SpectraLink Phone Design and Deployment Guide

Document ID: 70442

Introduction
Prerequisites
- Requirements
- Components Used
- Conventions

SpectraLink IP Telephony Overview
- SpectraLink Call Capacity Considerations
- NetLink SVP100 Server Capacity

Architecture Overview
- SpectraLink Site Survey Recommendations
- Recommended Environment for NetLink Telephones

Quality of Service
- WLAN Traffic Transmission Collision Avoidance
- SVP Server QoS Configuration
- QoS for Voice Traffic

VoWLAN Deployments Cisco Recommendations
- Recommendations for Multifloor Buildings, Hospitals, and Warehouses

Security Mechanisms Supported
- LEAP Considerations

Wireless Network Infrastructure
- Voice and Data VLANs
- Network Sizing
- Switch Recommendations

Deployments and Configuration
- Phone Configuration
- Wireless Network Infrastructure Configuration
- SSID Configuration
- Enable EDCF for the Spectralink Phone
- Enable SVP on the Controller and Access Points

Wireless IP Telephony Verification
- Association, Authentication, and Registration
- Common Roaming Issues
- Audio Problems

Appendix A
- Packet Traces

Appendix B
- AP and Antenna Placement
- Interference and Multipath Distortion
- Signal Attenuation

Related Information

Introduction

This document provides design considerations and deployment guidelines for an implementation of the SpectraLink Voice over Wireless LAN (WLAN) (VoWLAN) technology on the Cisco Unified Wireless Network infrastructure.

Note: Obtain support for SpectraLink products directly from SpectraLink support channels. Cisco Technical Support is not trained to support SpectraLink−related issues.

This guide is a supplement to Deploying Cisco 440X Series Wireless LAN Controllers and only addresses the configuration parameters that are particular to SpectraLink VoWLAN devices in a lightweight architecture. All documents that are referenced here are available on Cisco.com.

Prerequisites

Requirements

This document builds on ideas and concepts in these two Solution Reference Network Design (SRND) documents:

- Cisco IP Telephony Solution Reference Network Design (SRND) for Cisco CallManager 4.0 and 4.1
- Cisco Wireless IP Phone 7920 Design and Deployment Guide

This document assumes that you are familiar with the terms and concepts in these two SRND documents.

Components Used

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

Conventions

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

SpectraLink IP Telephony Overview

The SpectraLink NetLink telephones make use of the proprietary SpectraLink Voice Priority (SVP) and the SpectraLink Radio Protocol (SRP) for all communications among themselves and other pieces of the SpectraLink VoWLAN infrastructure. The different pieces of a typical SpectraLink deployment can consist of an SVP server and/or SVP gateway, access points (APs), and NetLink telephones. You must understand the goals that SVP tries to accomplish.

The NetLink phones do not support Dynamic Transmit Power Control (DTPC). Therefore, the size of the cell grows to that of the client with the highest transmit power. If the phones did use DTPC and other Cisco Compatible Extensions (CCX) features, the WLAN controller (WLC) could control the transmit power of the client, as well as provide other advantages of the enhancements from CCX version 4 (CCXv4).

Note: The SVP solution does not make use of the IEEE 802.11e QoS Basis Service Set (QBSS) or Call Admission Control (CAC) logic that is implemented on the Cisco Unified WLAN system. Therefore, it is possible to overload a radio frequency (RF) channel and create call quality/capacity issues.

There are a number of different SpectraLink SVP servers, which can be directly mapped to the size of the wireless voice network that is needed. The remainder of this section provides details.

SpectraLink Call Capacity Considerations

The NetLink SVP server capacity ranges from 10, 20, or 80 simultaneous calls per server.

Here is an excerpt from the data sheet:

"A single SVP Server supports up to 120 simultaneous calls. In most cases, this provides sufficient call capacity for a NetLink Gateway system, which has a maximum capacity of 640 handsets. **When used with an IP telephony server, a single SVP Server will support up to 80 simultaneous calls. Multiple SVP Servers can be used to support more than 800 simultaneous calls in the IP telephony server environment.** The SVP server supports multiple configurations to provide Quality of Service (QoS) for customers of all sizes. For small businesses or remote offices, the SVP server is available in 10 and 20 user configurations. **Up to four of these servers can be stacked** to provide cost−effective scalability as your business grows. For larger customers, **a third SVP server option is available supporting up to 80 simultaneous calls.** Up to 16 of these servers can be combined to provide a maximum system capacity greater than 800 simultaneous calls or approximately 8,000 users."

Note: Although the data sheet mentions a simultaneous call capacity of 128 calls, **this capacity can only be reached with more than one SVP server deployed**.

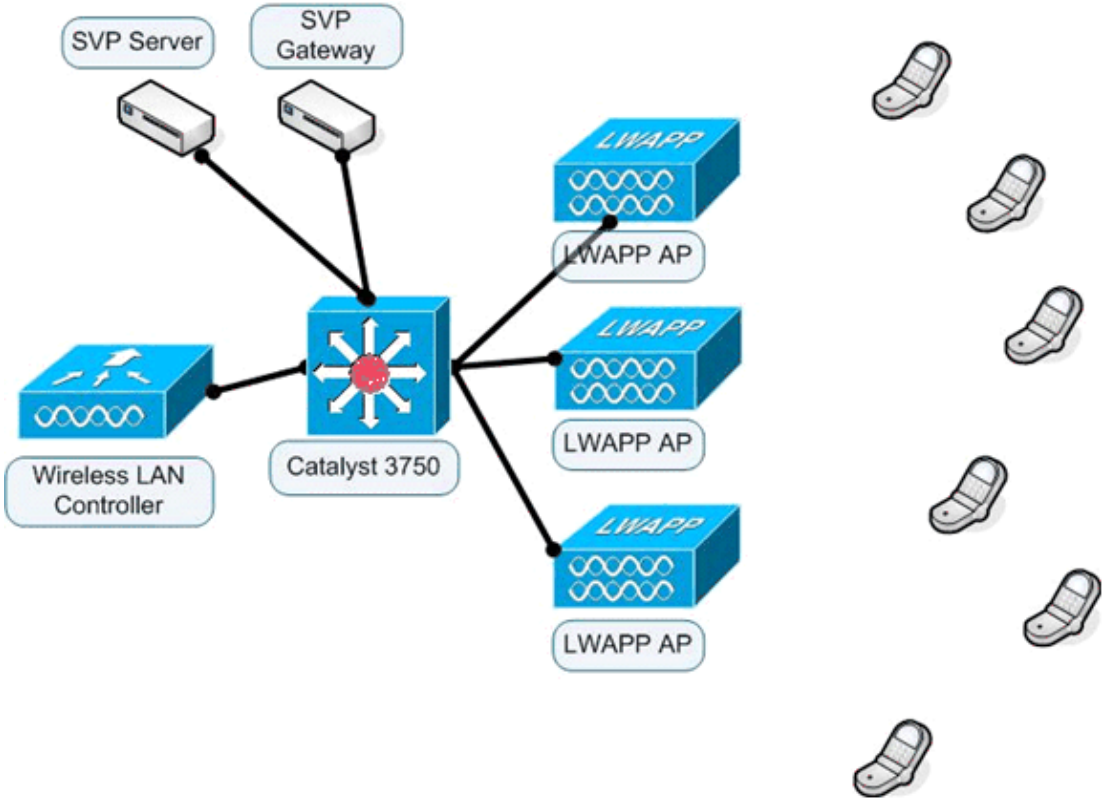
NetLink SVP100 Server Capacity

The number of active calls that are handled determines the capacity of the SVP100 Server. This table shows the capacity of an IP gateway in a multiple−SVP server environment.

SVP Servers	Calls per Server	Total Calls	Erlangs	10% Use	15% Use	20% Use
1	80	80	65	500	433	325
2	64	128	111	1000	740	555
3	60	180	160	1500	1067	800
4	58	232	211	2000	1407	1055
5	57	285	262	2500	1747	1310
6	56	336	312	3000	2080	1560
7	56	392	367	3500	2447	1835
8	55	440	415	4000	2767	2075
9	55	495	469	4500	3127	2345
10	55	550	524	5000	3493	2620
11	55	605	578	5500	3853	2890
12	54	648	621	6000	4140	3105
13	54	702	674	6500	4493	3370
14	54	756	728	7000	4853	3640
15	54	810	782	7500	5213	3910
16	54	864	836	8000	5573	4180

Architecture Overview

This diagram represents a very simplified SpectraLink solution deployment:



SpectraLink Site Survey Recommendations

The SpectraLink white paper Best Practice Guide for Deploying SpectraLink 8020/8030 Wireless Telephones states that at least one AP needs to have signal coverage to the SpectraLink phone of −70 dBm in all areas where the phone will be used. The white paper also states that the phone needs to be perceived at at least −60 dBm or better in order to ensure a data rate of 11 Mbps. The Cisco unified architecture designs the overall network in such a way that any AP shapes cell coverage edges to −65 dBm. Therefore, given that there are enough APs to provide service in the entire coverage to all user areas, and with the radio resource management (RRM) algorithms at work to detect and correct coverage holes, the Cisco architecture is ideally suited for SpectraLink deployments. However, some sites will have RF challenges that will require the manual configuration of RF parameters on the controller or Wireless Control System (WCS) (which depends on how the network is managed).

Recommended Environment for NetLink Telephones

This section describes the environment that is necessary for a successful voice deployment.

Note: These suggestions change when you use the deployed network for both data and voice. As the SpectraLink Site Survey Recommendations section mentions, SpectraLink recommends a cell of −70 dBm. However, −60 dBm are necessary in order to support an 11−Mbps cell.

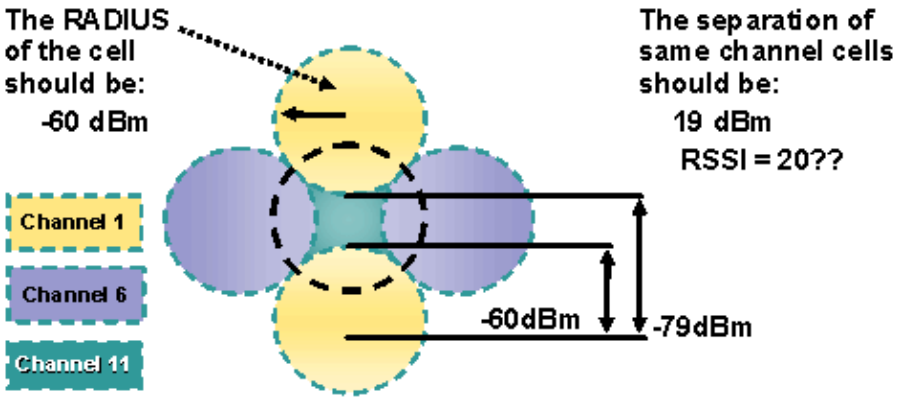
Determine the number of phones to be used in a given area before you conduct the site survey in order to appropriately determine the transmit power of the clients and AP (if needed). If you do so, you can turn down the transmit power in order to create smaller coverage cells, which increases the number of calls in a given floor space. You must test the values listed here, both during the site survey and when the network is enabled for all users.

Note: A reduction of transmit power equals smaller cells, which results in more calls per given coverage area.

Observe these guidelines when you set up the environment for the NetLink phone:

- Deploy a minimum of two APs on nonoverlapping channels, with a Received Signal Strength Indicator (RSSI) that is greater than 35 dBm at all times.
- Deploy no more than one AP per overlapping channel set, with an RSSI that is greater than 35 dBm.
- Although APs can appear to have an RSSI that is less than 35 dBm (on overlapping APs), this situation can still cause interference. Minimize this situation as much as possible. This interference or noise degrades voice quality.
- Noise is additive. If you have three extra APs on the same channel, all with low RSSIs, the situation can be as harmful as a single extra AP with a higher RSSI.
- This illustration shows a typical deployment, with a 15−percent to 20−percent overlap of a given AP cell from each of the adjoining cells. This configuration provides almost complete redundancy throughout the cell, and so complies with the requirements in this list.

Figure 1 Cell Overlap Guidelines



- If the netlink phone is to be operated in 802.11b mode, maintain at least 11 Mbps of available link speed at all times for data clients as well as voice clients. In certain situations, data rates below 11 Mbps must be enabled for legacy devices. If you must enable both 11 Mbps and 2 Mbps, these low speeds reduce the number of simultaneous calls that each AP can handle and the effective throughput. This also increases the radio cell, where the noise floor also can be increased, which can impact voice quality.

.

- Maintain an AP coverage overlap of at least 15 percent to 20 percent.
- Maintain a packet error rate (PER) of no higher than 1 percent (or a success rate of 99 percent).
- Maintain a minimum signal−to−noise ratio (SNR) of 25 dB.

Quality of Service

QoS is essential in order to ensure that voice traffic receives timely and reliable treatment with low delay, low jitter, and little or no packet loss on the network. QoS ensures that voice traffic receives priority treatment when the traffic travels across the network. QoS is a requirement for both wired and wireless VoIP networks.

