enable metrics collection.

Step 11 Click **Apply**.

Step 12 From the left sidebar menu, choose **802.11b/g/n** and then **Network**.

Note The RF bandwidth and roaming bandwidth percentage can be changed from the default to reflect the application requirements of a customer site.

Step 13 Check the 802.11b/g/n Network Status check box to enable the radio.

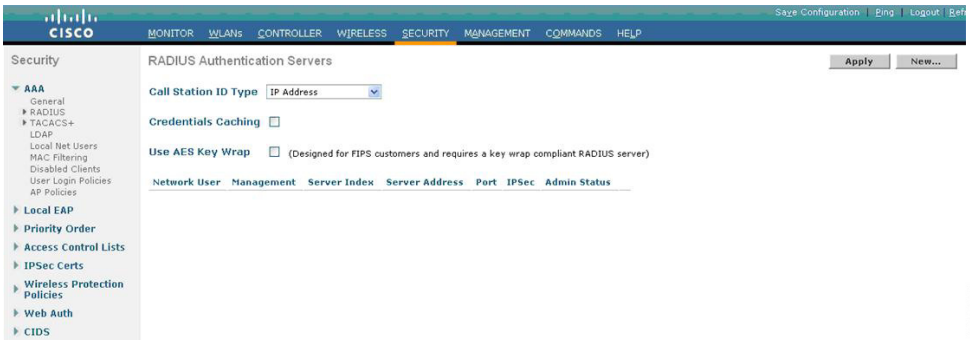
Configuring RADIUS Server Credential Caching

Follow these steps to configure RADIUS server credential caching.

Step 1 Choose **Security**.

Step 2 From the left sidebar menu, choose **RADIUS > Authentication**. The RADIUS Authentication Servers window appears (see Figure 9).

Figure 9 RADIUS Authentication Servers



Step 3 Click the check box to enable Credential Caching.

Note Credential caching may not be an option if you have software release 4.2 or later.

Step 4 Click **Apply**.

Creating a WLAN for Nokia Phones

Follow these steps to create an interface that defines the SSID, VLAN, authentication type, and QoS parameters for the VoWLAN client.

Step 1 Choose **WLANs**.

Step 2 Click **New**. The WLANs > New window appears.

Step 3 Enter a profile name, such as voice2.

Step 4 Enter a WLAN SSID, such as voice.

Note Because the profile name and SSID are user defined, they need not match.

Step 5 Click **Apply**.

Step 6 To further configure the voice interface for secure fast roaming, choose the **General** tab.

Step 7 Click the check box to enable WLAN Status.

Step 8 Change the Radio Policy parameter from *All* if a 5-GHz radio is not used for this voice interface.

Step 9 Use the Interface drop-down menu to select the profile name you created in Step 3.

Step 10 If you want the SSID broadcasted, leave the Broadcast SSID parameter set to Enabled.

Step 11 Click **Apply**.

Step 12 Click the **Security** tab. The Layer 2, Layer 3, and AAA Servers tabs appear (see Figure 10).

Figure 10 Security Tab

Step 13 At the Layer 2 Security drop-down menu, choose **WPA+WPA2**.

Step 14 Ensure that the WPA2 Policy check box is unchecked.

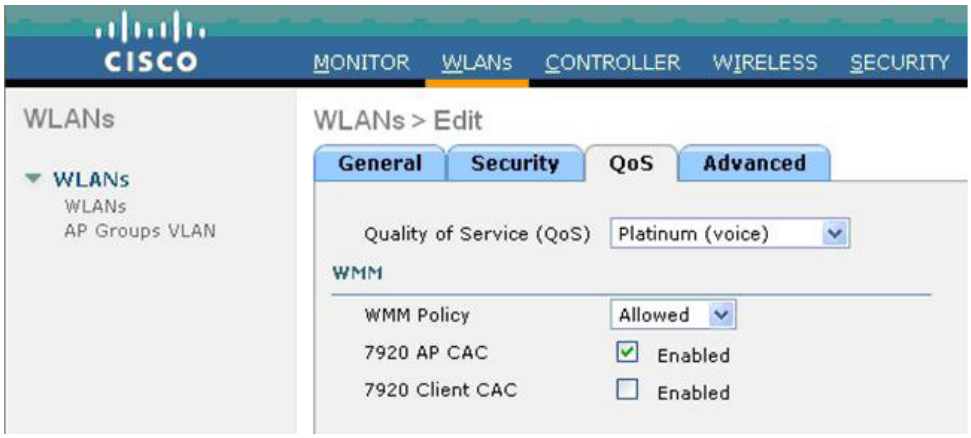
Step 15 At the WPA2 Encryption parameter, unselect **AES** and select **TKIP**.

Step 16 At the Auth Key Mgmt drop-down menu, choose **802.1X+CCKM**.

Step 17 Click **Apply**.

Step 18 Click the **QoS** tab (see Figure 11).

Figure 11 QoS Tab



Step 19 At the Quality of Service (QoS) drop-down menu, choose **Platinum (voice)**.

Step 20 At the WMM Policy drop-down menu, choose **Allowed**.

Note The *allowed* option means WMM and non-WMM clients can share the same WLAN. If only WMM clients are allowed, choose **Required** from the drop-down menu.

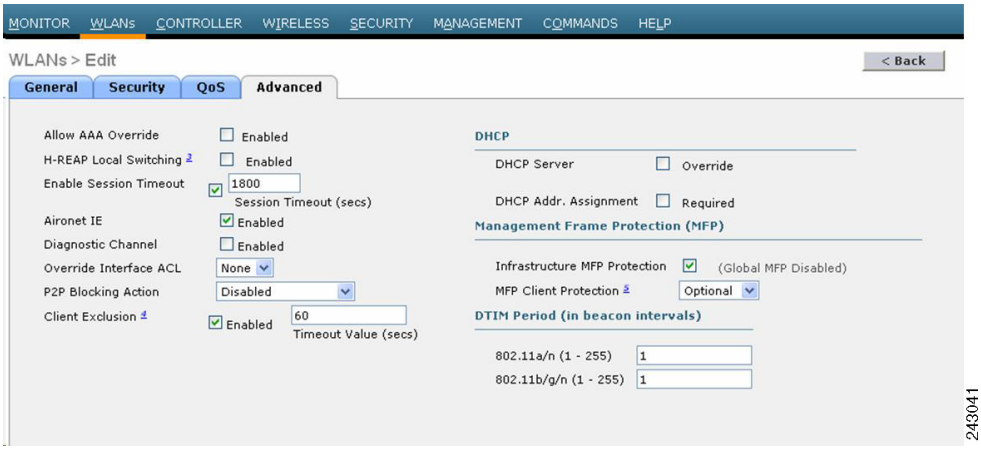
Step 21 Click the check box to enable 7920 AP CAC.

Note This is required only if WMM is allowed and other clients are using Cisco legacy QBSS.

Step 22 Click **Apply**.

Step 23 Click the **Advanced** tab (see Figure 12).

Figure 12 Advanced Tab



Step 24 The values on this tab can remain at the default unless the overall WLAN design requires changes.

Step 25 Click **Apply**.

Step 26 Click the **General** tab.

Step 27 Click the Status check box to enable it.

Step 28 Click **Apply**.

Step 29 Click **Wireless**.

Step 30 Click **QoS > Profiles** from the left sidebar menu.

Step 31 Click the **Platinum** profile name.

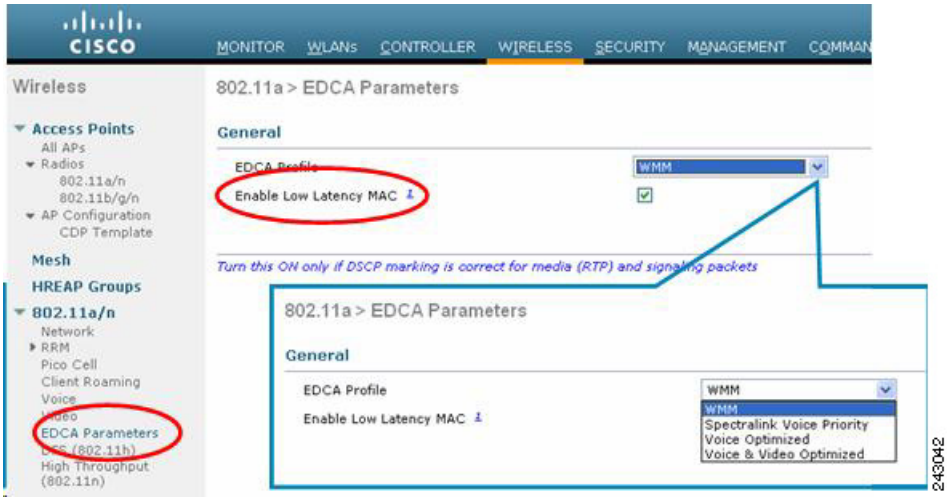
Step 32 At the Wired QoS Protocol Type drop-down menu, choose **802.1p**.

Step 33 At the 802.1p Tag parameter that appears, enter **6**.

Step 34 Click **Apply**.

Step 35 From the left sidebar menu, choose **802.11b/g/n > EDCA Parameters**.

Figure 13 EDCA Parameters



Step 36 From the EDCA Profile drop-down menu, choose **WMM**.

Step 37 Click **Apply**.

Monitoring WLC Voice Statistics

Follow these steps to monitor WLC voice statistics.

Step 1 Click **Monitor**.

