Cisco on Cisco Best Practices
Cisco Wireless LAN Design

Contents

Disclaimer

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE DESIGN RECOMMENDATIONS AND CONFIGURATIONS PROVIDED IN THIS DOCUMENT ARE SPECIFIC TO CISCO IT REQUIREMENTS. CISCO SYSTEMS DOES NOT ENDORSE OR APPROVE THE CONFIGURATIONS TO BE USED FOR ANY CUSTOMER. THE DESIGN STANDARDS PROVIDED HERE ARE MERELY PROVIDED TO SHARE CISCO IT BEST PRACTICES. EACH AND EVERY CUSTOMER REQUIREMENT WOULD BE DIFFERENT AND HENCE THOROUGH ANALYSIS AND RESEARCH SHOULD BE DONE BEFORE APPLYING ANY DESIGN STANDARD.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL INFORMATION IS PROVIDED “AS IS” WITH ALL FAULTS. CISCO DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

1. Overview

This document describes the technical specifics, standard configurations, and layouts of the 802.11 wireless LAN implemented across Cisco Systems' global corporate network. This document explains the baseline design and configuration for the network; it briefly touches upon the wireless infrastructure standards involved with enhanced services, such as voice over wireless and wireless guest hotspot. Detailed technical information about these enhanced wireless solutions will be covered in separate documents.

2. Architecture

2.1. Wireless LAN Architecture

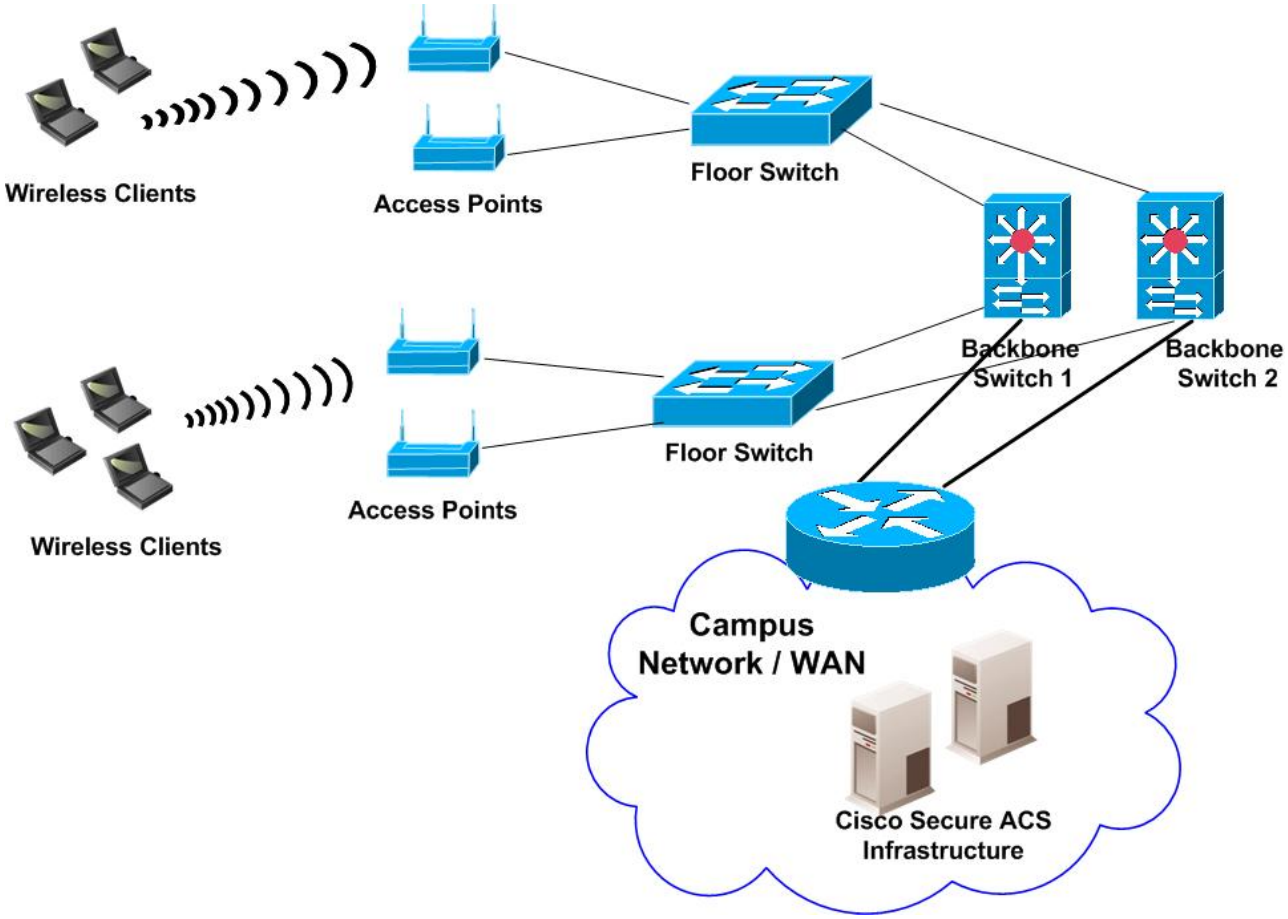
While Cisco IT constantly evaluates new products and technologies, the global configuration of the company's Aironet® access points adheres to the following standards.