WLAN Traffic Transmission Collision Avoidance

Similiar to wired Ethernet networks, 802.11b WLANs employ carrier sense multiple access (CSMA). But instead of the use of collision detection (CD), WLANs use collision avoidance (CA). Instead of an attempt by each station to transmit as soon as the medium is free, WLAN devices use a CA mechanism in order to prevent simultaneous transmit from multiple staions.

DSCP Marking

The Signaling Connection Control Part (SCCP) signaling messages are marked with differentiated services code point (DSCP) 26 or per−hop behavior (PHB) AF31. And Real−Time Transport Protocol (RTP) packets are marked with DSCP 46 (PHB EF). These markings match the DSCP markings of Cisco wired Ethernet IP phones and make the QoS settings consistent for both LAN and WLAN environments. The recommended DSCP or PHB marking for voice control signaling traffic has been changed from DSCP 26 (PHB AF31) to DSCP 24 (PHB CS3). A marking migration is planned within Cisco in order to reflect this change. However, many products still mark signaling traffic as DSCP 26 (PHB AF31). Therefore, in the interim, Cisco recommends that both PHB AF31 and PHB CS3 markings be used for access to call signaling queues.

Apart from DSCP, traffic can be prioritized based on the EDCF standards. 802.11 devices operates in the shared wireless medium. It uses RF waves in order to carry data. DCF is used in 802.11 networks in order to manage access to the radio frequency medium. EDCF called as Enhanced DCF is a part of IEEE 802.11e standard, which is used to prioritize the traffic in the wireless network on the client side. See the Enable EDCF for the Spectralink Phone section for more information on how to configure EDCF for the phones.

Additional Considerations

Beyond these provisions you must consider delay and jitter in the design. The simplest way to reduce delay and jitter is to stay within the guidelines for the number of WLAN clients per AP. If you exceed these guidelines, you create additional opportunities to introduce packet delay and jitter.

SVP Server QoS Configuration

You can reach the configuration menu for QoS settings on the SVP server via a serial connection or Telnet. The SpectraLink guide SpectraLink 8000 SVP Server SVP100, SVP020, SVP010 Administration Guide states that the DSCP value for all egress packets from the server is a default marking of 16. If left at the default settings, the voice packets are marked as "best effort". When those packets are encapsulated on the WLC, the Lightweight AP Protocol (LWAPP) packets have a similar marking as well.

The over−the−air (OTA) packets have access class queuing and OTA marking for best effort. **Cisco highly recommends that you set the traffic class for the SVP WT (In call) and RTP packets to the marking decimal value of 46 (Expedited Forwarding).** With expedited forwarding, LWAPP packets have Architecture for Voice, Video, and Integrated Data (AVVID)−recommended markings for voice and the OTA packets have 802.11e/Wi−Fi Multimedia (WMM)−recommended QoS marking and queuing for voice.

QoS for Voice Traffic

Wireless networks operate as a shared medium, which makes QoS even more difficult to achieve in comparison with wired networks. These characteristics apply to QoS for voice traffic on a wired network:

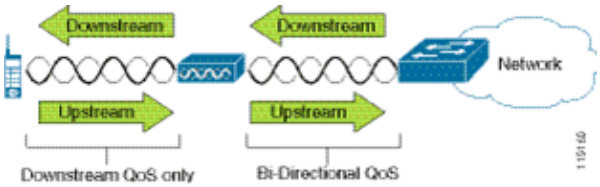
- Dedicated access per user or device (switched Ethernet, point−to−point WAN)
- Packets marked with IEEE 802.1p and IP type of service (ToS) or DSCP
- QoS can be applied to upstream or downstream traffic
- Can provide complete CAC

As a contrast, QoS for voice traffic on a wireless network displays these characteristics:

- Shared access to bandwidth
- Packets marked with 802.1p and IP ToS or DSCP
- QoS is currently available to downstream traffic from the AP, but few devices can provide upstream QoS toward the AP

- Can provide only limited admission control
- Unlike wired networks with dedicated bandwidth, WLAN networks must consider traffic direction when they implement QoS. Traffic is considered either upstream or downstream from the point of view of the AP, as Figure 2 shows:

Figure 2 Upstream and Downstream Traffic



VoWLAN Deployments Cisco Recommendations

Wireless IP Telephony networks require careful RF planning. A thorough voice site survey is often required in order to determine the proper levels of wireless coverage and to identify sources of interference. AP placement and antenna selection choices can be greatly eased with the help of the results of a valid voice site survey. Undoubtedly, the most important consideration is the transmit power of the wireless phone. Ideally, the phone will learn the transmit power of the AP and adjust its transmit power to that of the AP.

Although the majority of the wireless networks today are deployed after extensive RF site surveys, those surveys are done keeping data service in mind. VoWLAN phones are likely to have different roaming characteristics and different coverage requirements than those of a typical WLAN adapter for a mobile client such as a laptop. Therefore, an additional site survey for voice is often recommended in order to prepare for the performance requirements of multiple VoWLAN clients. This additional survey gives the opportunity to tune the APs to ensure that the VoWLAN phones have enough RF coverage and bandwidth to provide proper voice quality.

For additional information on RF design considerations, refer to the Radio Frequency and Site Survey section of the Cisco Wireless IP Phone 7920 Design and Deployment Guide.

Recommendations for Multifloor Buildings, Hospitals, and Warehouses

Consider the factors that this section lists when you survey multifloor buildings, hospitals, and warehouses.

Construction Methods and Materials

Many aspects of the building construction are unknown or hidden from the site survey. So you may have to acquire that information from other sources, such as architectural drawings. Some examples of typical construction methods and materials that affect the range and coverage area of APs include:

- Metallic film on window glass
- Leaded glass
- Steel−studded walls
- Cement floors and walls with steel reinforcement
- Foil−backed insulation
- Stairwells and elevator shafts
- Plumbing pipes and fixtures

Inventory

Various types of inventory can affect the RF range, particularly those with high steel or water content. Some items to watch for include:

- Cardboard boxes
- Pet food
- Paint
- Petroleum products
- Engine parts

Levels of Inventory

Make sure that you perform a site survey at peak inventory levels or at times of highest activity. A warehouse at a 50 percent stocking level has a very different RF footprint than the same warehouse at an inventory level of 100 percent.

Activity Levels

Similarly, an office area after hours (without people) has a different RF footprint than the same area when it is full of people during the day. Although you can conduct many parts of the site survey without full occupation, you *must* conduct the site survey verification and tweak key values at a time when the location is occupied. The higher the utilization requirements and the density of users, the more important it is to have a well designed diversity solution. When more users are present, more signals are received on each user device. Additional signals cause more contention, more null points, and more multipath distortion. Diversity on the AP (antennas) helps minimize these conditions.

Multifloor Buildings

Keep these guidelines in mind when you conduct a site survey for a typical office building:

- Elevator shafts block and reflect RF signals.
- Supply rooms with inventory absorb signals.
- Interior offices with hard walls absorb RF signals.
- Break rooms (kitchens) can produce 2.4−GHz interference through the use of microwave ovens.
- Test labs can produce 2.4−GHz or 5−GHz interference, creating multipath distortion and RF shadows.
- Cubicles tend to absorb and block signals.
- Conference rooms require high AP coverage because they are areas of high utilization.

Administer extra precaution when you survey multifloor facilities. APs on different floors can interfere with each other as easily as APs that are located on the same floor. You can use this behavior to your advantage during a survey. If you use higher−gain antennas, it can be possible to penetrate floors and ceilings and provide coverage to floors above as well as below the floor where the AP is mounted. Be careful not to overlap channels between APs on different floors or APs on the same floor. In multitenant buildings, there can be security concerns that require the use of lower transmission powers and lower−gain antennas in order to keep signals out of neighboring offices.

Hospitals

The survey process for a hospital is similar to the survey process for an enterprise. But the layout of a hospital facility tends to differ in these ways:

- Hospital buildings tend to go through many reconstruction projects and additions. Each additional construction is likely to have different construction materials with different levels of attenuation.

- Signal penetration through walls and floors in the patient areas is typically minimal, which helps create microcells.
- The need for bandwidth increases with the increasing use of WLAN ultrasound equipment and other portable imaging applications. Of course, the need for bandwidth increases with the addition of wireless voice as well.
- Healthcare cells are small, and seamless roaming is essential, especially with voice applications.
- Cell overlap can be high, and so can channel reuse.
- Hospitals may have several types of wireless networks installed, which include 2.4−GHz non−802.11 equipment. This equipment can cause contention with other 2.4−GHz networks.
- Wall−mounted diversity patch antennas and ceiling−mounted diversity omnidirectional antennas are popular. But keep in mind that diversity is required.

Warehouses

Warehouses have large, open areas, which often contain high storage racks. Many times, these racks reach almost to the ceiling, where APs are typically placed. Such storage racks can limit the area that the AP can cover. In these cases, consider the placement of APs on other locations besides the ceiling, such as side walls and cement pillars. Also consider these factors when you survey a warehouse:

- Inventory levels affect the number of APs that are needed. Test coverage with two or three APs in estimated placement locations.
- Unexpected cell overlaps are likely because of multipath variations. The quality of the signal will vary more than the strength of that signal. Clients may associate and operate better with APs that are farther away than with nearby APs.
- During a survey, APs and antennas usually do not have an antenna cable that connects them. But in a production environment, the AP and antenna can require antenna cables. All antenna cables introduce signal loss. The most accurate survey includes the type of antenna to be installed and the length of cable to be installed. A good tool to use to simulate the cable and its loss is an attenuator in a survey kit.

A survey of a manufacturing facility is similar to a survey of a warehouse, except that there may be many more sources of RF interference in a manufacturing facility. In addition, the applications in a manufacturing facility usually require more bandwidth than the applications of a warehouse. These manufacturing facility applications can include video imaging and wireless voice. Multipath distortion is likely to be the greatest performance problem in a manufacturing facility.

Security Mechanisms Supported

In addition to static Wired Equivalent Privacy (WEP) and Cisco Light Extensible Authentication Protocol (LEAP) for authentication and data encryption, the NetLink telephones also support Wi−Fi Protected Access (WPA)/WPA2 Pre−Shared Key (WPA2−PSK).

LEAP Considerations

LEAP allows devices to be authenticated mutually (phone−to−AP and AP−to−phone) based on a user name and password. Upon authentication, a dynamic key is used between the phone and the AP in order to encrypt traffic.

If LEAP is used, a LEAP−compliant RADIUS server, such as the Cisco Access Control Server (ACS), is required to provide access to the user database. The Cisco ACS can either store the user name and password database locally, or it can access that information from an external Microsoft Windows NT directory. When you use LEAP, ensure that strong passwords are used on all wireless devices. Strong passwords are defined as being between 10 and 12 characters in length and can include both uppercase and lowercase characters, as

well as the special characters.

Because most users save their passwords on the phone, Cisco recommends that you use different user names and passwords on data clients and wireless voice clients. This practice helps with tracking and troubleshooting as well as security. Although it is a valid configuration option to use an external (off−ACS) database in order to store the user names and passwords for the phones, Cisco does *not* recommend this practice. Because the ACS must be queried whenever the phone roams between APs, the unpredictable delay to access an off−ACS database can cause excessive delay and poor voice quality. The use of Cisco Centralized Key Management (CCKM) can help here, where reassociations are done at Layer 2 and roam times are minimized to 150 ms or less.

Wireless Network Infrastructure

The Wireless IP Telephony network, just like a wired IP Telephony network, requires careful planning for VLAN configuration, network sizing, multicast transport, and equipment choices. For both wired and wireless IP Telephony networks, the use of separate voice and data VLANs is often the most effective way of deployment in order to ensure sufficient network bandwidth and ease of troubleshooting.

Voice and Data VLANs

VLANs provide a mechanism to segment networks into one or more broadcast domains. VLANs are especially important for IP Telephony networks, for which the typical recommendation is to separate voice and data traffic into different Layer 2 domains. Cisco recommends that you configure separate VLANs for voice and data traffic in this way:

- A native VLAN for AP management traffic
- A data VLAN for data traffic
- A voice or auxiliary VLAN for voice traffic

A separate voice VLAN enables the network to take advantage of Layer 2 marking and provides priority queuing at the Layer 2 access switch port. This ensures that appropriate QoS is provided for various classes of traffic and helps to resolve addressing issues such IP addressing, security, and network dimensioning.

Network Sizing

IP Telephony network sizing is essential in order to ensure that adequate bandwidth and resources are available to meet the demands that the presence of voice traffic presents. In addition to the usual IP Telephony design guidelines for sizing components such as Public Switched Telephone Network (PSTN) gateway ports, transcoders, WAN bandwidth, and so forth, also consider these two 802.11b issues when you size your wireless IP Telephony network:

- **Number of 802.11b devices per AP**

  Cisco recommends that you have no more than 15 to 25 802.11b devices per AP.
- **Number of active calls per AP**

  SpectraLink recommends 10 to 12 calls per AP.

  Note: The number of active calls per AP drops to six when push−to−talk (PTT) traffic exists on the network.