Step 2 From the left sidebar menu, choose **Clients**.

Step 3 Choose **802.11b TSM** for Nokia. Click **Detail**. The Clients Detail window appears.

Figure 14 Client Details

Step 4 Click a link in the Client MAC Addr column to see the details of a Nokia phone. The CCX version number is displayed on the first page.

The Client Detail window appears and shows the phone RSSI value (see Figure 15). The RSSI value represents how well the access point hears the phone. If the value is on the high end (around –35 dBm), the phone is very near an access point. A value such as –67 dBm is near the cell edge.

Figure 15 Client Details Client MAC Addr

The window example in Figure 15 shows the client is associated to an access point configured with an 802.1 tag value of 6. The U-APSD value of 15 in Figure 15 indicates that the client is misconfigured and is using a WMM setting for video.

Step 5 Ensure that the U-APSD value is 7 for voice.

Using WCS Templates for Nokia Wi-Fi Connections

WCS is a Cisco Unified Wireless Network tool for management of the wireless LANs. WCS configures WLCs, monitors the RF channels, and reports the performance of the network. Templates are stored on the WCS, edited and maintained on the WCS, and then distributed to the controller(s). The templates are used to audit the configuration of a WLC.

This chapter provides recommendations for a Nokia WLC configuration and the steps to create the WCS templates for those recommendations. The complete configuration is not given, but the recommended settings to best configure the WLC for quality calls with a Nokia Eseries phone is provided. Refer to the *Cisco Wireless Control System Configuration Guide* for further information. The link to this guide is in the appendix.

Creating a Template for Nokia Phones

Follow these steps to create a template for Nokia phones:

Step 1 Log into WCS.

Step 2 Choose **Configure > Controller Templates**.

Step 3 Choose **Add Template** from the Select a command drop-down menu and click **GO** (see Figure 16).

Figure 16 Adding a Controller Template

Step 4 At the Template Name parameter, enter a descriptive name and purpose for the Nokia device.

Step 5 Use the Symmetric Tunneling Mode drop-down menu to choose **Enable** if the LWAPP transport mode is Layer 3.

Step 6 Enter a descriptive Default Mobility Domain Name.

Step 7 Enter an RF Network Name.

Step 8 Update other fields as necessary.

Step 9 Click **Save**.

Creating a QoS Template for the Nokia Phone

Follow these steps to create a QoS Profile for voice support on a Nokia phone.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **System > QoS Profiles**.

Step 3 Click the **Platinum (Voice)** option. The Edit QoS Profile Template appears (see Figure 17),

Figure 17 Edit QoS Profile Template Window

Step 4 From the Protocol drop-down menu, choose **802.1P**.

Step 5 Enter **6** at the 802.1P Tag parameter.

Step 6 Click **Save**.

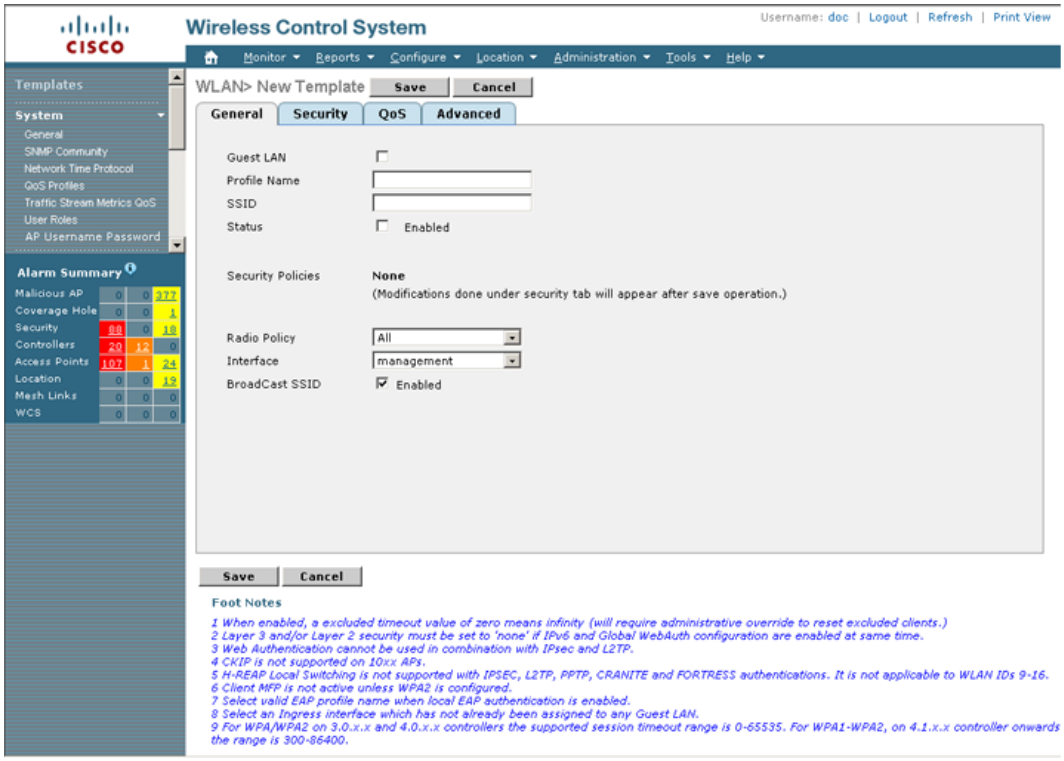
Step 7 From the left sidebar menu, choose **Traffic Stream Metrics QoS** to set up the traffic stream reporting.

Step 8 Click **Save**.

Step 9 Choose **WLANs > WLAN**.

Step 10 From the Select a command drop-down menu, choose **Add Template** and click **GO.** The WLAN > New Template window appears (see Figure 18).

Figure 18 WLAN > New Template Window



Step 11 Enter the profile name for the Nokia phone.

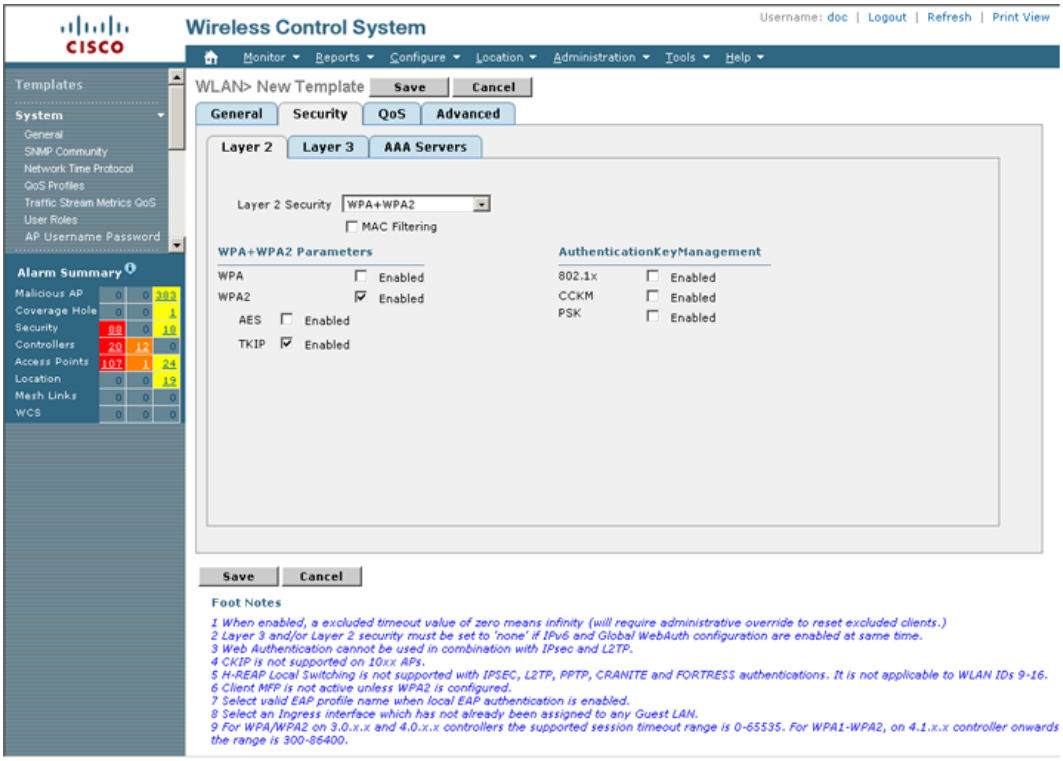
Step 12 Enter the SSID for the Nokia phone WLAN.

Step 13 Use the Interface drop-down menu to choose the name created for the Nokia phone.

Step 14 Click **Save**.

Step 15 Click the **Security** tab. The three Security template tabs appear (see Figure 19)

Figure 19 Security Template Tab



Step 16 On the Layer 2 tab, choose **WPA+WPA2**.

Step 17 Click the **WPA2** check box to enable it.

Step 18 Click the **TKIP** check box to enable it.

Step 19 In the Authentication Key Management section, click to enable **802.1x** and **CCKM**.

Step 20 Click **Save**.

Step 21 Click the **AAA Servers** tab.

Step 22 Set the AAA servers as needed.

Step 23 Click **Save**.

Step 24 Click the **QoS** tab and update if needed.

Step 25 Click the **Advanced** tab and update if needed.

The new Nokia template should be similar to the WLAN template shown in Figure 20.