- Use of a single-radio SSID globally to allow easy migration from one theatre to another.
- Fixed 11 Mbps for best throughput configured on the access point.
- Design criteria ratio of 25:1 users per access point.
- Use of strong security measures, including 802.1X-based Extensible Authentication Protocol (EAP) authentication, dynamic key rotation, Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC), and Broadcast Key Rotation (BKR).
- One wireless VLAN that spans an entire building, allowing users to roam within the Layer 2 domain.
- Nonoverlapping channels and cell size that can be adjusted using transmit power on the access point via site survey.
- Use of existing IDF switches where possible to provide the access point uplink.
- Inline power.
- Asynchronous console access to all access points.

Detailed information on each of these features as deployed by Cisco IT is available in the wireless LAN case study at:
http://www.cisco.com/web/about/ciscoitatwork/downloads/ciscoitatwork/pdf/Cisco_IT_Case_Study_Wireless_LAN_2004.pdf

Figure 1 shows a simple connection for a two-storied building.

Figure 1. Sample Office WLAN Architecture



3. Solution Design

This section provides an overview and recommended configurations to use for specific components of a Wireless LAN.

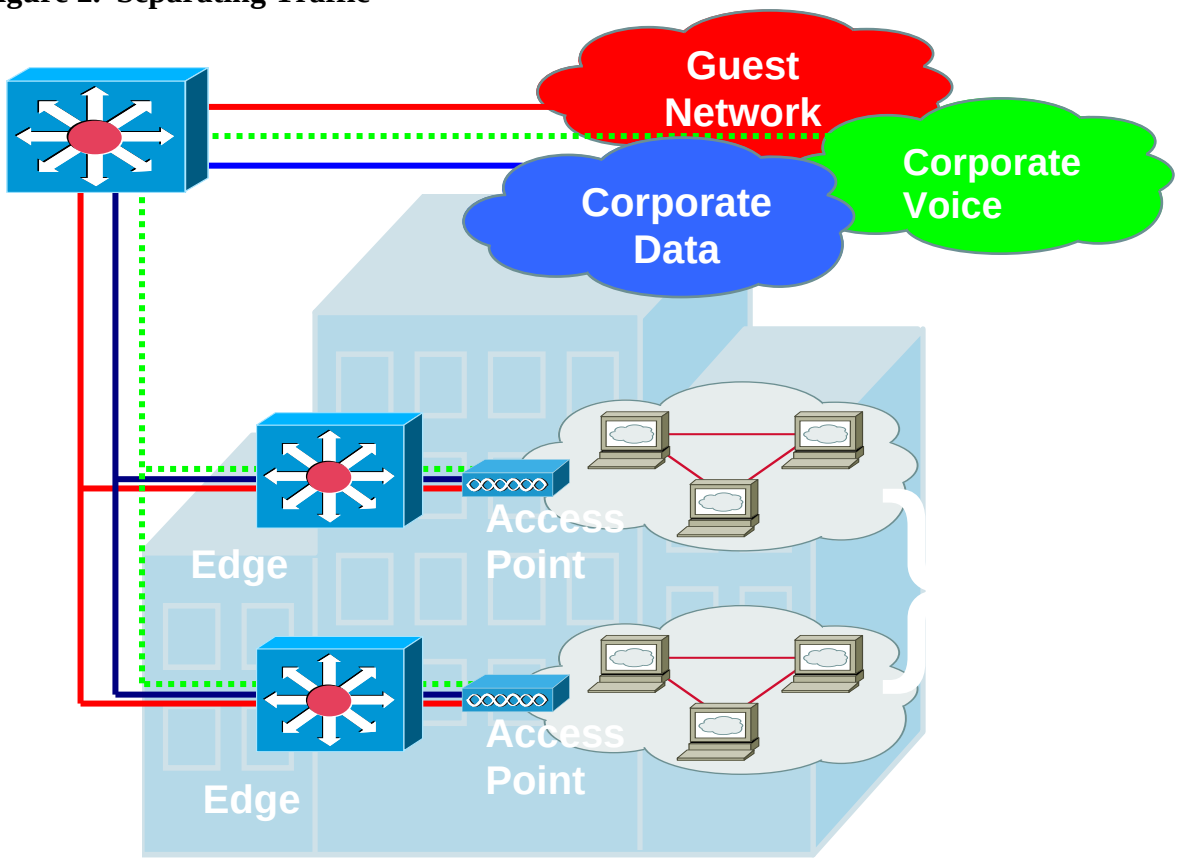
- Connection to the Wired LAN Network
- Wireless SSID
- User Roaming
- Multi-Data Rate
- VLAN Standards
- Wireless Security
- Wireless Management
- Other Design Considerations
- Wireless Client Configuration
- Link Status Meter (LSM)
- Cisco Aironet Client Monitor
- Network Login
- Coverage Check
- Roaming