Switch Recommendations

Note: If you use a Cisco Catalyst 4500/4000 series switch as the main router in the network, ensure that it contains, at a minimum, either a Supervisor Engine 2+ (SUP2+) or Supervisor Engine 3 (SUP3) module. The Supervisor Engine 1 or Supervisor Engine 2 module can cause roaming delays, as can the Catalyst 2948G, 2980G, 2980G−A, 4912, and 2948G−GE−TX switches.

You can create a switch port template for use in the configuration of any switch port for connection to an AP. This template should add all the baseline security and resiliency features of the Standard Desktop template. In addition, when you attach the AP to a Catalyst 3550 switch, you can optimize the performance of the AP if you use Multilayer Switching (MLS) QoS commands in order to limit the port rate and to map class of service (CoS) to DSCP settings.

It is also advantageous to use the policing and rate limiting capabilities of the Catalyst 3550 in order to eliminate excessive dropped packets by the AP.

An AP can send out unwanted Layer 2 broadcast/multicast traffic in these scenarios:

- When the upstream switch does **not** have Internet Group Management Protocol (IGMP) snooping functionalities, the AP gets **all** broadcast/multicast streams in the same VLAN.
- When a client of one radio interface is interested in one multicast stream, the AP sends it to the other radio interface as well.
- When the last client of a multicast stream roams away, the AP can still get the multicast stream and send it out to both radios unnecessarily.

Any traffic that is not required by WLAN clients should not be sent to an AP. Design a template in such a way that it helps to create a secure and resilient network connection with these features:

- Return port configurations to "default" This clears any preexisting port configurations and prevents configuration conflicts.
- Disable Dynamic Trunking Protocol (DTP) This disables dynamic trunking, which is not necessary for connection to an AP.
- Disable Port Aggregation Protocol (PAgP) PAgP is enabled by default but is not needed for user−facing ports.
- Enable PortFast This allows a switch to quickly resume forwarding traffic if a spanning tree link goes down.
- Configure wireless VLAN This creates a unique wireless VLAN that isolates wireless traffic from other data, voice, and management VLANs. This traffic isolation ensures greater control of traffic.
- Enable QoS; do not trust port (mark down to 0) This ensures the appropriate treatment of high−priority traffic, which includes softphones, and prevents the user consumption of excessive bandwidth through the reconfiguration of user PCs.

You can use the Cisco 3550−24−PWR Inline Power Switches to provide power to APs that are able to receive inline power.

Deployments and Configuration

Phone Configuration

Refer to the SpectraLink website.

Wireless Network Infrastructure Configuration

Follow the Cisco Unified Wireless Network design and deployment guide for the overall configuration of your WLCs. This section provides additional recommendations that are specific to SpectraLink VoWLAN phones.

Make sure that the wireless infrastructure configuration devices that you use have passed the Voice Interoperability for Enterprise Wireless (VIEW) certification.

The Voice Interoperability for Enterprise Wireless (VIEW) Certification Program of SpectraLink is designed to ensure interoperability and high performance between NetLink wireless telephones and Wireless LAN infrastructure products.

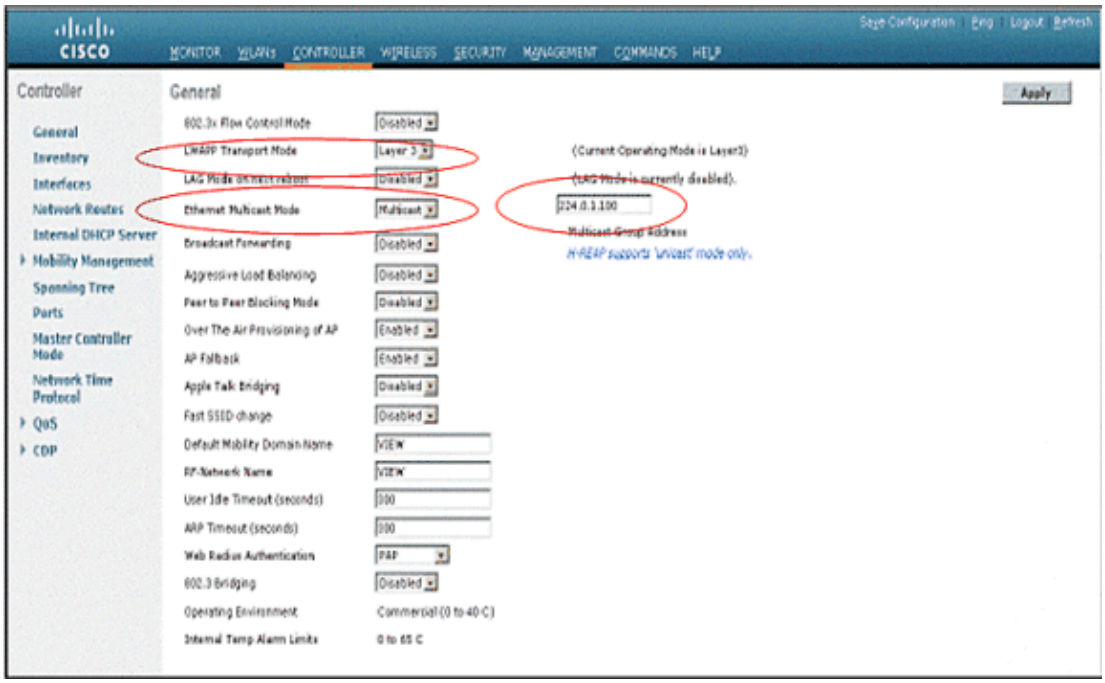
Manufacturer:	Cisco Systems: www.cisco.com			
Approved products:	4400 series WLC, WiSM and 3750G with LWAPP-capable 1130†, 1200, and 1300 series APs			
RF technology:	802.11b/g/a			
Radio:	2.4 GHz 802.11b/g), 5 GHz (802.11a)			
Tested security :	WPA-PSK, WPA2-PSK			
AP and WLC software version tested:	4.1.171.0			
Handset models tested:	e340/h340/i640	8000 Series		
Handset software tested:	89.134	122.010 or greater		
Radio mode:	802.11b	802.11b	802.11g	802.11a
Maximum telephone calls tested per AP:	10	10	12*	
Network topology	Switched Ethernet (recommended)			

† Denotes products directly used in Certification Testing.

* Maximum calls tested during VIEW Certification and the recommended setting in the SVP Server. The certified product may actually support a higher number of maximum calls for 802.11a and 802.11g radio modes.

The initial setup of the controller is this:

1. From the main menu, click **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 used on your network for the Multicast Group Address. This multicast address is preferably in the private multicast range (rfc 2365).
4. Click the **Apply** button.
5. Click **Save Configuration**.



Create Interfaces

Under the Controller tab at the top of the window, click **Interfaces**.

Note: Your VLAN Identifier and IP Address will vary from the example. The window in Figure 4 provides sample addressing. Do not follow the example directly.

Figure 4 List of WLC Interfaces

Create the Voice Interface

Complete these steps:

1. Choose **New**.

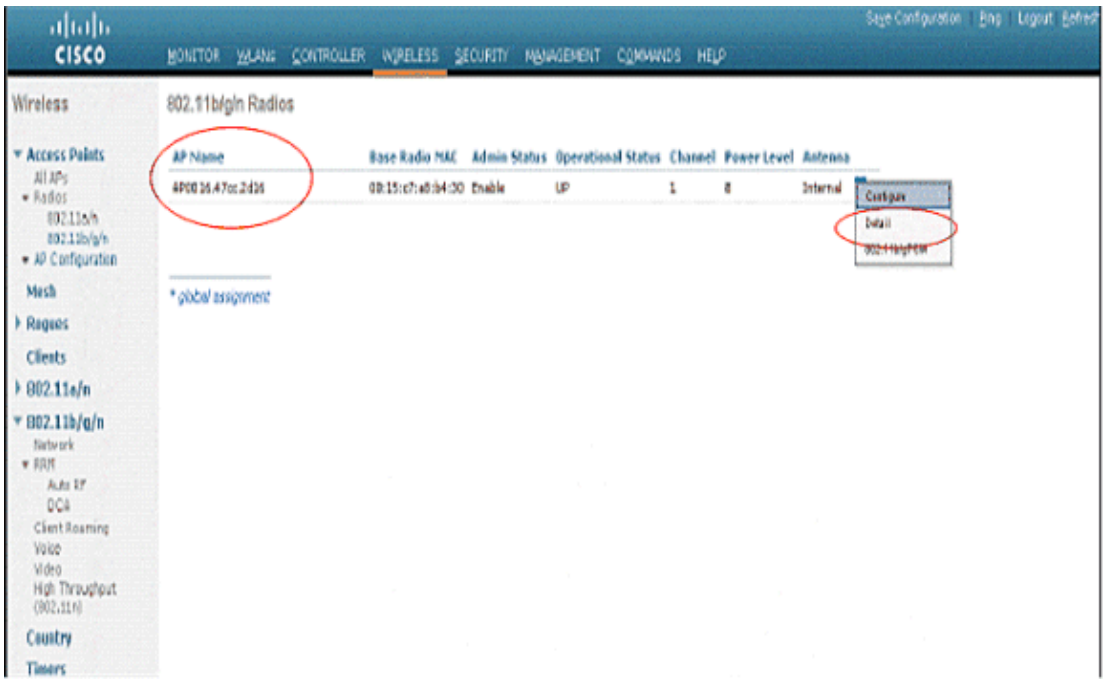
2. In the Interface Name field, enter a tag name that is representative of your SpectraLink VoWLAN network.
3. In the VLAN ID field, enter the VLAN number of that VoWLAN network.
4. Choose **Apply**, and then choose **Edit** in order to edit the interface that is created.
5. Enter the IP addressing for this interface that is in the range of the VLAN and other related information.
6. Choose **Apply**.

Note: The drop−down menu shows QoS Profiles. The profile options on the controller are separate and are not related to the QoS options that are recommended for the SVP server. The QoS Profile on the controller should be fine with the defaults, while the SVP servers QoS must have the DSCP values for WT (In call) and RTP packets must be set to a marking decimal value of 46 (Expedited Forwarding).

AP Configuration

Perform these procedures:

1. Power−on and connect the APs to the network. Wait a few minutes for the APs to find the controller.
2. Verify that the APs are associated to the WLC.
3. From the main menu, click **Wireless**.
4. Choose **Detail** from the drop−down list for the Access Point for which you want to configure the AP details.



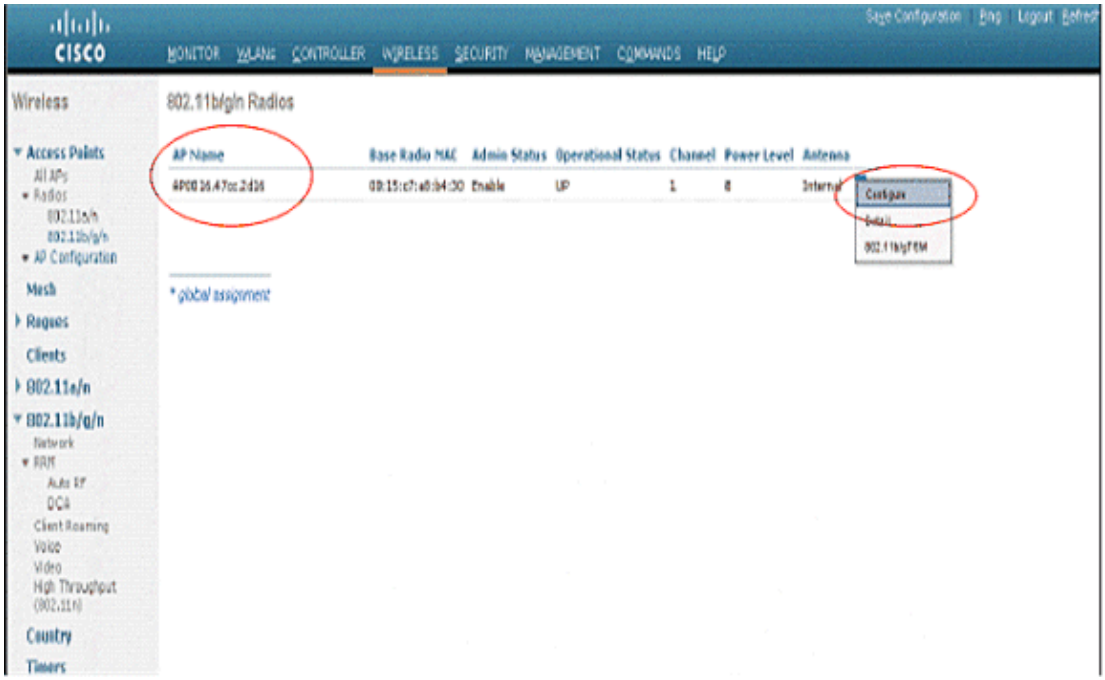
5. Ensure that the AP is configured for DHCP. Because the APs are connected to the network, they automatically find the controller through the LWAPP discovery algorithms. The Dynamic Host Configuration Protocol (DHCP) server assigns each AP an IP address.