Figure 20 WLAN Template Window

Creating a Template for an 802.11b/g/n Radio

The Nokia Eseries phones have 802.11b/g radios. A 2.4-GHz network is recommended. If the site does not have a requirement to support 802.11b, a configuration that does not include 802.11b data rates is recommended. The lower data rates reduce call capacity and call quality on the RF channel.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **802.11b/g/n > Parameters**.

Step 3 From the Select a command drop-down menu, choose **Add Template** and click **GO**. The 802.11b/g Parameters > New Template window appears (see Figure 21).

Step 4 Set the 1, 2, 5.5, and 11 Mb/s data rates to **Disabled**.

Step 5 Enter a policy name, such as Nokia 11G only.

Step 6 Click the check box to enable 802.11b/g network status.

Step 7 Click the check box to enable short preamble.

Step 8 Click the check box to enable dynamic Tx power control.

Step 9 Click **Save**.

Step 10 Choose **802.11b/g/n > Voice Parameters** from the left sidebar menu.

Step 11 From the Select a command drop-down menu, choose **Add Template** and click **GO**.

Step 12 Enter a descriptive template name.

Step 13 Click the **Enable Expedited Bandwidth** check box.

Step 14 Click **Save**.

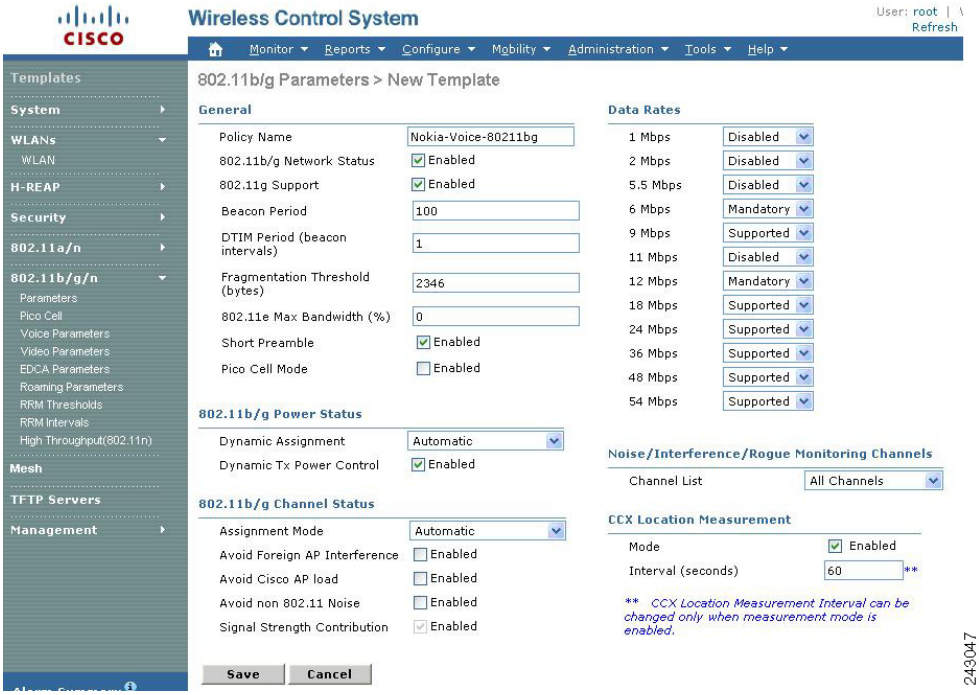
Note Current Nokia phone code versions do not use CAC or upstream traffic metrics.

Step 15 Choose **802.11b/g/n > EDCA Parameters** from the left sidebar menu.

Step 16 From the Select a command drop-down menu, choose **Add Template** and click **GO**.

Step 17 Enter a descriptive template name.

Figure 21 Disable Data Rates



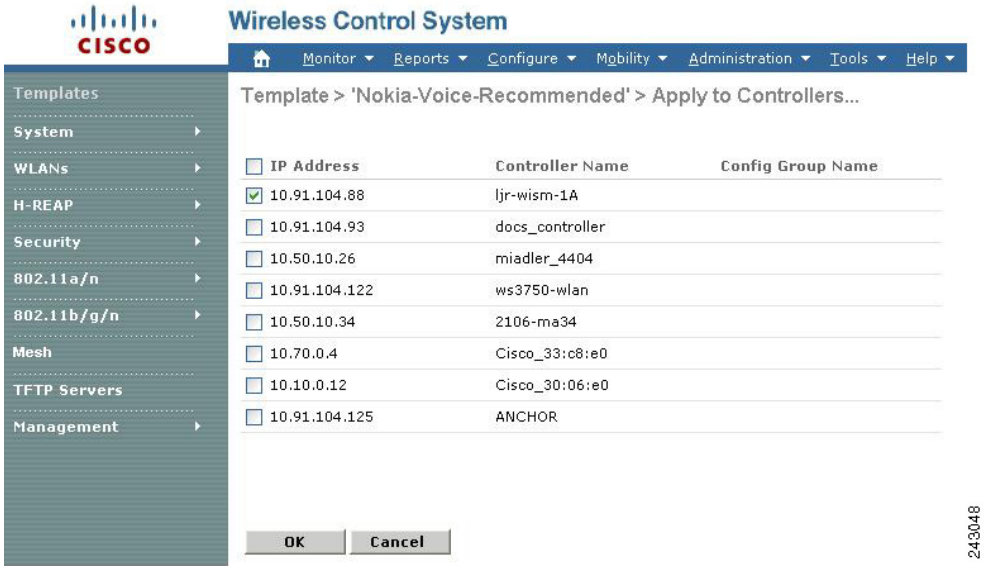
Step 18 From the EDCA Profile drop-down menu, choose **WMM**.

Step 19 Click **Save**.

Step 20 After the templates have been saved, choose them from the Template Name list and click **Apply to Controllers**.

Step 21 Choose the IP address to which you want the template applied (see Figure 22).

Figure 22 Applying Template to Controllers



Step 22 Click **OK**.

Voice Readiness, Auditing, and Reporting

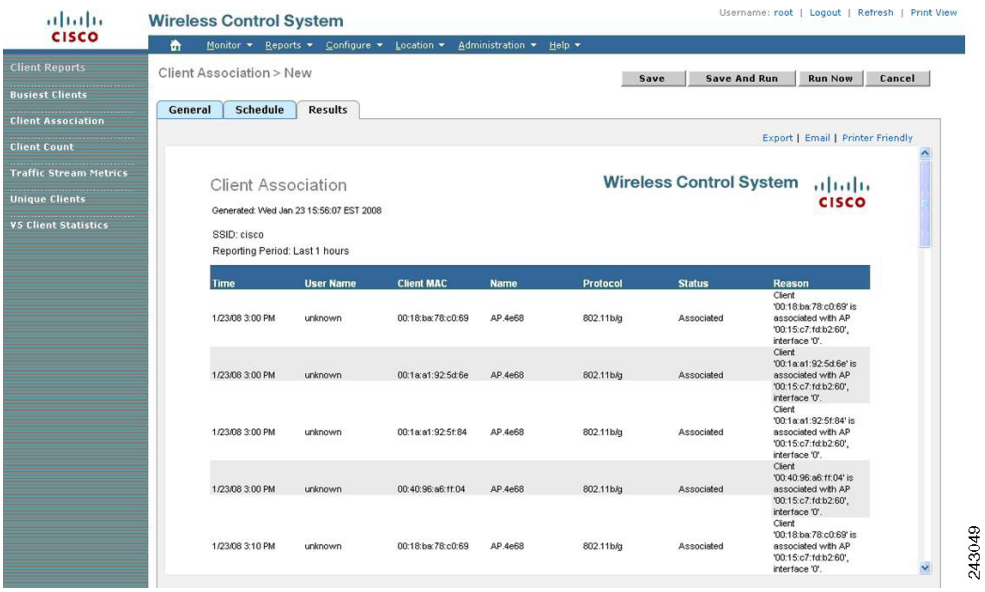
This section describes the reporting that is available on WCS and includes actual steps to run the reports. A planning tool helps determine the number of access points for a given floor space. It does a path loss calculation to graphically present the estimated coverage of the access points. Another WCS feature is a report of voice statistics and radio frequency channel utilization. WCS can run an audit across all of the controllers to ensure that they are properly configured for voice. You can export many of the generated statistical reports as a CSV file or as email.

Voice Statistics

You can generate several voice statistics reports.

- Choose **Reports > Clients > Client Association** to generate a report on clients associated to a voice WLAN (see Figure 23).

Figure 23 Client Association Report



- Choose **Reports > Performance Reports** to generate a report on radio utilization, transmit power and channel, or voice statistics (see Figure 24).