2.2. Access Point Configuration

2.2.1. Connection to the Wired LAN Network

This section presents an overview of the connection to the network switch. Traffic through the access point is separated into three categories: corporate data network, guest network, and corporate voice network (Figure 2). In locations that have wireless voice deployed, an additional voice VLAN and a voice SSID are configured.

Figure 2. Separating Traffic



Access points are connected to the Cisco Catalyst® access switches through 100BASE-T Ethernet. The standard limitations of Fast Ethernet are taken into consideration and the maximum cable length is kept less than 100 meters. Fixed IP addresses are allocated for the access points for management purposes only. Every Ethernet-connected access point role is to be set as “access point” to allow communication with wireless clients while prohibiting associating with other access points also configured as “access point/root” over wireless. This port is part of the console network and is used for managing the access point, which is connected to the switch in the same manner as the laptop/desktop users. Port fast is enabled on the uplink ports on the access switch with Bridge Protocol Data Unit (BPDU) Guard turned on. Ports are labelled clearly on the access switches, especially if a dedicated VLAN is used (as is generally the case at larger campuses).

Access to the Internet is provided through the corporate and guest network through the Internet gateways.

<snip>

```
! Physical interface on the AP connecting to the Wired LAN
interface FastEthernet0
 no ip address
 no ip route-cache
 speed 100
 full-duplex
```



```
!Trunk on Sub interface for carrying data traffic
interface FastEthernet0.<data vlan ID>
 encapsulation dot1Q <data vlan ID> native
 no ip route-cache
 bridge-group 6
 no bridge-group 6 source-learning
 bridge-group 6 spanning-disabled

!Trunk on Sub interface for carrying voice traffic
interface FastEthernet0.<voice vlan ID>
 encapsulation dot1Q <voice vlan ID>
 no ip route-cache
 bridge-group 7
 no bridge-group 7 source-learning
 bridge-group 7 spanning-disabled

! Trunk on Sub interface for carrying guest traffic
interface FastEthernet0.<guest vlan ID>
 encapsulation dot1Q <guest vlan ID>
 no ip route-cache
 bridge-group 8
 no bridge-group 8 source-learning
 bridge-group 8 spanning-disabled
```