Configuration of Access Point for Netlink Telephones that Operate in 802.11g/b Mode

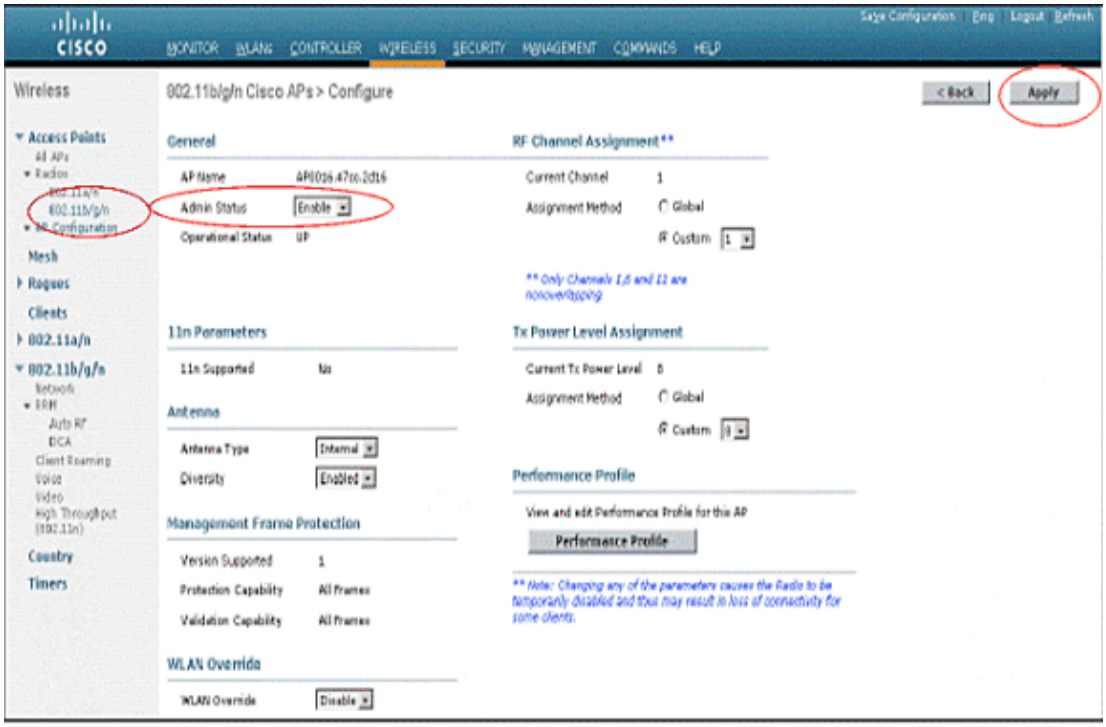
Perform these procedures:

1. From the main menu, click **Wireless**.
2. In the navigation pane, under **Access Points**, choose **Radios**, and then choose **802.11b/g/n**. All the APs that are connected are listed and show their Operational Status as UP.

3. Choose **Configure** from the drop−down list for the access point that you wish to change.



4. Set the Admin Status to **Enable**. Also make sure that Diversity is set to **Enabled**.
5. Configure any other settings that are relevant to your deployment, as needed.
6. Click the **Apply** button to save all changes.

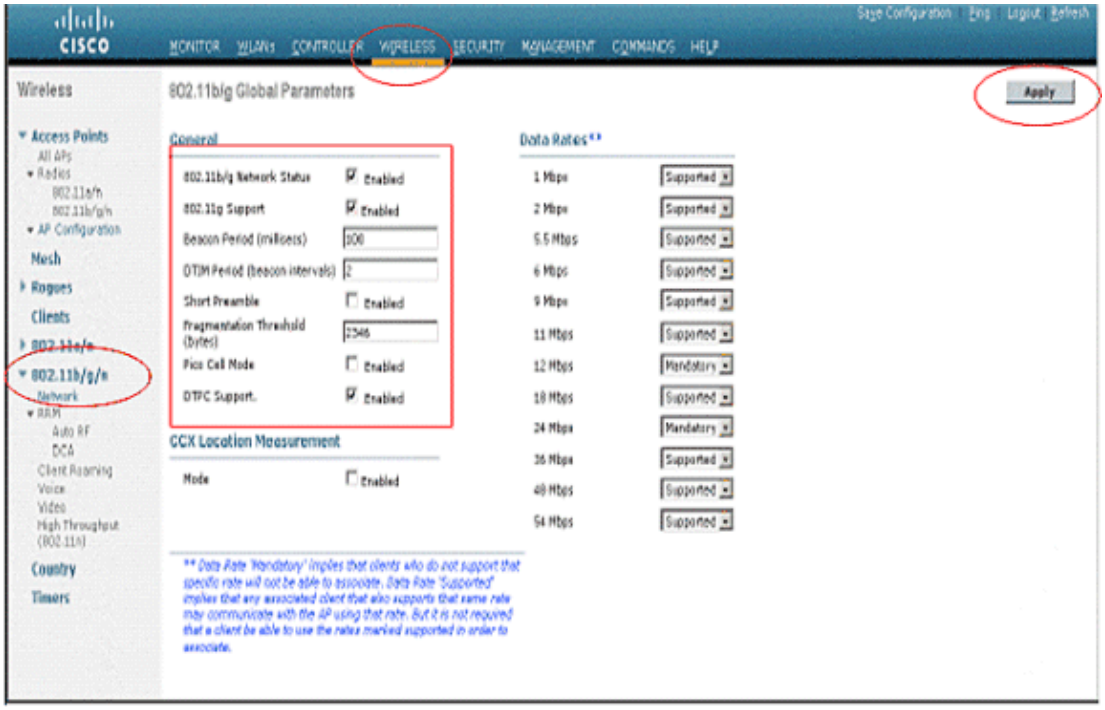


7. In the navigation pane, under 802.11b/g/n, choose **Network**.
8. For 802.11b/g Network Status and 802.11g Support, click the **Enabled** check box if the NetLink wireless telephones are configured for 802.11g−only mode.
9. For setting up the Data Rates, consult the RF site survey of your facility that is designed for voice traffic to determine if you have sufficient coverage to support all data rates. NetLink wireless telephones require this minimum dBm reading to support the correspondent Mandatory data rate setting in the access point.

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11b	-70 dBm	1 Mb/s
	-60 dBm	11 Mb/s
802.11g	-63 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

10. Use the default Fragmentation Threshold (2346 bytes).
11. Set the Beacon Period to **100**.
12. Set the DTIM Interval to **2** .
13. Do not enable Short Preamble unless the environment is an 802.11g−only environment.
14. NetLink handsets do not support dynamic power and do not utilize the information element that is set when the DTPC Support is enabled. NetLink handset power must be configured to match the highest transmit power of the APs.
15. Click the **Apply** button to save the settings.

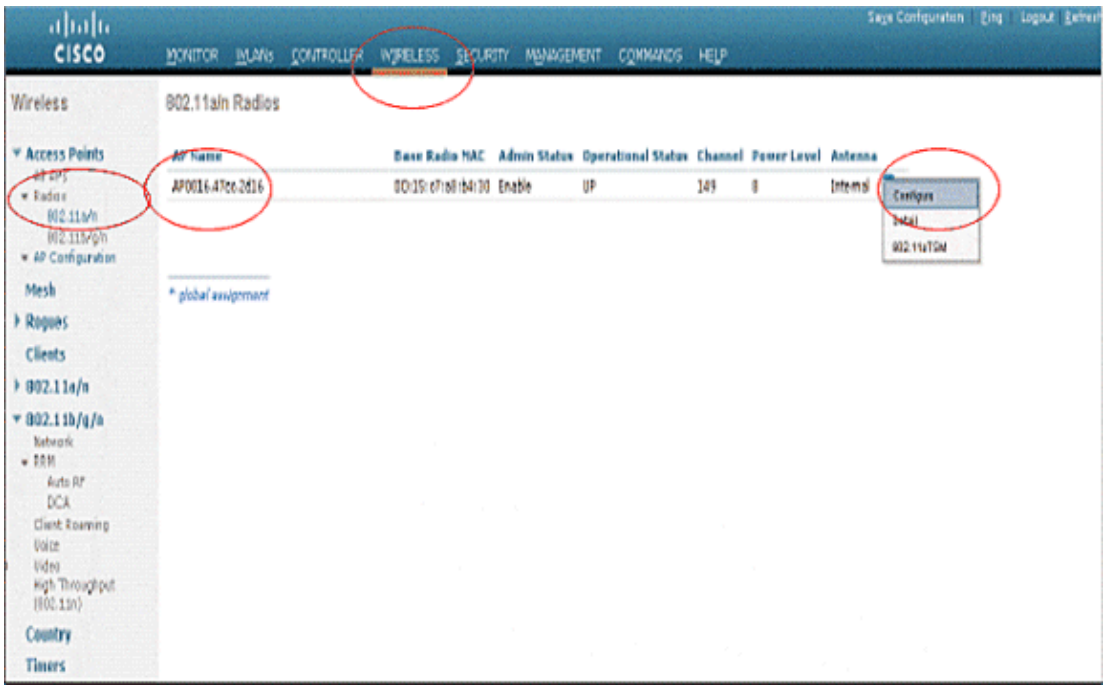
This is a screenshot that explains steps 7 to 14.



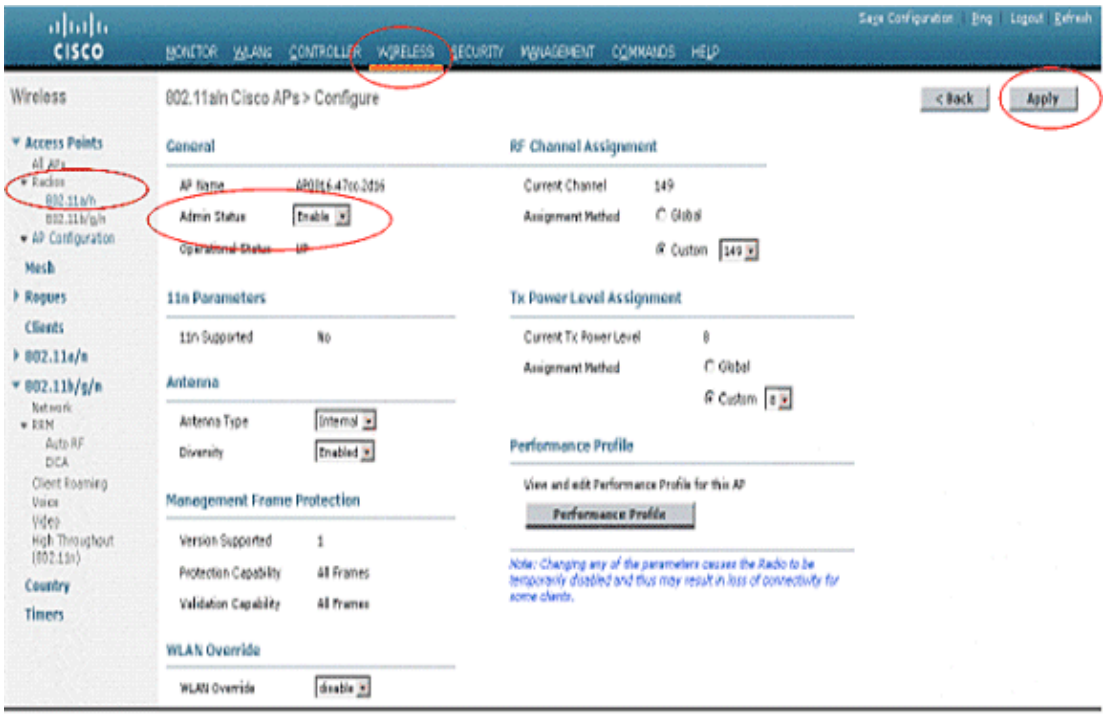
Configuration of Access Point for Netlink Telephones that Operate in 802.11a Mode

Perform these procedures:

1. From the main menu, click **Wireless.**
2. In the navigation pane, under **Access Points**, choose **Radios**, and then choose **802.11a /n**. All the APs that are connected must be listed and show their Operational Status as UP.
3. Choose **Configure** from the drop−down list for the access point that you wish to change.