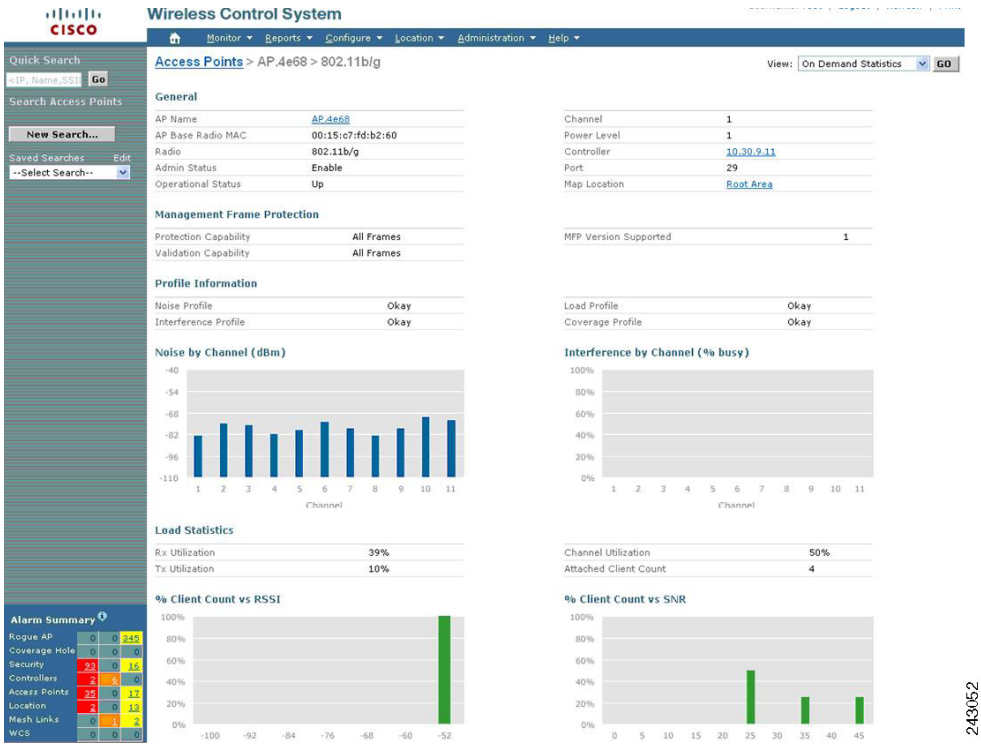
Figure 24 Traffic Stream Metrics (graphical) Report

The voice statistics report shows only the metrics of voice packets going from the access point to the Nokia client. The Nokia client is not providing uplink metrics (see Figure 25).

Figure 25 Voice Statistics Report

The Radio Utilization report shows any radio channel issues (see Figure 26).

Figure 26 Radio Utilization Report



- Choose **Report > Client > Traffic Stream Metrics** for a graphical report that shows the packet loss at an access point (see Figure 27). A traffic stream metrics report can also be in table format and provide red or green ratings of the call quality (see Figure 28).

Figure 27 Packet Loss Graphic Format

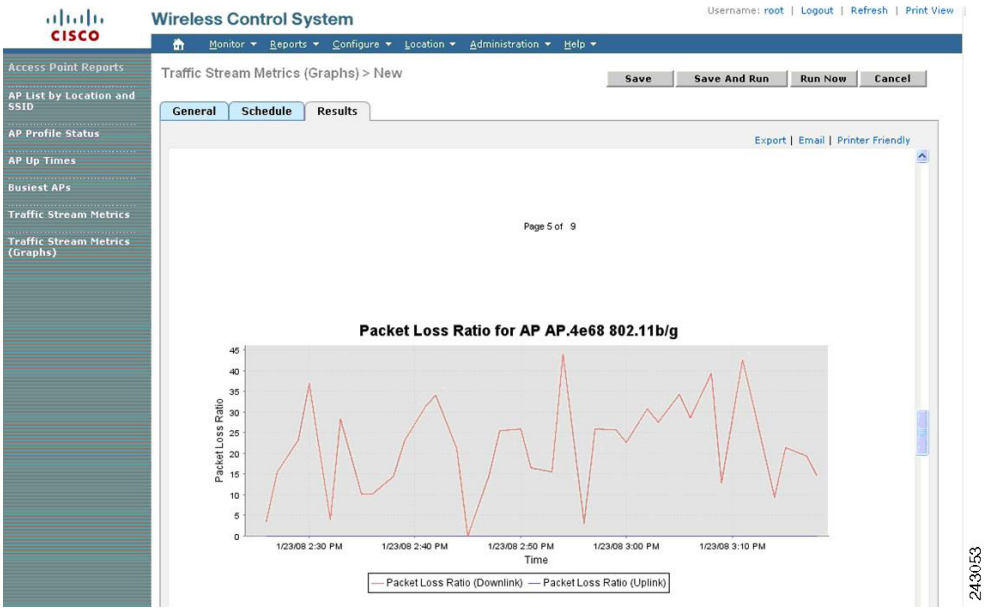
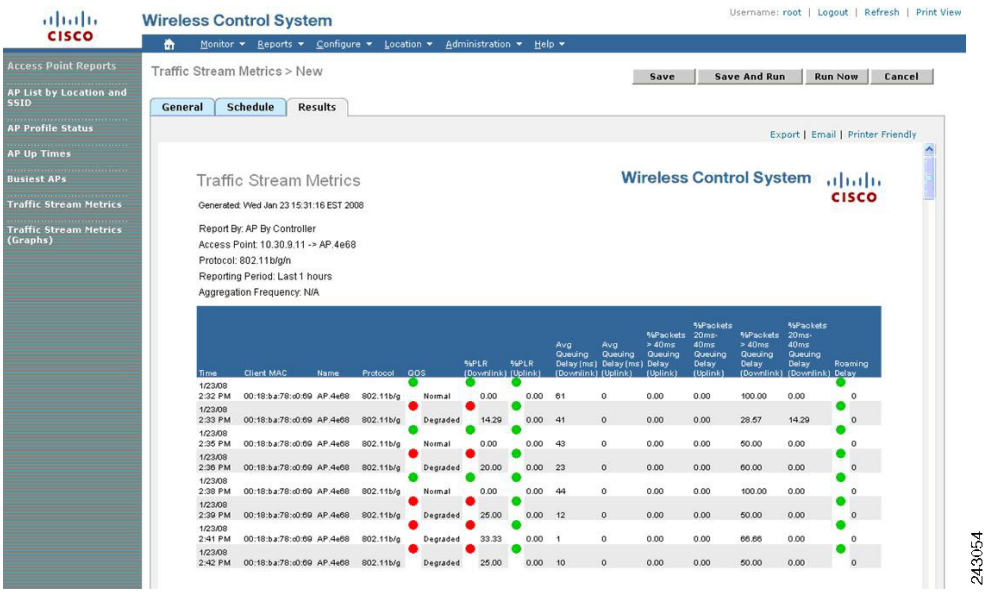


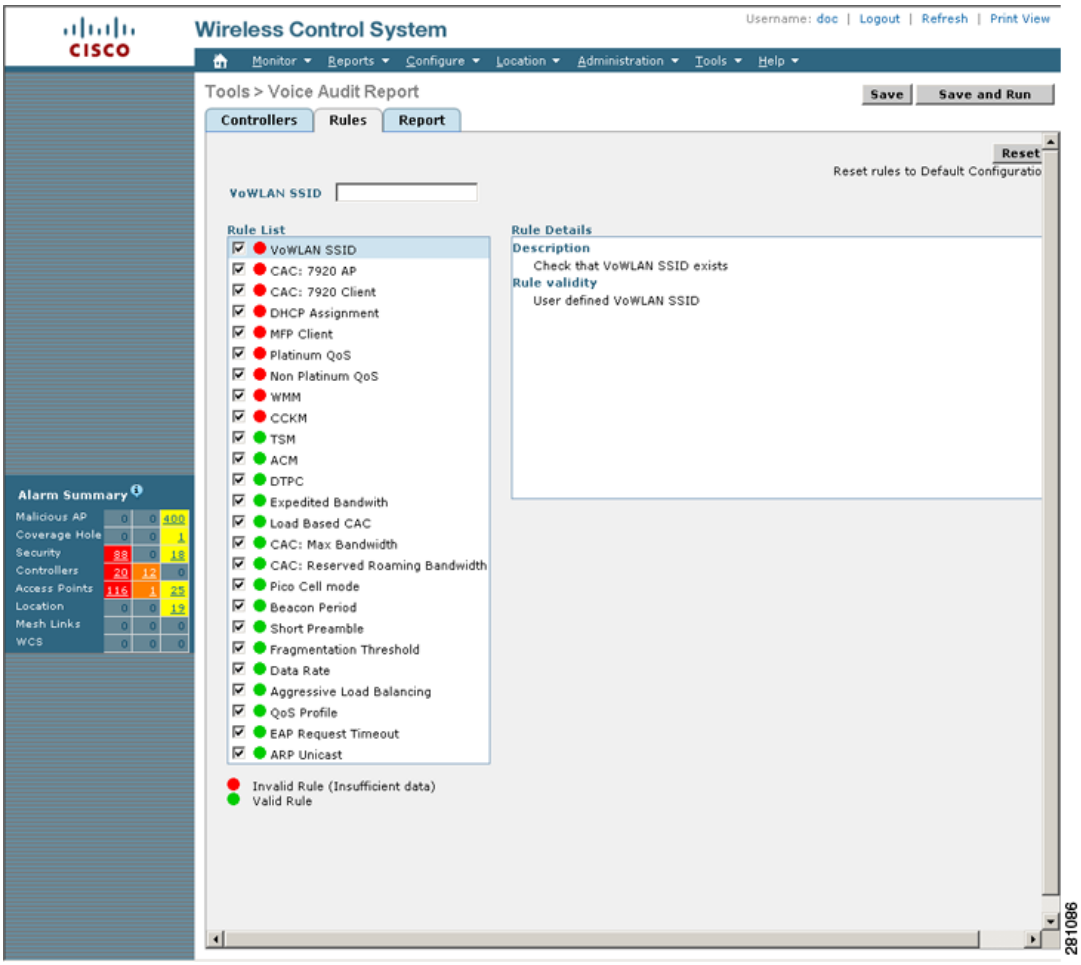
Figure 28 Packet Loss Table Format



Voice Configuration Audit

Under Tools, you can choose **Voice Audit**. This report compares the configurations of the controllers to each other. It verifies voice readiness and alerts you as to which parameters are not set for the best quality performance. The rules and reporting are configurable (see Figure 29).