<snip>

2.2.2. Wireless SSID

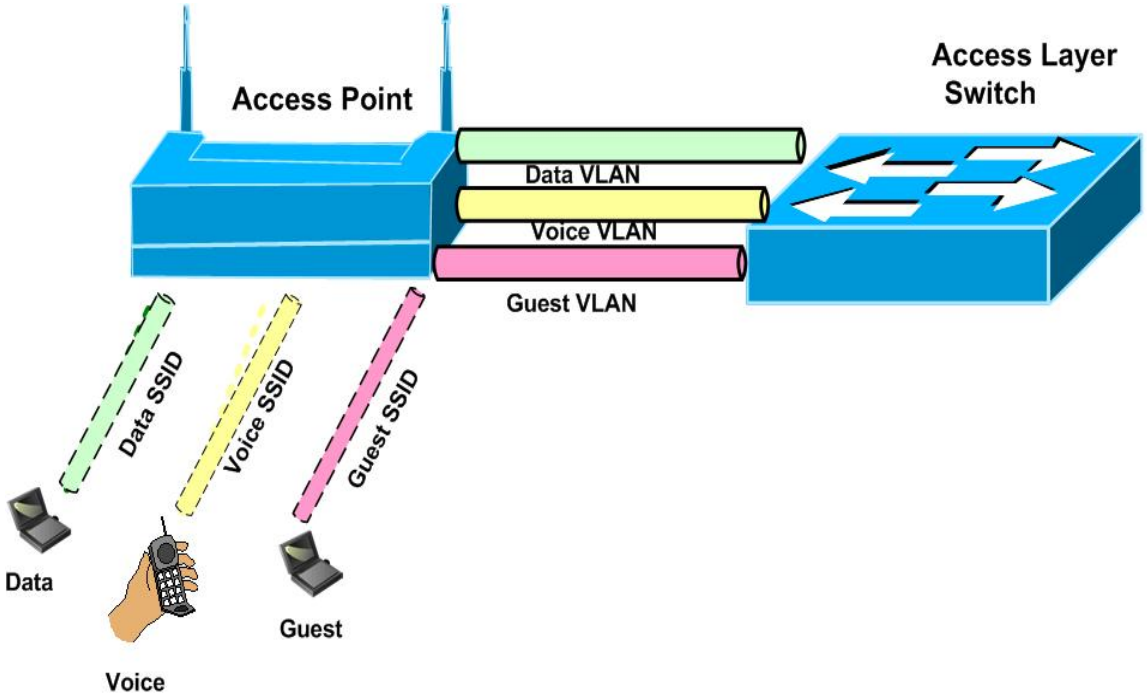
Cisco uses three SSIDs for the radio frequency (RF) network:

data vlan users	: data
voice vlan users	: voice
guest vlan users	: guest

SSID is not considered a security feature. By itself, it allows separation between WLAN networks if they share the same physical area or are in close RF proximity to each other. This type of situation may occur in offices located in metropolitan areas. SSID helps Cisco users stay within their RF management area.

There are some restrictions on the availability of channel numbers in the 2.4-GHz band. Regulations are country-specific, so the number of available channels may vary. Different channel numbers do not guarantee total separation of two devices. Generally, the three nonoverlapping channels used are channels 1, 6 and 11. As WLAN technology becomes more popular, it is necessary to check channel availability by doing site surveys prior to installations. Choice of specific antenna types is up to the local theatre's support team. However, the 2-dBi Standard Dipole (AIR-ANT4941) antenna is suitable for most locations.

Figure 3. Wireless SSID for Data, Voice and Guest networks



<snip>

```
! ssid configuration for data traffic
ssid data
    vlan <data vlan ID>
    authentication network-eap eap_methods

! ssid configuration for data traffic
 ssid voice
    vlan <voice vlan ID>
    authentication network-eap eap_methods

! ssid configuration for guest. This SSID is configured in sites that provide hotspot access
 ssid guest
    vlan <guest vlan ID>
    authentication open
    guest-mode
 !
```