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

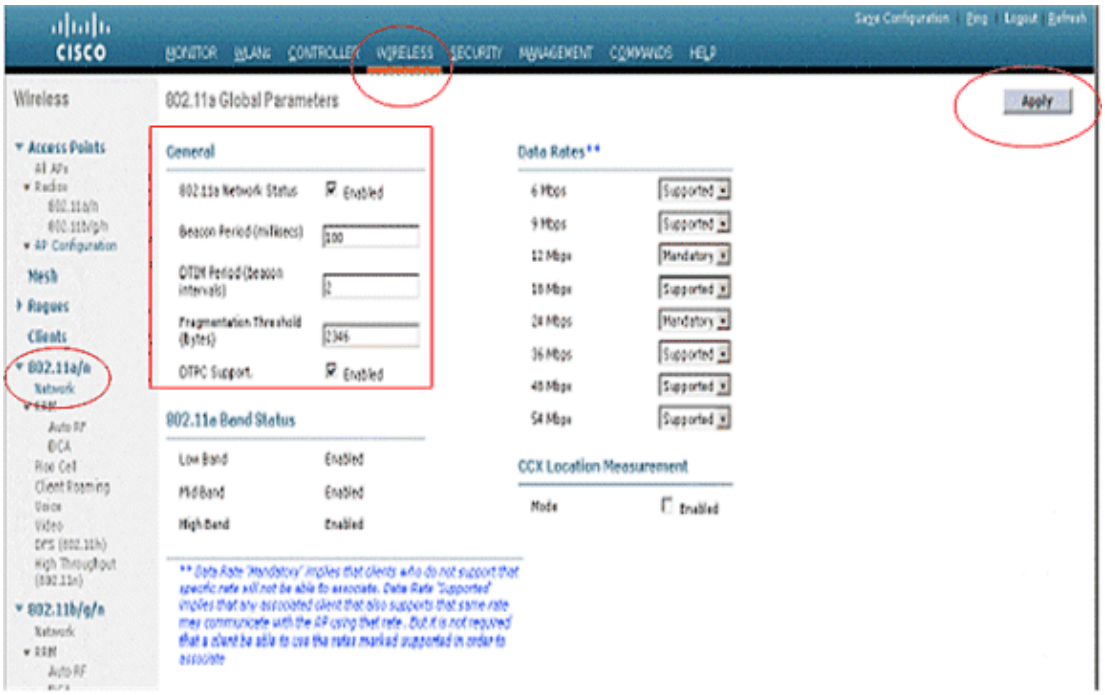


7. In the navigation pane under **802.11a/n**, choose **Network**.
8. For **802.11a Network** Status, click the **Enabled** check box.
9. For setting up the Data Rates, consult the RF site survey of your facility that is designed for voice traffic to determine if you have sufficient coverage to support all data rates. NetLink wireless telephones require this minimum dBm reading to support the correspondent Mandatory data rate setting in the access point.

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11b	-70 dBm	1 Mb/s
	-60 dBm	11 Mb/s
802.11g	-63 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

10. Use the default Fragmentation Threshold (2346 bytes).
11. Set the Beacon Period to **100**.
12. Set the DTIM Interval to **2** .
13. NetLink handsets do not support dynamic power and do not utilize the information element that is set when the DTPC Support is enabled. NetLink handset power must be configured to match the highest transmit power of the APs.
14. Click the **Apply** button to save the settings.

This is a screenshot that explains steps 7 to 13.



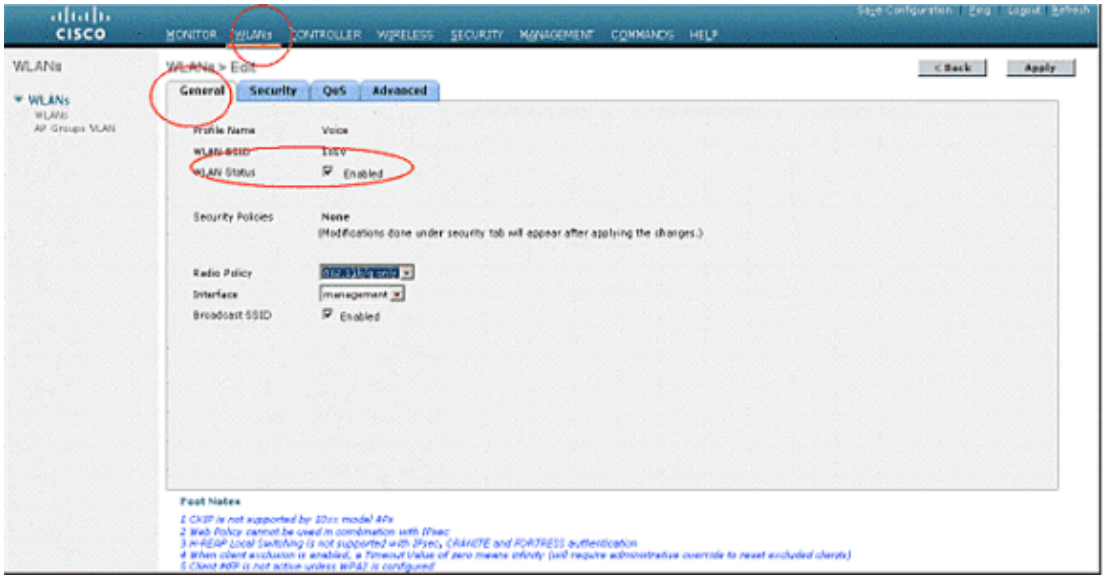
SSID Configuration

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 QoS, and the data SSID must be set to Silver for QoS.

1. From the main menu, click **WLANs**.
2. In the **WLANs** screen, click the **New**&. button.

3. Enter the Profile Name and SSID.
4. Click the **Apply** button.

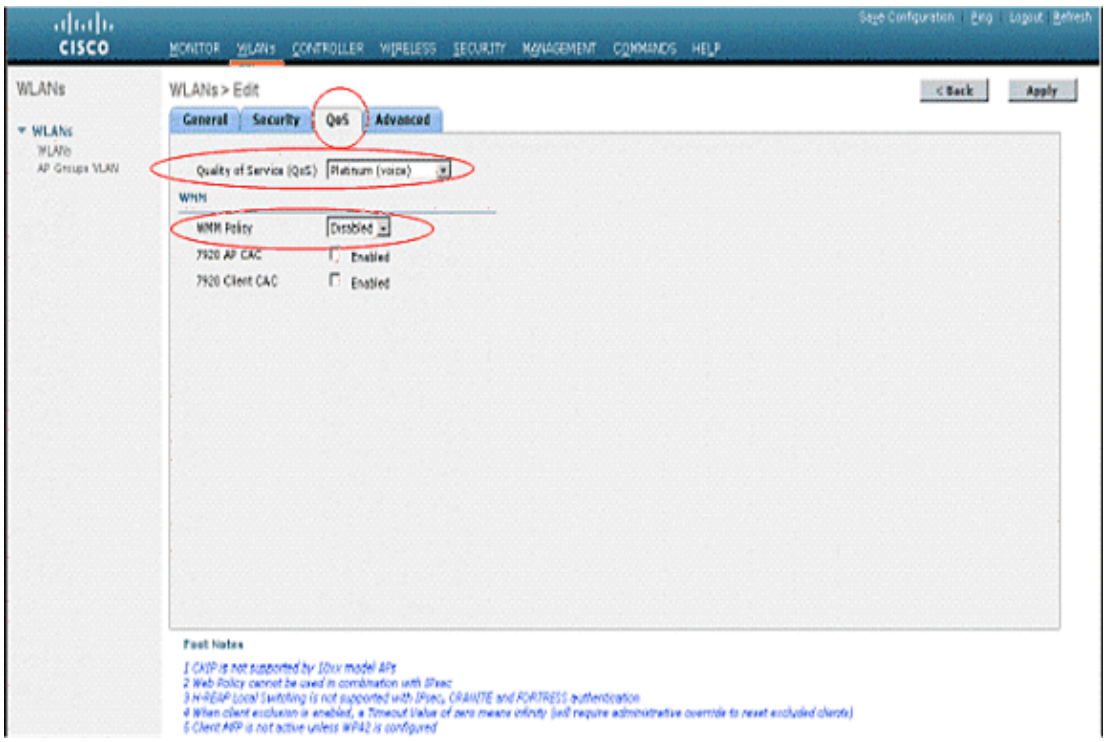
5. Choose the Profile Name for the voice SSID.
6. Under the **General** tab, set the Radio Policy to **802.11b/g or 802.11a**, dependent upon the radio settings of the NetLink wireless telephone.
7. Enable WLAN Status.



8. Under the QoS tab, set Quality of Service to **Platinum**.

   Note: This is the required setting for voice traffic.
9. Set WMM Policy to **Disabled**.

   Note: This is required for usage with NetLink handsets.

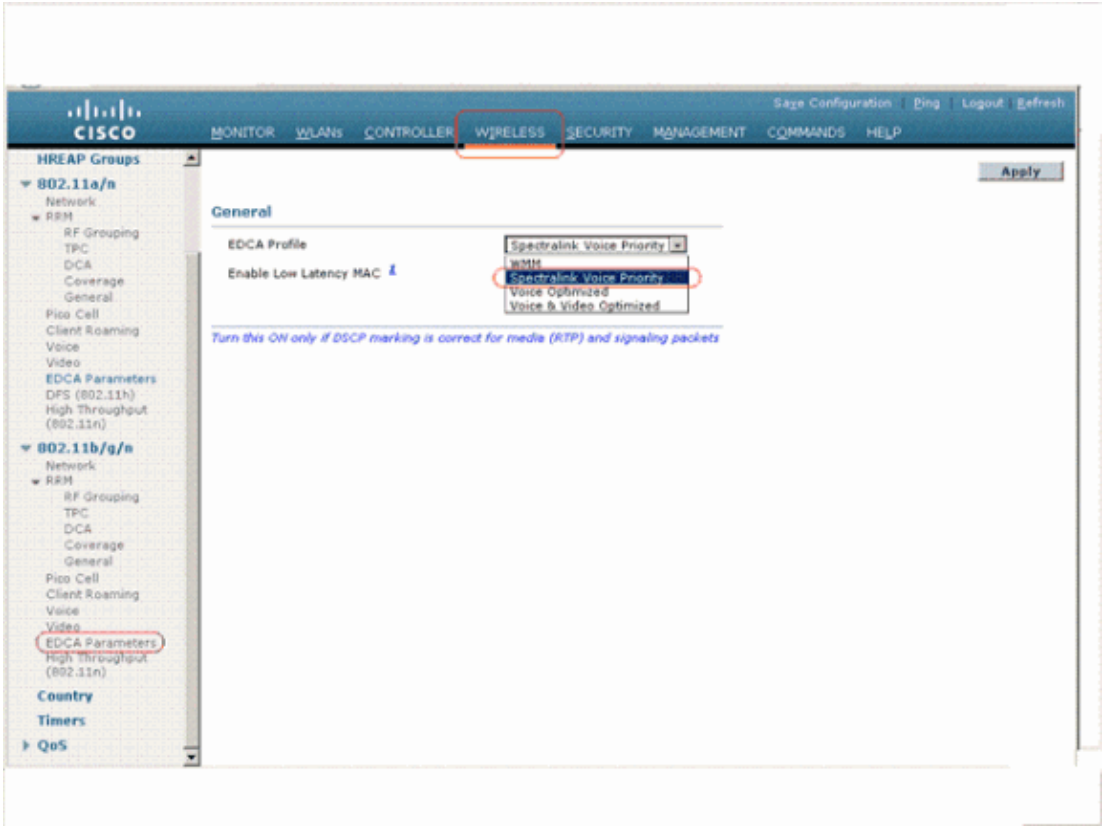


10. Click the **Apply** button to save all changes.

Enable EDCF for the Spectralink Phone

Complete these steps in order to enable EDCF for the spectralink phone:

1. From the WLC GUI , click **Wireless**.
2. Choose **802.11 b/g/n** or **802.11 a/n** from the list of options available in the left hand side.
3. From the EDCA profile, choose **Spectralink Voice Priority**.
4. Click **Apply** in order to save the changes.



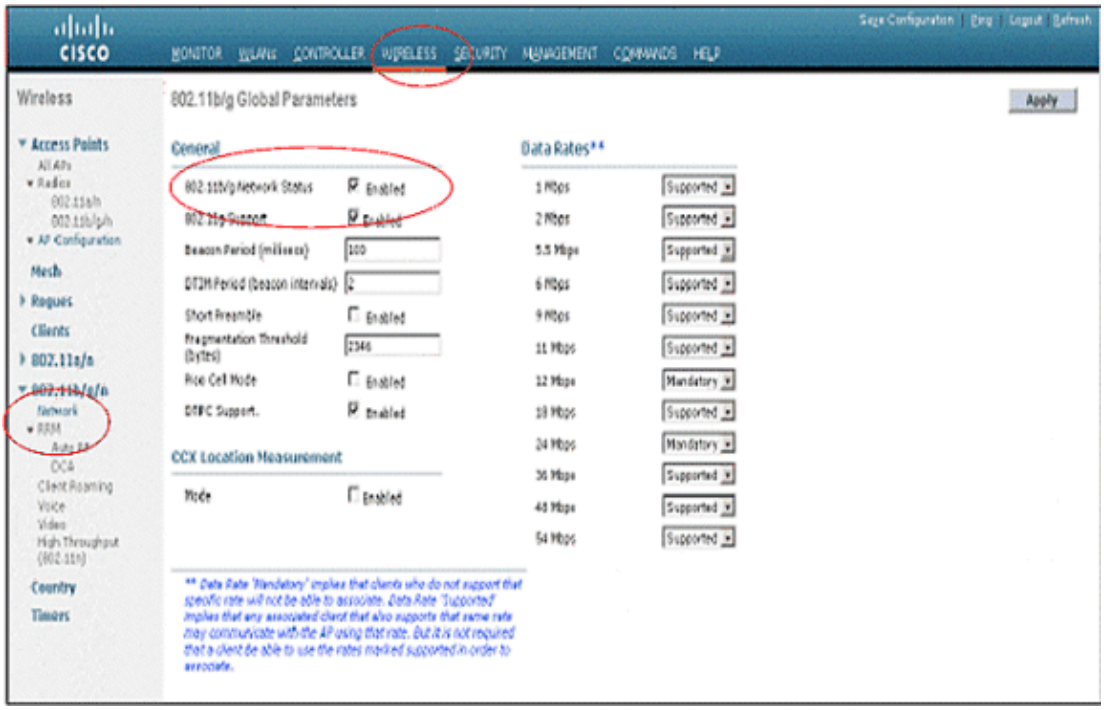
Enable SVP on the Controller and Access Points