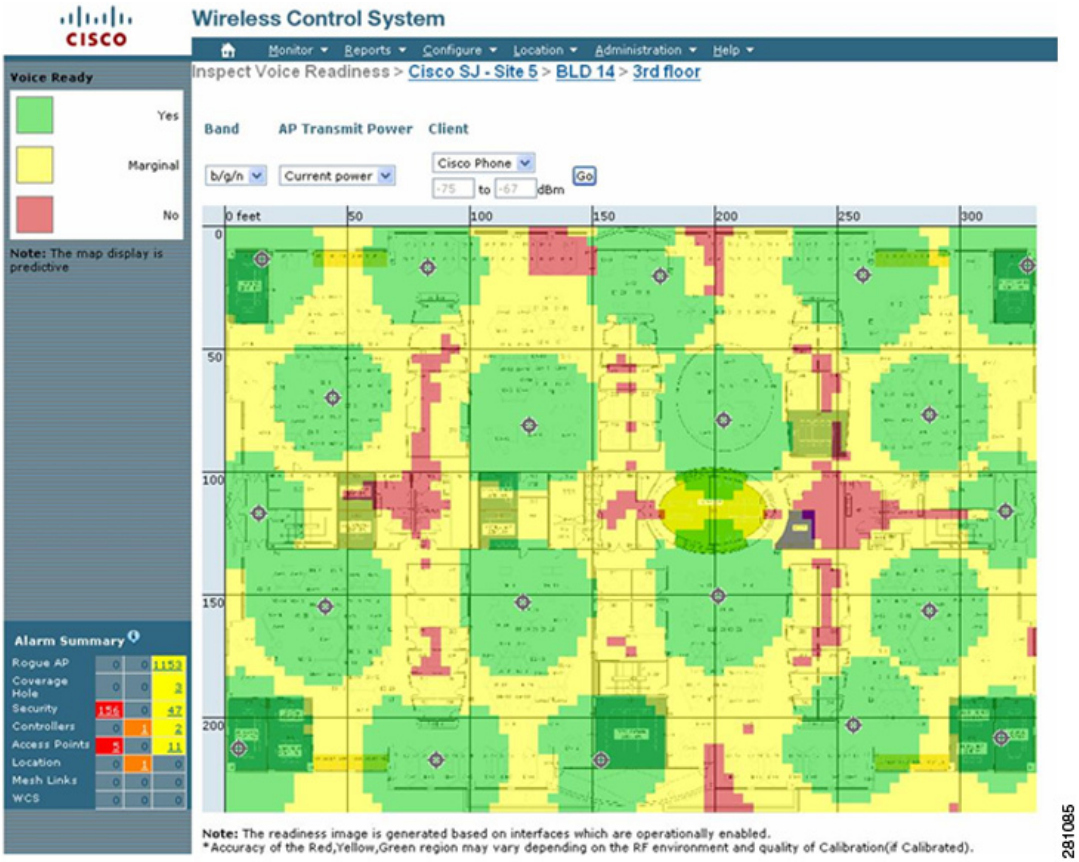
Figure 29 Rules and Reports for Voice Audit



Voice Coverage Readiness

The readiness tool uses an imported floor plan to determine whether the current configuration is suitable for supporting VoWLAN based on signal propagation between access points (see Figure 30). The default uses the Cisco 802.11b/g phone as the client device for coverage simulation. For the current Nokia 802.11b/g Eseries phone, the *Cisco Phone* client type is recommended. The transmit power for most sites should be 16 dBm or less.

Figure 30 Readiness Tool



Symmetric Mobility Tunneling

Cisco Wireless LAN Controllers enable users to roam transparently across all access points in the network. Clients roam seamlessly and maintain IP addressing and session state, even where controllers reside across routed boundaries from one another.

This Layer 3 mobility functionality was designed to deliver traffic with as little added latency as possible and with the capability to roam across wireless networks of all scales without altering the wired network configuration. Controllers can be placed anywhere in the network, and as clients roam from access point to access point across these controllers, clients remain connected, IP addresses remain unchanged, and session state is preserved.

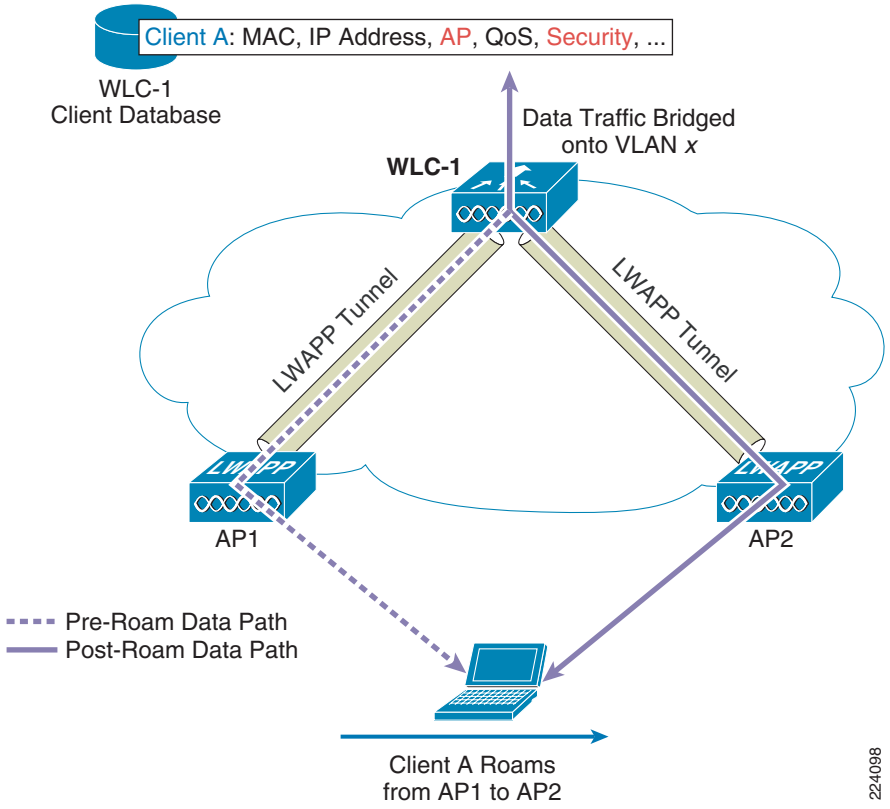
This seamless Layer 3 mobility capability was achieved within Cisco's Unified Wireless Network architecture with an asymmetric traffic pattern, whereby a roamed client's egress traffic terminates on the new, foreign subnet (sourced from its original IP address). The client's ingress traffic is routed according to the original IP address that is maintained, which means that it arrives at its original anchor controller, is then tunneled to the new foreign controller, and then delivered to the roamed client.

This Layer 3 mobility operation works flawlessly in most environments. In networks where traffic is not allowed to be sourced on non-native subnets, asymmetric mobility tunneling between controllers does not function. The RPF checks and firewall rules prevent the operation. Cisco's new Symmetric Mobility Tunneling feature is designed to correct this problem.

Background on Mobility in Cisco's Unified Wireless Network

When a wireless client associates and authenticates to an access point, the access point's joined WLC places an entry for that client in its client database. This entry includes the client's MAC and IP addresses, security context and associations, QoS context, WLAN, and associated access point. The WLC uses this information to forward frames to and receive them from the wireless client. Figure 31 depicts what happens when the wireless client roams from one access point to another if both access points are joined to the same WLC.