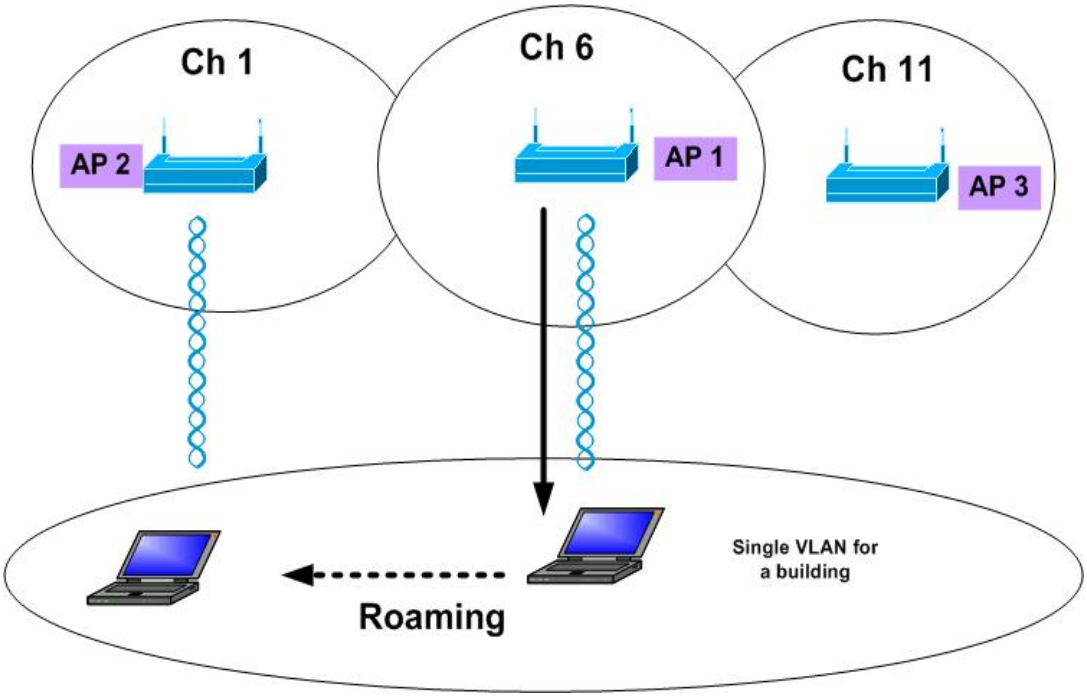
<snip>

2.2.3. User Roaming

Cisco wireless access points provide bridging between wireless media and the wired network backbone. Access points are permanently fixed devices, while wireless clients are allowed to roam. The IEEE 802.11b standard describes client's handover procedure between access points using Inter Access Point Protocol (IAPP) if both access points are located on the same logical segment.

With campus buildings, Cisco IT supports a “one-VLAN” architecture for the building. For small field sales offices (FSOs), wireless can be integrated into the existing office subnet/VLAN; this assumes that all access points in the office can be placed in the same VLAN. In most cases, the wireless VLAN is no bigger than a /23. Local networking teams decide on the exact sizing of the IP subnet. Cisco IT is deploying Wireless Domain Service (WDS) to support all of the Cisco SWAN features.

Figure 4. Client Roaming



2.2.4. Multi-Data Rate

For 802.11b radios, Cisco IT uses a single-data rate with 11 Mbps for several reasons:

1. Site surveys are performed based on 11 Mbps (the maximum throughput for *all* users) per cell, with a cell size of –75 dBm signal strength, full coverage on every floor, and use of nonoverlapping channels.

2. Performance. When a radio has to transmit at a lower data rate, for example at 2 Mbps instead of 11 Mbps, it uses significantly longer radio time to push the packet into the air space. This results in significantly reduced performance (throughput), especially if a lower speed client needs to transmit a lot of data. Keeping them at 11 Mbps provides maximum performance for everyone.

3. Standardizing on 11 Mbps per cell allows for easy troubleshooting and support. Users physically located in one floor of a multi-storeyed building are associated to an access point in the same floor. Providing better location identification for E911 requirements with voice over wireless is another consideration.

4. Site survey concerns: the ability to control cell size based on using one adjustment factor, the power. No significant RF exists outside the building: this limits the area of RF coverage within the building.

5. To combat low S/N APs power can be increased or more APs installed if necessary (to cover any dead spots identified). Switching down to 5.5 will defeat the purpose of WLAN optimization to offer maximum possible access.

A sample configuration is shown below.

<snip>

Interface dot11radio 0
! for 802.11b radio, the speed is set to 11 mbps only
speed basic-11.0

<snip>

Interface dot11radio 0
! for 802.11g radio, guarantee 11mpbps for 802.11b clients and anything above for 802.11g clients
speed basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0

<snip>

2.2.5. VLAN Standards

A standard best practice followed by Cisco IT is to use the same set of VLAN numbers for data, voice, and guest in all theatres. Following the standards across the globe helps maintain consistency and simplifies troubleshooting and management. Cisco IT supports a one-VLAN architecture, meaning that each building at a campus site is associated with a single VLAN. For small FSOs, wireless can be integrated into the existing office subnet/VLAN; this assumes that all access points in the office can be placed in the same VLAN. In most cases, the wireless VLAN is no bigger than a /23. Local networking teams decide on the exact sizing of the IP subnet.

2.2.6. Wireless Security

Cisco uses 802.1x-based EAP for authentication of its wireless networks. The Cisco versions of TKIP and MIC are used to enhance security and help ensure the confidentiality and integrity of wireless communications. Cisco IT also uses security techniques like dynamic key and broadcast key rotation to increase the security in wireless networks.