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

1. Use a console cable to access the controller CLI. In admin mode, enter **config advanced edca−parameters svp−voice**. This command will enable QoS for SpectraLink packets.
2. In order 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, click **Wireless.**
4. In the navigation pane, **under 802.11b/g/n or 802.11a/n**, (dependent upon NetLink handset radio configuration) choose **Network**.
5. Disable the **802.11b/g Network Status or 802.11a Network Status** (dependent upon the NetLink handset radio configuration) and click the **Apply** button.
6. Re−enable the **802.11b/g Network Status or 802.11a Network Status** (dependent upon the NetLink handset radio configuration) and click the **Apply** button.
7. In order to verify that 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 displays this 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
```



Wireless IP Telephony Verification

After you conduct an RF site survey and configure the APs and the phones, it is crucial to conduct verification tests in order to ensure that everything works as desired. Perform these tests at all these locations:

- The primary area of each AP cell (where the phones will most likely connect to that particular AP)
- Any location where there may be high call volume
- Locations where usage may be infrequent but coverage still must be certified (for example, stairwells and restrooms)
- At the fringes of the AP coverage area

You can perform these tests in parallel or series. If you perform the tests in parallel, ensure that the phones are turned off between testing points in order to test full association, authentication, and registration at each location. Roaming and load tests must, of course, be the final tests.

Association, Authentication, and Registration

This section explains how to verify that the phone properly associates, authenticates, and registers properly.

1. At multiple points throughout the environment, power up the phone and verify association with the AP.

   If the phone does not associate with the AP, perform these checks:

   a. Check the phone configuration in order to ensure the proper service set identifier (SSID), authentication type, and so forth.
   b. Check the WLC configuration in order to ensure the proper SSID, authentication type, radio channels, and so forth.

c. Check your site survey in order to ensure that the location has adequate RF coverage.

2. At multiple points throughout the environment, ensure that the phone authenticates through the AP successfully.

   If the client does not authenticate, check either the WEP key or the LEAP user name and password on the phone. Also, check the user name and password on the authentication, authorization, and accounting (AAA) server with use of a wireless laptop with identical credentials.
3. At multiple points throughout the environment, ensure that the phone registers with the SVP server and receives the proper phone number.

   If the client does not register, perform these checks:

   a. Verify that the phone has the correct IP Address, Subnet Mask, Primary Gateway, Primary TFTP, Primary/Secondary and Domain Name System (DNS).
   b. Perform phone calls and load testing.
   c. Verify that calls can be placed successfully from the IP phone with acceptable voice quality.

   The remainder of this section explains how to perform this verification.
4. Check stationary phone calls.

   At multiple points throughout the environment, while you stand still, make a phone call to a wired phone and conduct 60− to 120−second voice tests in order to check voice quality. If the voice quality is unacceptable, make a call with the wired phone and determine if the voice quality is acceptable. If the voice quality is not acceptable, verify the wired network design against the guidelines.
5. Use the site survey tools in order to verify that there is not more than one AP per RF channel from that location with a signal strength (RSSI) of greater than 35 dBm.

   If there are two APs present on the same channel, ensure that the SNR is as high as possible in order to minimize interference. For instance, if the stronger AP has an RSSI of 35 dBm, ideally, the weaker AP should have an RSSI of less than 20 dBm. In order to achieve this goal, you may have to reduce the transmit power of one AP or move the AP.
6. Check the QoS settings on the AP in order to confirm the proper recommended settings.
7. Check roaming phone calls.

   Place a call to a wired IP phone and continually check the voice quality while you traverse the total wireless coverage area. Cisco recommends the use of an earpiece so that you can test the voice quality while you look at the site survey information on the phone. If the voice quality is insufficient, complete these steps:

   a. Listen for all unacceptable changes in voice quality and take note of the values in the phone site survey.
   b. Watch and listen for the phone to roam to the next AP.
   c. Note the other available APs in the site survey in order to check coverage and interference.
8. Make adjustments to the AP placement and settings in order to fine−tune the WLAN, and perform these checks in order to ensure voice quality:

   a. Use the site survey tools in order to verify that there is not more than one AP per channel with an RSSI value of greater than 35 dBm in any given location.

      Ideally, all other APs on the same channel should have RSSI values that are as low as possible (preferably less than 20 dBm). At the border of the coverage area where the RSSI is 35 dBm, the RSSI for all other APs on the same channel should ideally be less than 20 dBm.
   b. Use the site survey tools in order to verify that there are at least two APs (total, on separate channels) that are visible in all locations and have sufficient signal strength.

c. Check that the APs in a given roaming area are all on a Layer 2 network.

Load Testing

Complete these steps:

1. Gather a sampling of all the planned wireless phone users and equip them with the SpectraLink phones.
2. Have up to 10 users begin to make phone calls in a given area.

   Note: SpectraLink documentation suggests that a Cisco AP should handle 10 calls.
3. Have the users start to move apart while they place new calls.

   Continue to check voice quality during this process.

Common Roaming Issues

These roaming issues can occur:

- The phone does not roam when it is placed directly under an AP.
- The phone is most likely not reaching the roaming differential thresholds for the RSSI and channel utilization (CU).

  Adjust the power settings on the APs.
- The phone does not receive beacons or probe responses from the AP.
- The phone roams too slowly.

Phone Loses Connection When Roaming

Perform these checks:

- Check authentication for a possible WEP mismatch.
- The phone is capable of seamless Layer 2 roaming only (unless a Layer 3 mobility mechanism is configured). Therefore, ensure that the new AP does not serve a different IP subnet.