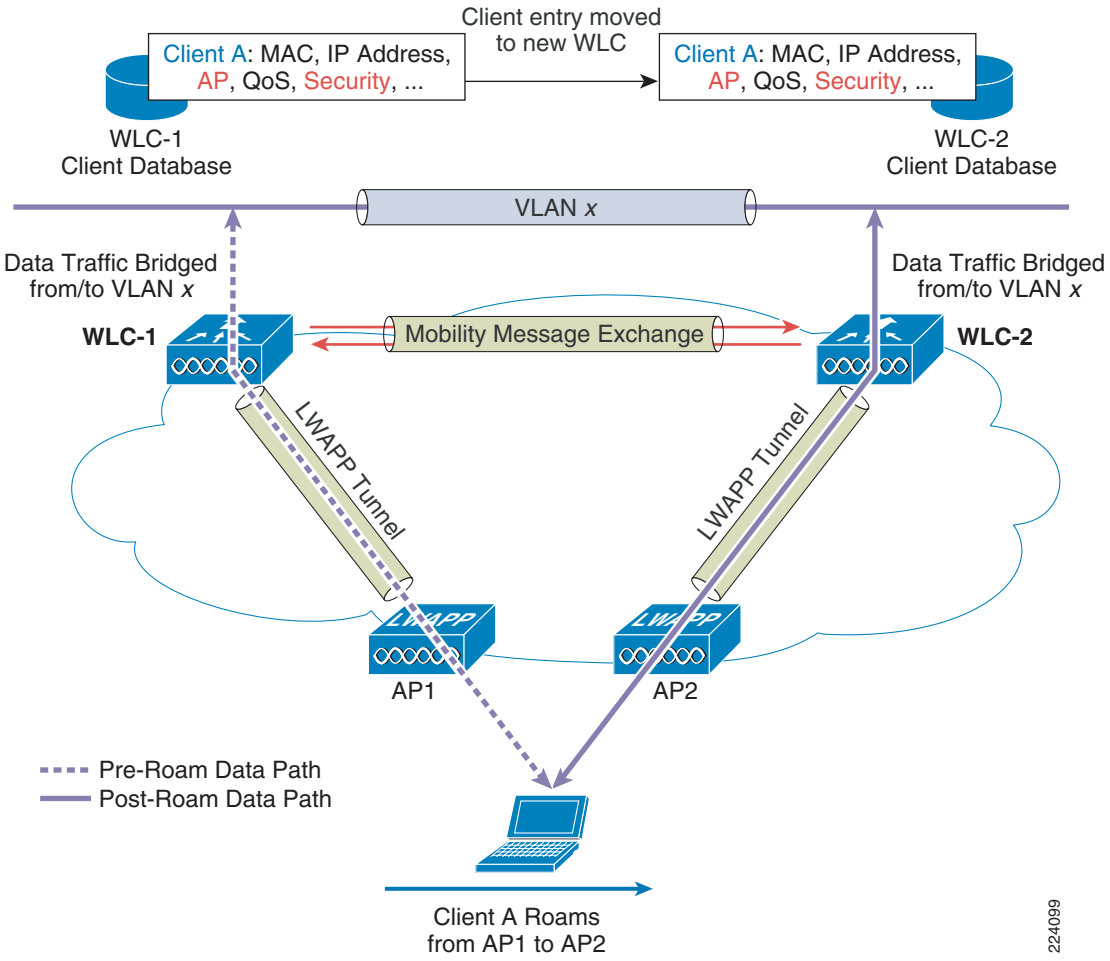
Figure 31 Clients Roaming Between Access Points Joined by Same WLC



When the wireless client moves its association from one access point to another, the WLC simply updates the client database with the new associated access point. If necessary, new security context and associations are established as well.

Now, consider what happens when a client roams from an access point joined to one WLC and an access point joined to a different WLC. Figure 32 illustrates an inter-controller roam in the event of a Layer 2 roam. In this example, the participating controllers are terminating the given WLAN's traffic on the same subnet.

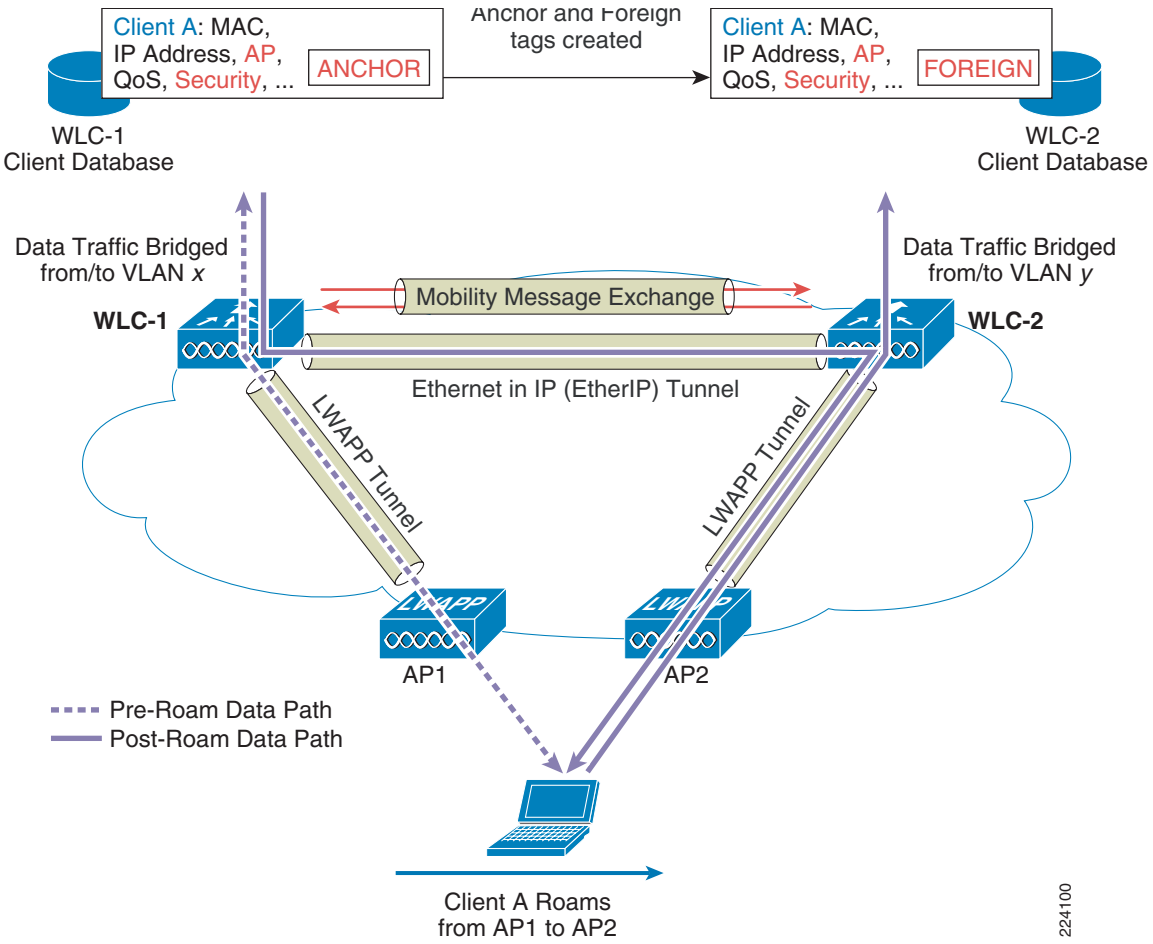
Figure 32 Layer 2 Inter-Controller Roam



As illustrated, a Layer 2 roam occurs when the controllers bridge the WLAN traffic on and off the same VLAN and the same IP subnet. When the client re-associates to an access point connected to a new WLC, the new WLC exchanges mobility messages (via UDP port 16666, or 16667 if controllers are configured to secure these messages with AES). These messages are exchanged with the original WLC, and the client database entry is moved to the new WLC. New security context and associations are established if necessary, and the client database entry is updated for the new access point. All of this is transparent to the end user.

Figure 33 illustrates an inter-controller roam in the event of a Layer 3 roam. In this example, the participating controllers are not terminating the given WLAN's traffic on the same subnet.

Figure 33 Layer 3 Inter-Controller Roam



In Figure 33, a Layer 3 roam occurs when the controllers bridge the WLAN on and off different VLANs and IP subnets. The inter-controller roaming is similar to Layer 2 roaming in that the WLCs exchange mobility messages upon a client roaming. However, instead of moving the client's entry to the new controller's client database, the original WLAN controller marks the client with an "Anchor" entry in its own client database. The database entry is copied to the new controller client database and marked with a "Foreign" entry in the new WLC. The roam is still transparent to the wireless client, and the wireless client maintains its original IP address. Security credentials and context are re-established if necessary.

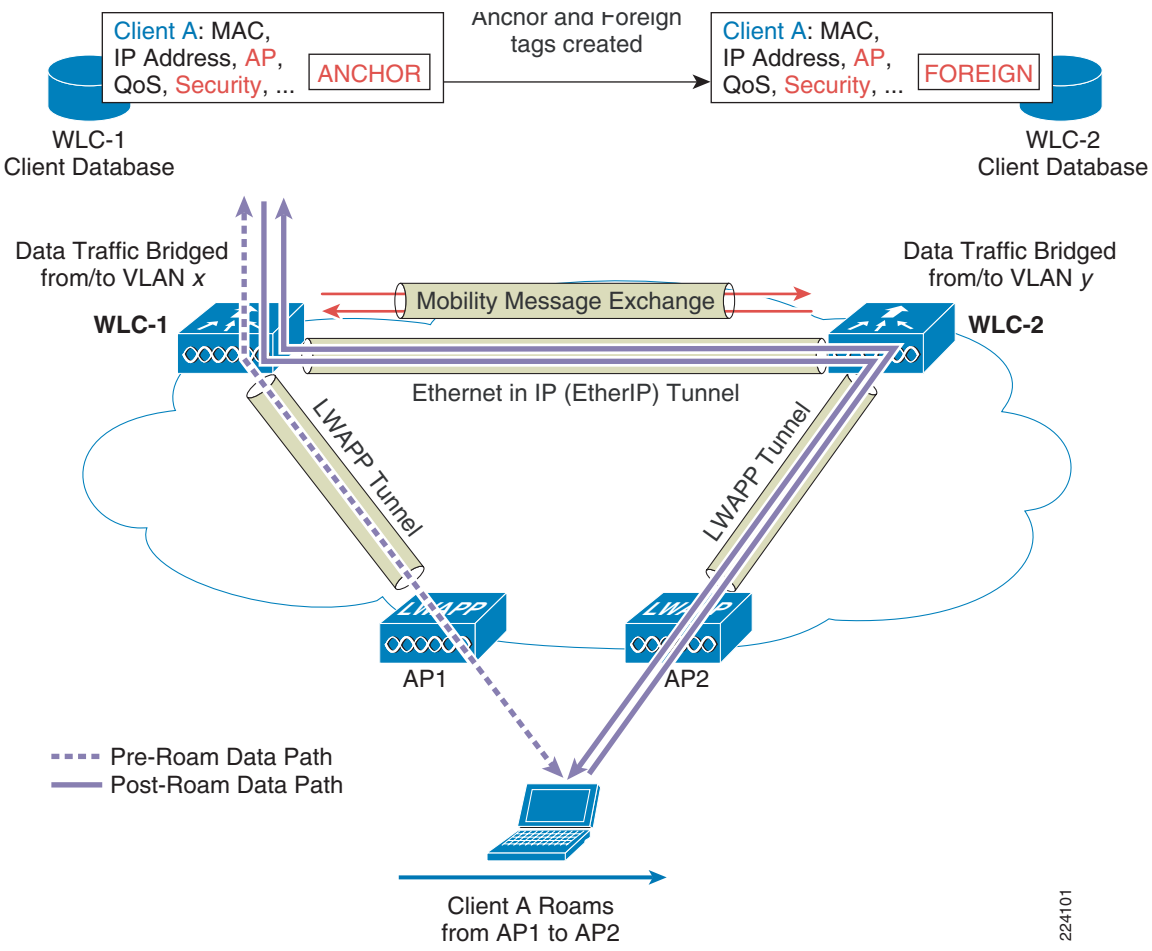
After a Layer 3 roam, data moving to and from the wireless client flows in an asymmetric traffic path. Traffic from the client to the network is forwarded directly into the network by the foreign WLC. Traffic to the client arrives at the Anchor WLC, which forwards the traffic to the Foreign WLC in an Ethernet-in-IP tunnel (EtherIP, defined in IETF RFC 3378). The Foreign WLC then forwards the data to the client.