<snip>

!configuration under radio interface
interface Dot11Radio0
encryption vlan <vlan ID> mode ciphers <cipher-type>
broadcast-key vlan <vlan ID> change <timeout>

!global radius configuration
radius-server host < IP1> auth-port 1645 acct-port 1646 key <xxx>
radius-server host <IP2> auth-port 1645 acct-port 1646 key <xxx>

!global aaa configuration
aaa group server radius auth-eap
server < IP1> auth-port 1645 acct-port 1646
server <IP2> auth-port 1645 acct-port 1646
aaa authentication login eap_methods group auth-eap

<snip>

Next steps: Cisco IT has migrated from Cisco TKIP and Cisco MIC, to Wi-Fi Protected Access (WPA)-based TKIP and MIC. The next goal is to support 802.11i-based security. Cisco IT has also migrated from Cisco LEAP for EAP-Flexible Authentication via Secure Tunnelling (FAST) as the corporate EAP authentication method.

2.2.7. Wireless Management

Cisco IT has been using the internally developed EMAN (enterprise management) system for Internet Control Message Protocol (ICMP) monitoring and managing code upgrade and configuration changes on the access points. The team is currently deploying the CiscoWorks Wireless LAN Solution Engine (WLSE), primarily for radio management, rogue access point detection, and fault alerting.

2.2.8. Other Design Considerations

Multicast over wireless—In most cases, Cisco IT does not provide multicast over wireless; this is accomplished by not enabling Protocol-Independent Multicast (PIM) on the wireless VLAN interfaces. Cisco supports a rate-limited unicast delivery method for wireless users that want to view multicast streams. The unicast is rate-limited to 100 kbps.

Dynamic Host Control Protocol (DHCP) lease timeout—The main aspect of wireless LAN deployment is mobility. When users roam between buildings, their IP addresses also change based on their locations. The best practice is to adjust the DHCP lease times to make sure IP addresses are not wasted and are repurposed appropriately. The DHCP lease timeout for wireless is configured to four hours.

Antennae—For most deployments, 2-dBi Standard Dipole (AIR-ANT4941) antennas are sufficient. Depending on the shape of the building and room, and also materials from which the room is made of, it may be suitable to use directional antennas. For example, large conference rooms benefit from directional antennas. The local operations team takes the final decision on the type of antennae used.

Channel overlap between floors—The best practice in multistoried buildings is to ensure that channels do not overlap between floors. This is included in the site survey requirements for the site.

Power level on access points—Cisco IT standard for power level range is 1–30MW, with the standard being 5MW.

<snip>

Interface dot11 radio 0

Power local 5

<snip>

2.3. Wireless Client Configuration

2.3.1. Link Status Meter (LSM)

An LSM is used to troubleshoot communications problems and to monitor the status of a wireless link. For reliable communication, the link quality and signal strength should be above 35–40 percent.

2.3.2. Cisco Aironet Client Monitor

The Cisco Aironet Client Monitor is a useful tool located on the task bar when Aironet Client Utility 6.x is installed on the client PC. Cisco Aironet Client Monitor provides quick access to several tools and shortcuts for the Cisco Aironet Client Utility client profile manager, including radio on and off selection, reauthentication, connection status (via its colour), and troubleshooting tools. The Cisco Aironet Client Monitor icon displays in one of four colours: Green denotes a good connection; yellow denotes a marginal connection, red denotes a poor connection, and white signifies that the radio is off. Users are encouraged to turn off their wireless radios whenever docked. This helps reduce congestion in the radio frequency and helps improve efficiency.

2.3.3. Network Login

The wireless client should be able to perform authentication with Cisco EAP-FAST using valid Active Directory user account credentials (name and password, for example) through any onsite access point.

2.3.4. Coverage Check

This checks that access points are providing the appropriate coverage after the installation. Site survey methodology can be used to determine cell boundaries. The output power of access points can be adjusted if necessary.

2.3.5. Roaming

Cell-to-cell roaming should be tested, with careful examination of overlapping areas. A wireless client should reliably communicate with one access point on site at 11 Mbps and roam to another access point when it physically moves to the neighbouring cell. In addition, client software is configured *not* to “Search for a Better Access Point.” This reduces excessive roaming caused by multiple factors such as moving laptops, access point load balancing, or signal degradation due to excessive cell overlap.

For additional Cisco IT best practices, visit
Cisco on Cisco: Inside Cisco IT

www.cisco.com/go/ciscoit

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**