- If you use LEAP, check that the TCP ports are not blocked by filters on the AP. If you use ACS, the port for authentication can be 1645 or 1812. Other RADIUS servers typically use port 1812.
- Verify that the associated AP/controller has IP connectivity to the SVP server and SVP gateway.
- Check the RF signal strength.

Phone Loses Voice Quality While Roaming

Check for these issues:

- Check for a low RSSI on the destination AP.
- Channel overlap can be insufficient. The phone must have time to hand off the call smoothly before the phone loses its signal with the original AP.
- The signal from the original AP may be lost.

Audio Problems

There are a few common configuration errors that can cause some easily resolved audio issues. If possible, check audio problems against a wired phone in order to help narrow the problem to a wireless issue. Common audio problems include:

- No audio
- One−sided audio
- Choppy or robotic audio
- Registration and authentication problems

No Audio

A common reason for no audio is that Temporal Key Integrity Protocol (TKIP) and/or Message Integrity Check (MIC) are configured on the AP and not on the phone.

One−Sided Audio

These are potential causes of one−sided audio:

- The problem can occur in the fringe areas of an AP, where a signal can be too weak on either the phone side or the AP side. When possible, match the power settings on the phone and the AP in order to try to fix this problem. This problem is most common when the variation between the AP setting and the phone setting is large (for example, 100 mW on the AP and 20 mW on the phone).
- Check the gateway and the IP routing for voice quality.
- Check to see if a firewall or Network Address Translator (NAT) is in the path of the RTP packets. By default, firewalls and NATs cause one−way audio or no audio. Cisco IOS® Software and PIX NATs and firewalls have the ability to modify those connections so that two−way audio can flow.
- One−way audio can occur if ARP caching is not configured on the AP.

Choppy or Robotic Audio

These are potential causes of choppy or robotic audio:

- A common reason for choppy or robotic audio is when a microwave operates nearby. Microwaves start at channel 9 and can extend from channels 6 to 14.
- If there is a specific data rate set on the phone or AP, the rates must match or the phone must be set to its default of automatic.
- Set the AP to enable the appropriate data rate for legacy devices.

Registration and Authentication Problems

When you encounter problems with authentication, perform these checks:

- Check the SSIDs in order to be sure that they match on the phone and the AP (or network). Also, be sure that the network has a route to the SVP server.
- Check the WEP keys in order to be sure that they match. It is a good idea to reenter them on the phone because a typing error is easy to make when you enter a WEP key or password.

These messages or symptoms can occur:

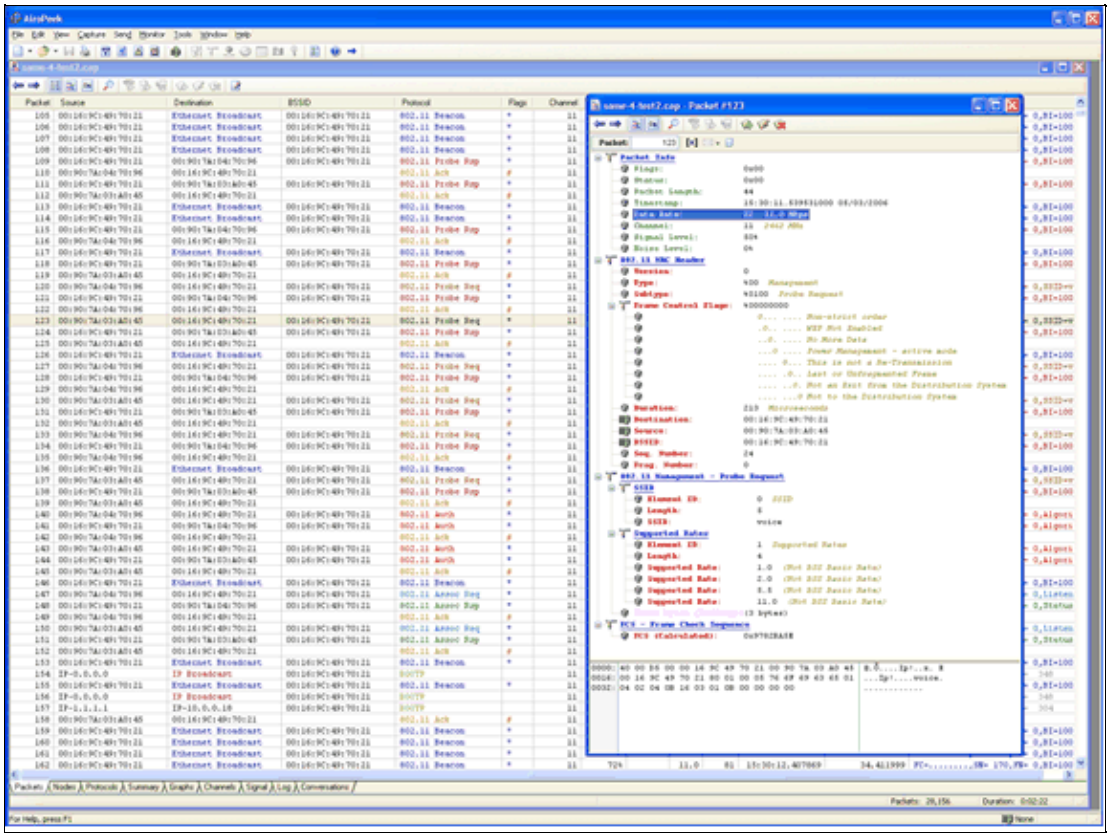
- Registration Rejected This error is most likely a SVP gateway issue.
- Cannot Support All Requested Capabilities There is most likely an encryption mismatch between the AP and the client.
- Authentication Failed/No AP Found Ensure that the authentication types match on the AP and client.
- No Service IP Config Failed If you use static WEP, ensure that the keys are configured correctly. Ensure that other clients can receive DHCP with use of the same SSID.
- Deauthenticate all TKIP clients from AP This problem happens when the AP detects two MIC errors within 60 seconds. This countermeasure keeps all TKIP clients from reauthenticating for 60 seconds.

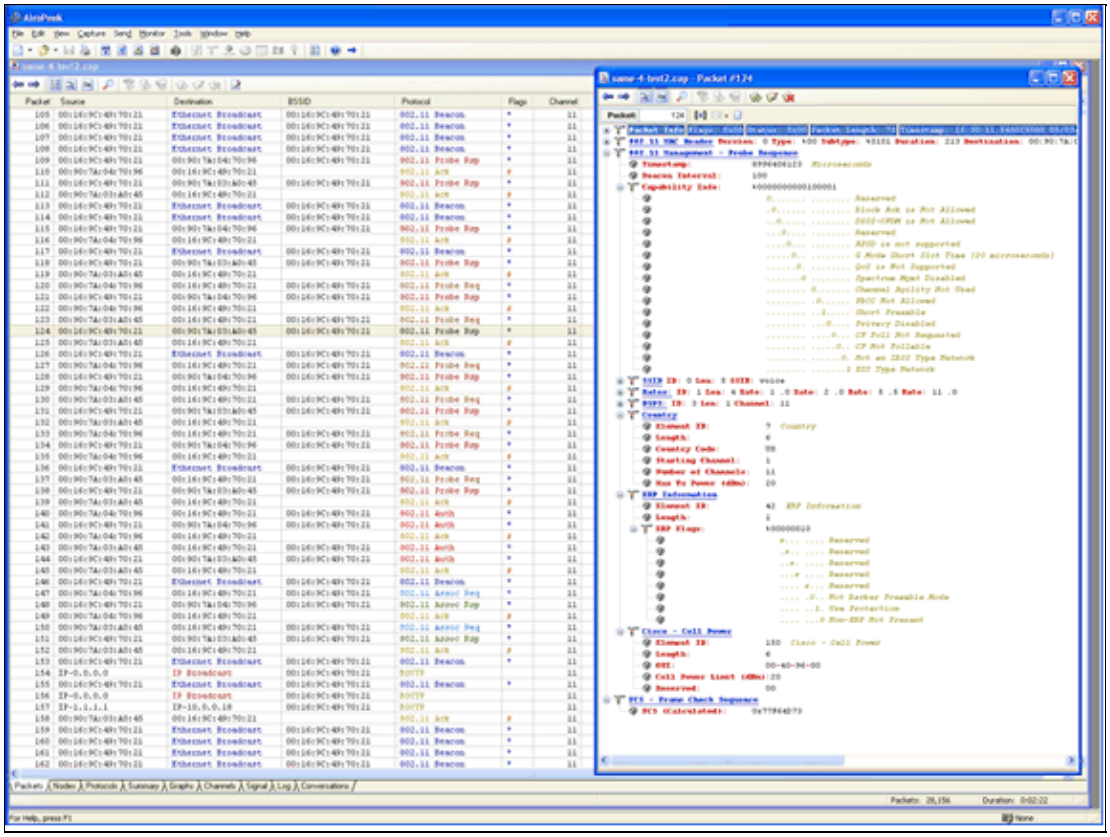
- Reauthentication/Session timeout If it is configured, a session timeout triggers a reauthentication, which causes gaps in the voice stream (300 ms + the WAN delay for IEEE 802.1x authentication).

Appendix A

Packet Traces

Figure 8 Probe Request from the SpectraLink i640 Phone

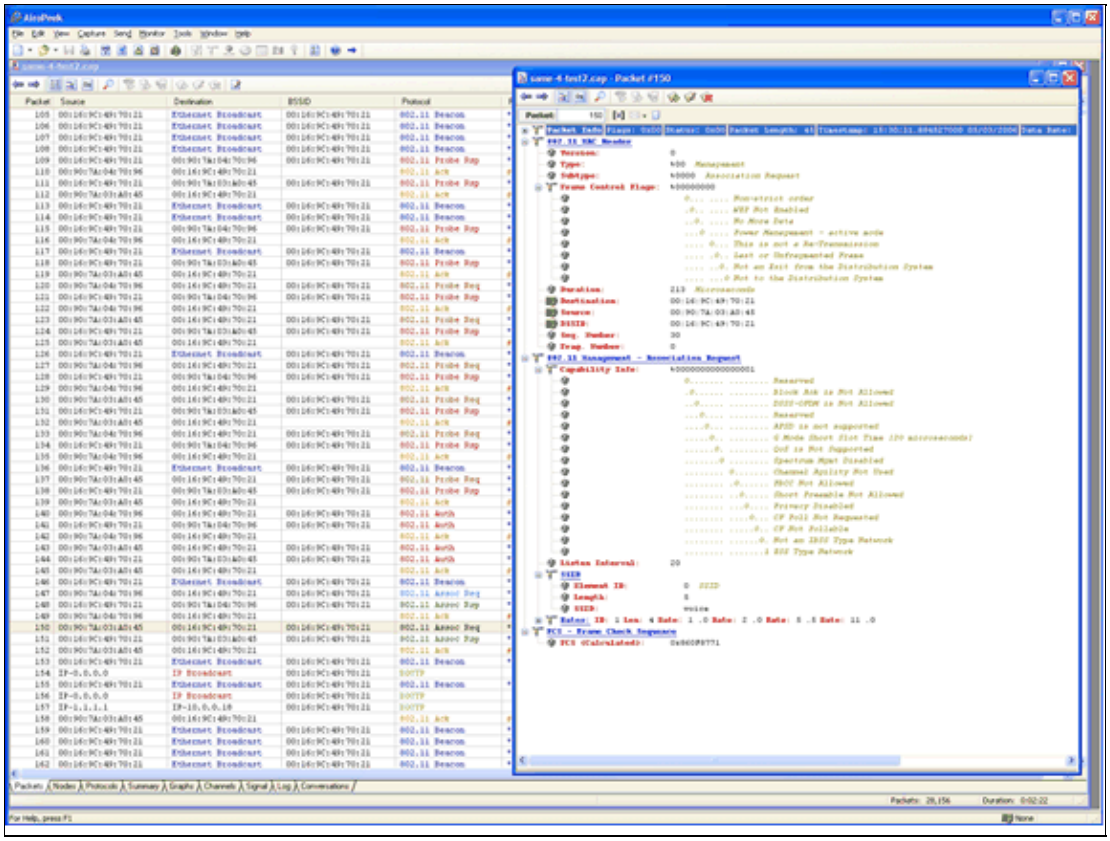




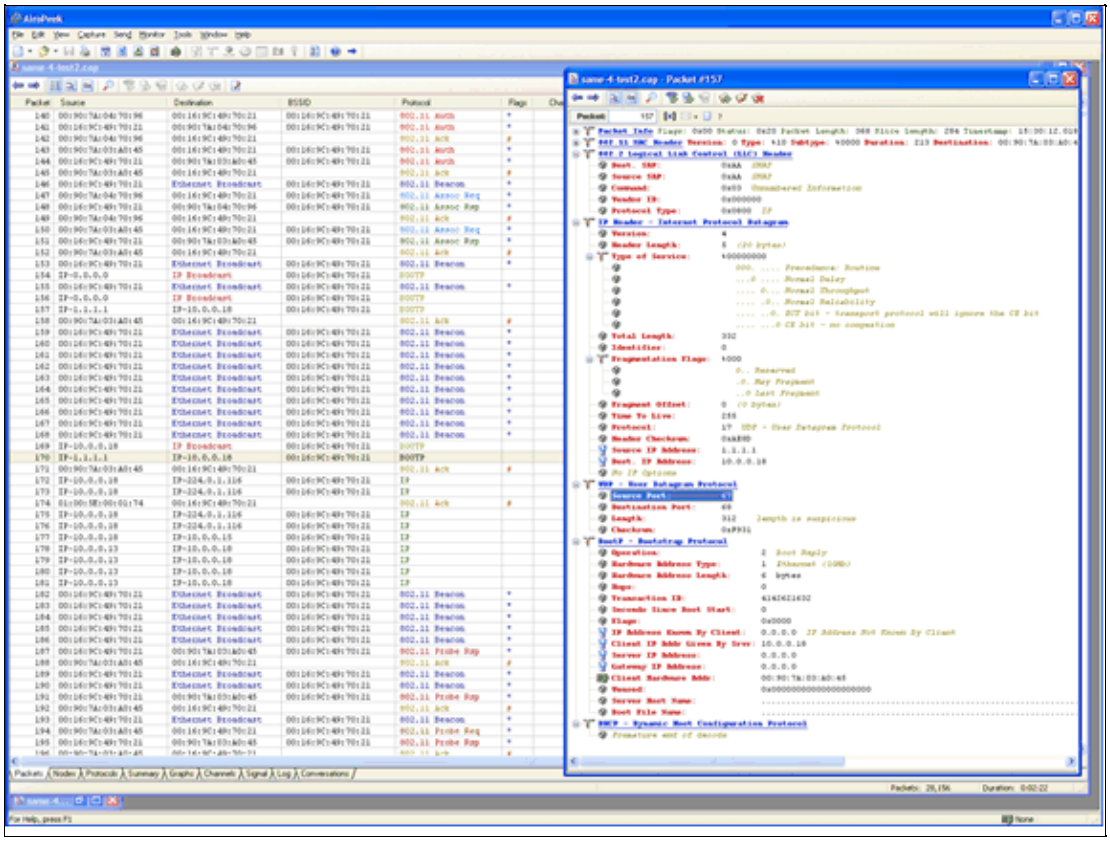
Probe Response from the LWAPP AP

The response is very ordinary. But even after the SpectraLink phone sends an acknowledgment (ACK) to the probe response, it sends five more probe requests to the same AP and then acknowledges the five probe responses from that AP. The reason for this behavior is unknown but is not typical of 802.11 clients.

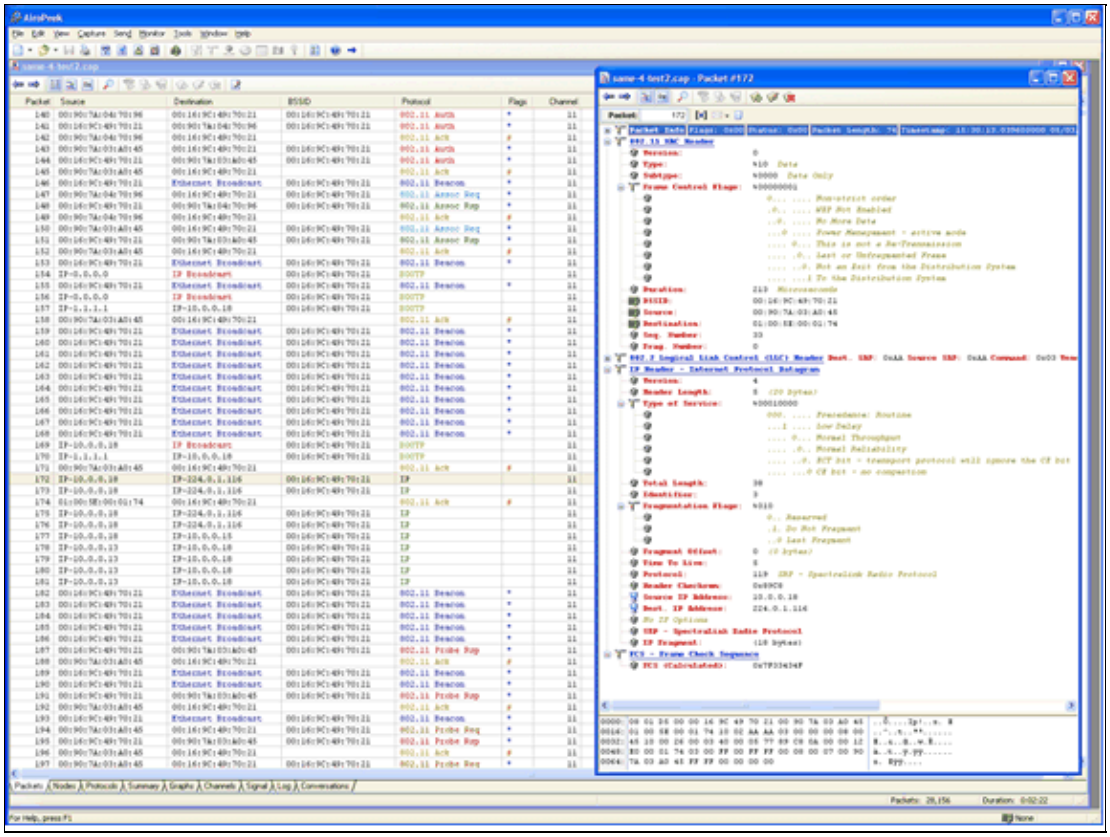
An association request is sent that indicates that the QoS is not supported, and the AP responds in kind. The i640 replies to the association response with an ACK.



The i640 does a Bootstrap Protocol (BOOTP) in order to get a DHCP−assigned address. The "voice" interface created on the controller for the SpectraLink phones responds with an IP address of "10.0.0.18" for the MAC address of the phone (00:90:7a:03:a0:45).



The i640 then seeks acknowledgment of the multicast address created on the **controller**.

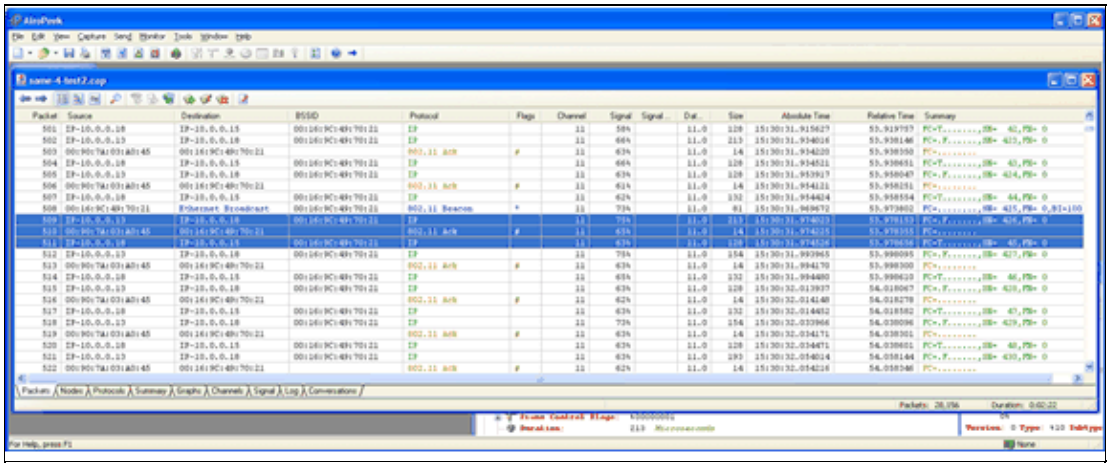


The i640 then communicates with the SpectraLink gateway (10.0.0.15) and the SpectraLink server (10.0.0.13).

This table shows packet sequences during a phone call and the device addresses:

Device	IP Address	MAC Address
SVP server	10.0.0.13	00:90:74:04:22:24
SVP gateway−PBX	10.0.0.15	00:90:74:02:49:63
Phone	10.0.0.17	00:90:7a:03:70:96
Phone	10.0.0.18	00:90:7a:03:a0:45
AP		00:16:9c:49:70:21

A "voice" packet that is sent from the SVP server to an SVP phone is sent with the IP address of the SVP server. When the SVP phone receives that "voice" packet, the phone sends an 802.11 RF−level ACK to the MAC address of the AP, and then sends a 128−byte IP packet to the IP address of the SVP gateway. The 128−byte packet does not seem to provide any data and seems to act as an SVP protocol acknowledgment. Typical RTP protocol does not do packet acknowledgments.



This is a redisplay of the 3 packets that are highlighted in blue in the example window:

Figure 9 Redisplay of the Highlighted Packets

508	00:16:9C:49:70:21	Ethernet Broad...	00:16:9C:49:70:21	802.11 ...	81	15:30:31.969672
509	IP-10.0.0.13	IP-10.0.0.18	00:16:9C:49:70:21	IP	213	15:30:31.974023
510	00:90:7A:03:A0:45	00:16:9C:49:70:21		802.11 Ack	14	15:30:31.974225
511	IP-10.0.0.18	IP-10.0.0.15	00:16:9C:49:70:21	IP	128	15:30:31.974526

Appendix B

AP and Antenna Placement

This section gives examples of both proper and improper placement of APs and antennas.

Figure 10 shows the improper placement of an AP and antennas close to an I−beam, which creates distorted signal patterns. Signal waves cross and create an RF null point, and the reflection of signal waves creates multipath distortion. This placement results in very little coverage behind the AP and reduced signal quality in front of the AP.

Figure 10 Improper Placement of Antennas Near an I−Beam

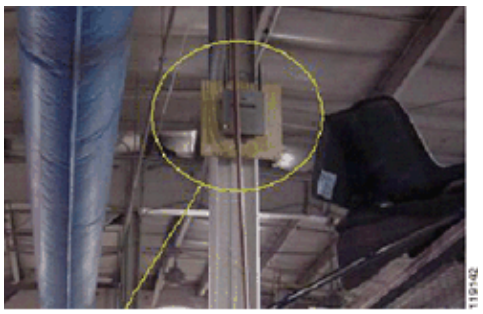
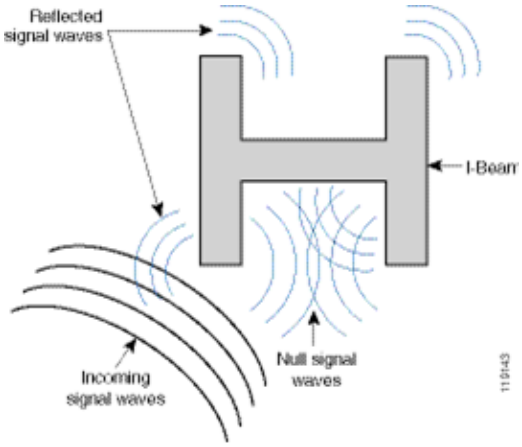


Figure 11 shows the signal propagation changes or distortions that an I−beam causes. The I−beam creates many reflections from both received packets and transmitted packets. The reflected signals result in very poor signal quality because of null points and multipath interference. However, the signal strength is high because the AP antennas are so close to the I−beam.