Note If a wireless client roams to a new foreign WLC, the client database entry is moved from the original foreign WLC to the new foreign WLC, but the original anchor WLC is always maintained.

Symmetric Mobility Tunneling Operation

The 4.1 Symmetric Mobility Tunneling feature allows both roamed clients' ingress and egress traffic to be tunneled to and from the anchor controller. This means that roamed clients reside logically in their anchor controller, and traffic patterns between the anchor and foreign controllers operate fully as a point-to-point symmetric tunnel. The only difference in operation between regular, asymmetric mobility tunneling and this new symmetric traffic flow is that the upstream traffic from roamed clients is not forwarded to the destination by the foreign controller. Upstream traffic is tunneled to the anchor controller first, where delivery to the network occurs (see Figure 34):

Figure 34 Symmetric Mobility Tunneling



This feature allows the underlying wired network architecture to remain fully unchanged when such security features as reverse path forwarding or filtering (RPF) checking is enabled on intermediary Layer 3 interfaces or when firewall rules prevent such operation between controllers configured in a mobility group (a cluster of controllers between which roaming is desired).

Mobility Configuration

The first step to configure Symmetric Mobility Tunneling is to verify that all controllers between which seamless roaming must occur are properly configured for mobility operations. When basic mobility is configured and verified, Symmetric Mobility Tunneling may be enabled.

Mobility configurations can be made through WCS or through the controller's GUI or CLI (though only one configuration interface should be employed for each given configuration step).

Configuring Asymmetric Mobility in WCS

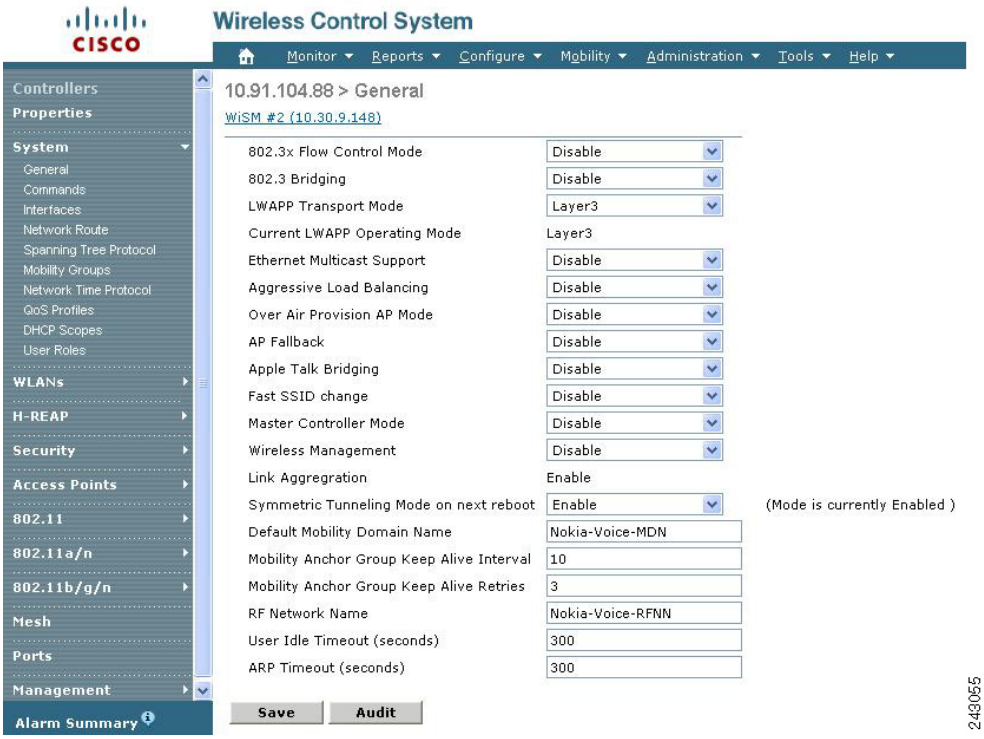
Follow these instructions to configure basic, asymmetric mobility tunneling in WCS.

Step 1 Choose **Configure > Controllers.**

Step 2 Click on the controller of choice.

Step 3 From the left sidebar menu, choose **System > General** (see Figure 35).

Figure 35 System > General



Step 4 Change the Mobility Domain Name (sometimes referred to as the Mobility Group Name) for any controllers which do not share the same Mobility Domain Name.

Step 5 When the Mobility Group Name is configured, choose **System > Mobility Groups** from the left sidebar menu. The selected controller's mobility list appears (see Figure 36).

Figure 36 Mobility Group Window

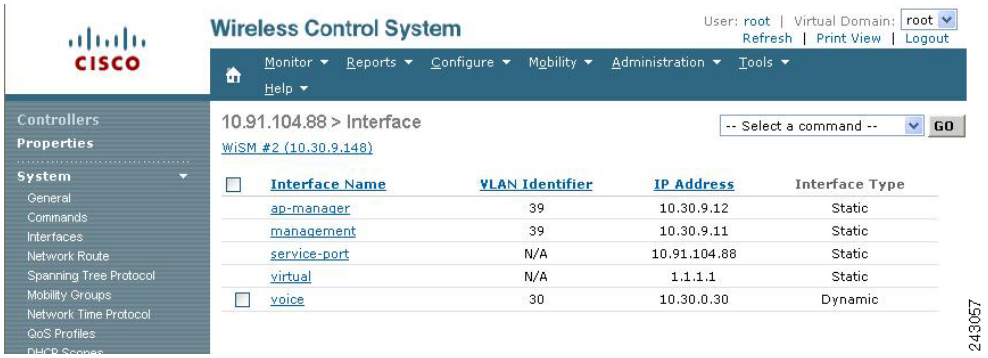
Step 6 To add members to the list, choose **Add Group Members…** from the Select a command drop-down menu and click **GO**. All of the controllers WCS is managing that are not in the individual controller's list are displayed.

Step 7 Click the check box to the left of desired controllers and click **Save**.

Note To perform this operation across multiple controllers, use the WCS controller template feature. This feature (Configure > Controller Templates) forwards identical configurations to a group of controllers simultaneously.

Step 8 Choose **System > Interfaces** to ensure that all controllers share the same virtual interface address (see Figure 37).

Figure 37 System > Interface Window



Step 9 To change the value so that all controllers have the same address, click on the link under the Interface Name column. Change the address and click **Save**.

Note **Note**: This value must be a non-routed address and must be identical across all controllers in the mobility group.

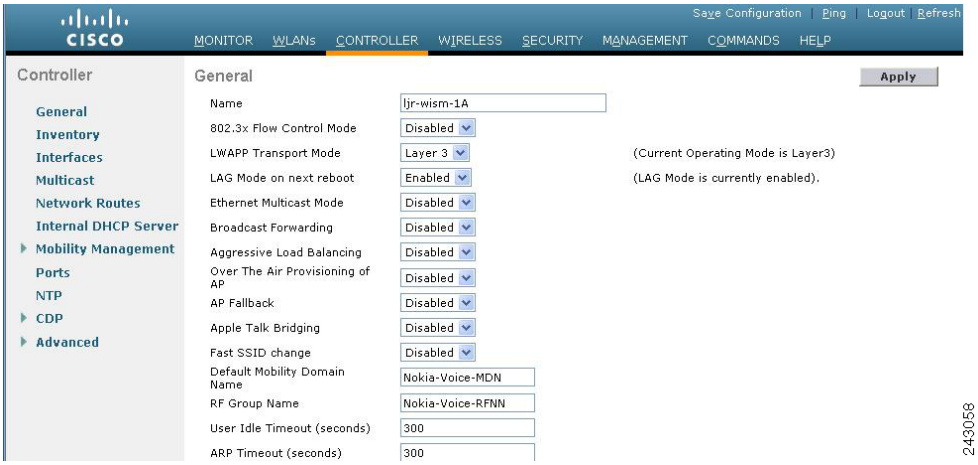
Step 10 Return to the main list of controllers by choosing **Configure > Controllers.** Ensure that all other necessary controllers are properly configured with identical Mobility Group Names and have all other controllers in the group in their Mobility Lists. Also, ensure that all controllers share the same Virtual Interface address.

Configuring Asymmetric Mobility from the WLC GUI

Follow these instructions to configure basic, asymmetric mobility tunneling from the WLC GUI.

Step 1 Choose the Controller tab at the top of the screen. The General heading is shown initially (see Figure 38). Ensure that the Default Mobility Domain Name value is consistent across all necessary controllers.

Figure 38 WLC General Window



Step 2 Choose **Mobility Management** under the Controller tab. Click **Mobility Groups** and make sure that all controllers have MAC and IP addresses in the controller's mobility lists (see Figure 39).

Figure 39 Static Mobility Group Members Window

Step 3 Perform one of the following:

- Click **New** from the upper right-hand corner to add a single controller. Enter the controller information and click **Apply**.

  or

- Click **Edit All** from the upper right-hand corner to add multiple controllers.

Step 4 Choose the **Interfaces** heading under the Controller tab to ensure that all WLCs have the same virtual interface address (see Figure 40).

Figure 40 Interfaces Window

Step 5 If changes are necessary, click **Virtual** in the Interface Name column and make the necessary changes. Click **Apply**.

All controllers are now properly configured for regular mobility.

Verifying Asymmetric Mobility Operation

Follow these WLC CLI instructions to verify that basic, asymmetric mobility is operational.

Note To properly trigger the asymmetric mobility tunneling feature (as well as the new Symmetric Mobility Tunneling feature), controllers must be across routed boundaries. If controllers are on the same subnet, then mobility events are not invoked. The client record is simply moved to the next controller, and traffic flows natively to and from that new controller (refer to the "Background on Mobility in Cisco's Unified Wireless Network" section on page 33 for a more in-depth discussion of mobility operations).

Follow the previous configuration steps to ensure correct configuration. Use the controller CLI to view the mobility configuration.

```
(Cisco Controller) >show mobility summary

Symmetric Mobility Tunneling (current) .......... Disabled
Symmetric Mobility Tunneling (after reboot) ..... Enabled
Mobility Protocol Port.......................... 16666
Mobility Security Mode.....................Disabled
Default Mobility Domain......................... test
Mobility Keepalive interval..................... 10
Mobility Keepalive count........................ 3
Mobility Group members configured............... 2

Controllers configured in the Mobility Group
MAC Address        IP Address       Group Name         Status
00:16:9d:ca:dc:c0    10.10.10.10      <local>          Up
00:19:07:24:12:e0    20.20.20.20      test             Up
```

The simplest indicators of proper mobility configuration are two ping variants run between controllers. To verify that configuration is sound and the intermediary network is properly forwarding the necessary traffic, run both the **eping** and **mping** commands from the CLI. Use the following command to test the operation of the EtherIP data tunnel between controllers.

```
(Cisco Controller) >eping [peer controller's management interface IP address]
```

Similarly, the operation of the UDP port 16666/16667 inter-controller management path can be tested by the following command.

```
(Cisco Controller) >mping [peer controller's management interface IP address]
```

When mobility has been verified as properly configured and operational, you can configure the wireless network for Symmetric Mobility Tunneling.

Note To work properly, all controllers in the mobility group MUST be configured for Symmetric Mobility Tunneling.

Configuring Symmetric Mobility in WCS

Follow these instructions to configure symmetric mobility tunneling in WCS.

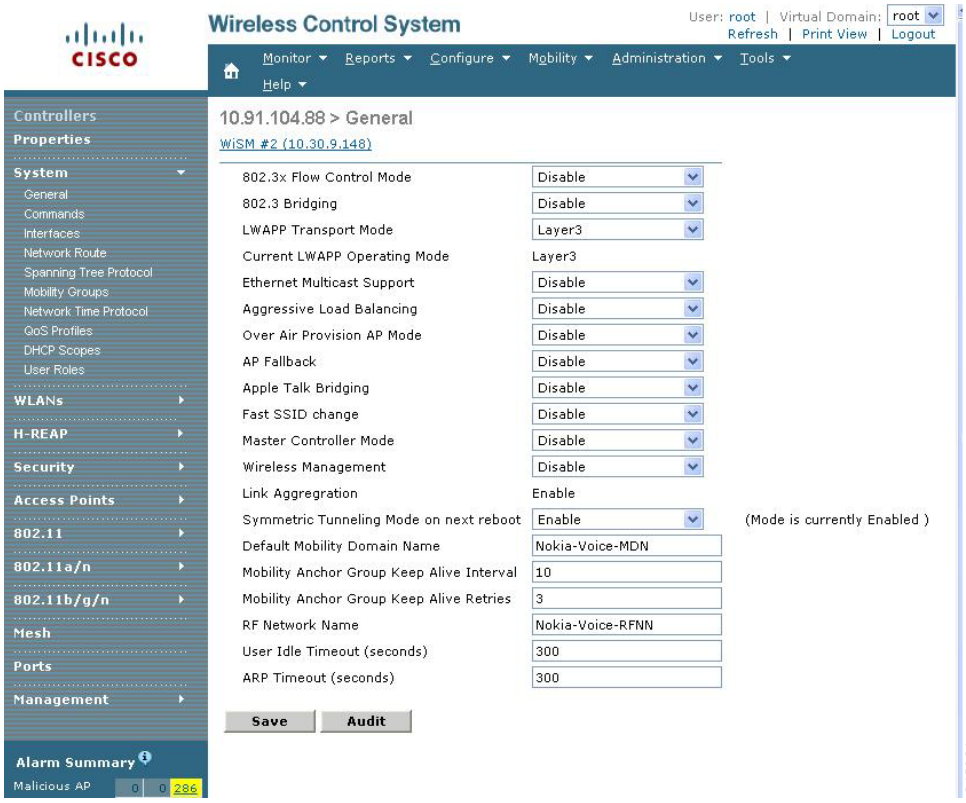
Step 1 Choose **Configure > Controllers** and then select the controller of choice.

Step 2 On the left sidebar menu, choose **System > General**.

Step 3 Choose **Enable** from the Symmetric Mobility Tunneling Mode on the Next Reboot drop-down menu (see Figure 41).

Figure 41 Enabling Symmetric Mobility Tunneling Mode on Next Reboot

.



Step 4 Click **Save**.

Note To perform this operation across multiple controllers, use the WCS controller template feature. This feature (Configure > Controller Templates) forwards identical configurations to a group of controllers simultaneously.

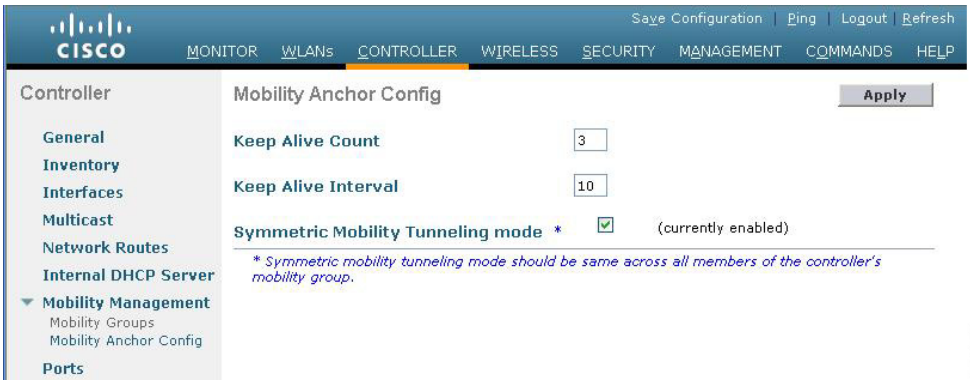
Configuring Symmetric Mobility from the Controller GUI

Follow these steps to configure Symmetric Mobility Tunneling from the WLC GUI.

Step 1 Go to **Controller > Mobility Management** and then select the **Mobility Anchor Config** subheading.

Step 2 Click the check box to enable Symmetric Mobility Tunneling mode and click **Apply** (see Figure 42).

Figure 42 Mobility Anchor Config



Note To configure the mobility anchor through the WLC CLI, enter the following command:

(Cisco Controller) >**config mobility symmetric-tunneling enable**

Step 3 Save the configuration and reboot each controller in the mobility group. (Again, in WCS, this process is easier using Configure > Controller Templates.)

Note Make sure all configurations are saved and the controllers rebooted. Without this step, Symmetric Mobility Tunneling will not work.

Reference Links

The documents referenced in this paper can be found at the following links.

Wireless LAN Compliance Status

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps4570_Products_Data_Sheet.html

Cisco Wireless Control System Configuration Guide

http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcspref.html

Cisco Wireless LAN Controller Configuration Guide

http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/c40sol.html

Cisco 2700 Series Wireless Location Appliance Deployment Guide

http://www.cisco.com/en/US/docs/wireless/technology/location/deployment/guide/depgd.html

Wi-Fi Location Based Services Design Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html

Voice over Wireless LAN Design Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan_ch8.html

Enterprise Mobility Design Guide

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns820/landing_ent_mob_design.html

Appendix A

Figure 43 shows the packet markings of the VoWLAN packets as they transition from VoWLAN client through the access point and then to the controller.

Figure 43 Transitioning VoWLAN Packets