Figure 11 Signal Distortions Caused by the Placement of Antennas Too Close to an I−Beam

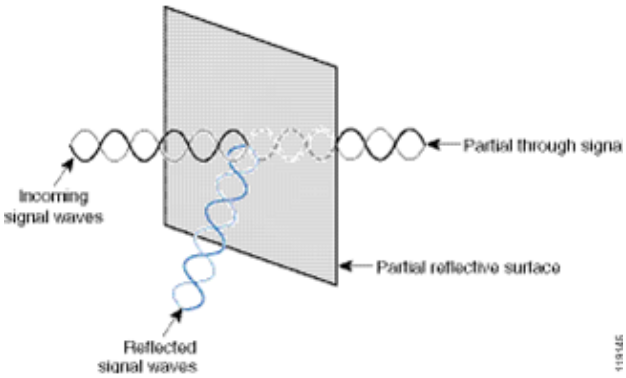


The AP and antenna placement in Figure 12 is better because the placement is away from the I−beams and there are fewer reflected signals, fewer null points, and less multipath interference. This placement is still not perfect because the Ethernet cable should not be coiled up so close to the antenna. Also, in this situation, you can turn the AP so that the 2.4−GHz antennas point to the floor in order to provide better coverage directly below the AP. There are no users above the AP.

Figure 12 AP and Antennas Mounted on a Wall, away from I−Beams

Figure 13 shows the signal propagation that the wall on which the AP is mounted causes.

Figure 13 Signal Reflection That a Wall Causes



These three AP/antenna placement examples also apply to the placement of APs and antennas in or near the ceiling in a standard enterprise environment. If there are metal air ducts, elevator shafts, or other physical barriers that can cause signal reflection or multipath interference, Cisco highly recommends that you move the antennas away from those barriers. In the case of the elevator, move the antenna a few feet away in order to help eliminate the signal reflection and distortion. The recommendation is the same with air ducts in the ceiling.

A survey that is conducted without sending and receiving packets is not sufficient. The I−beam example shows the creation of null points that can result from packets that have CRC errors. Voice packets with CRC errors are missed packets that adversely affect voice quality. In this example, those packets can be above the noise floor that is measured with a survey tool. Therefore, the site survey *must*, not only measure signal levels, but also generate packets and then report packet errors.

Figure 14 shows a Cisco Aironet 1200 AP that is properly mounted to a ceiling T−bar, with the antennas in an omnidirectional position.

Figure 14 Aironet 1200 AP Mounted to a Ceiling

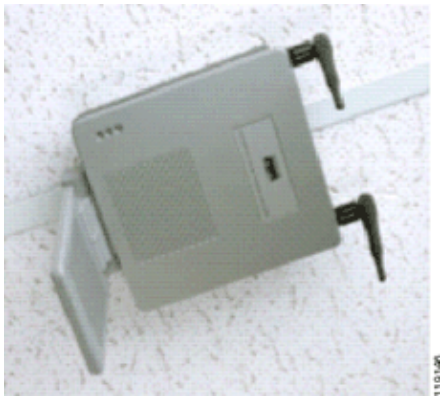


Figure 15 shows an Aironet 5959 omnidirectional diversity antenna that is properly mounted to a ceiling T−bar. In this case, the 1200 AP is mounted above the ceiling tile.

Figure 15 Aironet 5959 Antenna Mounted to a Ceiling

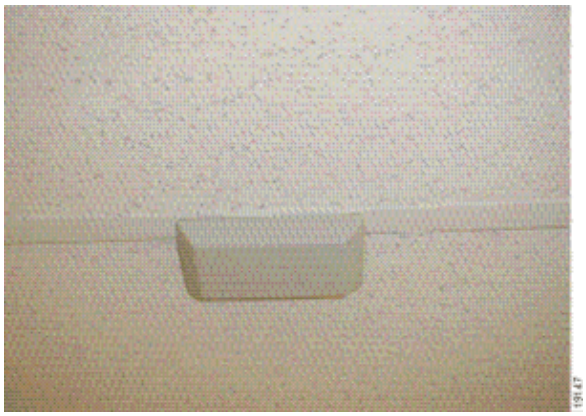


Figure 16 shows a 1200 AP that is properly mounted to a wall.

Figure 16 Aironet 1200 AP Mounted to a Wall

Figure 17 shows the Aironet 2012 diversity patch antenna that is mounted to a wall. In this case, the 1200 AP is mounted above the ceiling tile.

Figure 17 Aironet 2012 Antenna Mounted to a Wall

For areas where user traffic is high (such as office spaces, schools, retail stores, and hospitals), Cisco recommends placement of the AP out of sight and the placement of unobtrusive antennas below the ceiling. Separation for nondiversity antennas should not exceed 18 inches.

Interference and Multipath Distortion

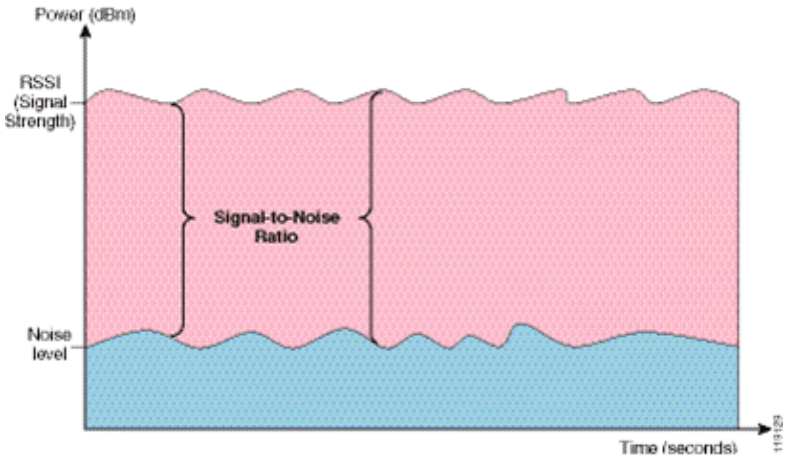
The throughput performance of the WLAN network is affected by unusable signals. Devices that generate WLAN interference include:

- Microwave ovens
- 2.4−GHz cordless phones
- Bluetooth devices
- Other electronic equipment that operates in the 2.4−GHz band

Interference also typically comes from other APs and client devices that belong in the WLAN but that are far enough away that their signal is weakened or has become corrupted. APs that are not part of the network infrastructure can also cause WLAN interference and are identified as rogue APs.

Interference and multipath distortion cause the transmitted signal to fluctuate. Interference decreases the SNR for a particular data rate. Packet retry counts go up in an area where interference and/or multipath distortion are high. Interference is also referred to as the noise level or noise floor. The strength of the received signal from its associated AP must be high enough above the receiver noise level to be decoded correctly. This level of strength is referred to as the SNR. The ideal SNR for the NetLink phone is 25 dB. For example, if the noise floor is 95 dBm and the received signal at the phone is 70 dBm, the SNR is 25 dB. See Figure 18.

Figure 18 SNR



A change in the type and location of the antenna can reduce multipath distortion and interference. Antenna gain adds to the system gain and can reduce interference if the interfering transmitter is not directly in the boresight of the directional antenna.

While directional antennas can be of great value for certain indoor applications, the vast majority of indoor installations use omnidirectional antennas. Directionality should be strictly determined by a correct and proper site survey. Whether you use an omnidirectional or patch antenna, indoor environments require diversity antennas to mitigate multipath distortion. The Aironet Series AP radios allow for diversity support.

Signal Attenuation

Signal attenuation or signal loss occurs even as the signal passes through air. The loss of signal strength is more pronounced as the signal passes through different objects. A transmit power of 20 mW is equivalent to 13 dBm. Therefore, if the transmitted power at the entry point of a plasterboard wall is at 13 dBm, the signal strength is reduced to 10 dBm when it exits that wall. This table shows the likely loss in signal strength that various types of objects cause:

Object in Signal Path	Signal Attenuation Through Object
Plasterboard wall	3 dB
Glass wall with metal frame	6 dB
Cinder block wall	4 dB
Office window	3 dB

Metal door

6 dB

Metal door in brick wall

12 dB

Human body

3 dB

Each site that is surveyed has different levels of multipath distortion, signal loses, and signal noise. Hospitals are typically the most challenging environments to survey because of high multipath distortion, signal losses, and signal noise. Hospitals take longer to survey, require a denser population of APs, and require higher performance standards. Manufacturing and shop floors are second in terms of the survey difficulty that they present. These sites generally have metal siding and many metal objects on the floor, which result in reflected signals that create multipath distortion. Office buildings and hospitality sites generally have high signal attenuation but a lesser degree of multipath distortion.

Related Information

- **Cisco Unified Wireless Network**
- **Cisco Unified Wireless Network: Reducing Large−Scale Enterprise Wireless LAN TCO**
- **Cisco IP Telephony Solution Reference Network Design (SRND) for Cisco CallManager 4.0 and 4.1**
- **Cisco Wireless IP Phone 7920 Design and Deployment Guide**
- **Wireless Site Survey FAQ**
- **Troubleshooting Problems Affecting Radio Frequency Communication**
- **Troubleshooting Connectivity in a Wireless LAN Network**
- **Deploying Cisco 440X Series Wireless LAN Controllers**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jul 17, 2008 Document ID: 70442