Enterprise Best Practices for Apple Mobile Devices on Cisco Wireless LANs

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Purpose of this Document

This document is intended for IT professionals responsible for designing, deploying, and managing Cisco Wireless LANs (WLAN). It assumes the reader has a working knowledge of Cisco WLAN components and features, and basic IP networking. The best practices cover implementation considerations, recommended network setup, and troubleshooting to provide best possible services for Apple devices and mixed client environments while maintaining infrastructure security.

The topics in this document include general guidance about configurations for different use cases, and specific guidance for the iPhones and iPads using the iOS6 operating system which supports Wi-Fi 802.11r fast transition secure authentication, and 802.11k neighbor list radio management.

Introduction

In this Bring Your Own Device (BYOD) world where students bring their wireless Apple iPhones and iPads on campus, and the majority of demographics includes users with multiple devices, IT managers are expected to accommodate an open access network environment while at the same time ensuring the security of network resources.

In addition to security concerns, these environments present a number of challenges in regards to quality of service, radio coverage, roaming scenarios, central switching versus local switching architectures, and legacy client mixes. How do you allow guest users to reach wireless printers but not corporate file servers? How do you guarantee trusted corporate users are given higher priority bandwidth? It's not only about secure access, it's also about simple onboarding and staying connected with good application performance.

This document describes some of the best practices for ensuring the best possible service for "iDevices" given a number of different factors that have to be considered. Apple is at the forefront of mobile devices with business applications. The iPhone5 supports the 5 GHz band and the 21 Wi-Fi channels in the North American channel set for the 5 GHz band. This gives the iPhone5 Wi-Fi dual-band support and greatly influences the adoption of the iPhone into business. The Apple iOS6 with support for 802.11k and 802.11r now supports two of the protocols that are designed to enhance roaming across Wi-Fi access points (AP). This document includes information on how to configure the Cisco Wireless LAN Controller (WLC) for those protocols.

Wi-Fi Channel Coverage

Overview of Wi-Fi Channel Coverage

The dual-mode iPhone5 and iPads support all of the 5 GHz channels approved for the U.S. Dual-mode capability allows those devices to operate on 21 additional Wi-Fi channels. Cisco recommends a 5 GHz coverage design. The 5 GHz channels are free of common 2.4 GHz devices such as Bluetooth interference and microwave ovens. The channel utilization of the 5 GHz channels is generally much lower than the 2.4 GHz channels. With more channels being available, the channel utilization on the 5GHz band will be lower due to the reduced channel re-utilization (co-channel interference) and overlap.

Using the Aloha protocol definition of channel utilization, a wireless packet network has reached capacity when the utilization reaches 34%. In dense 2.4 GHz networks, high channel utilization is not uncommon. Cisco recommends closely monitoring the channel utilization provided through the WLC reports. High channel utilization values may be an indication of new sources of interference, AP outages, or an influx of new Wi-Fi devices.

Another condition that should be monitored is APs changing channels. A site survey will find fixed or stationary sources of signals that will interfere with Wi-Fi performance. It is recommended that your 5GHz Wi-Fi channels that are affected by these conditions be added to the Dynamic Channel Allocation (DCA) exclusion list. WLC logic and configuration parameters, plus regulations, can temporally place 5 GHz channels into the DCA list. This is normal. But if certain channels are repeatedly added to the DCA, it may be best to add those channels into the DCA list if that interference cannot be managed.

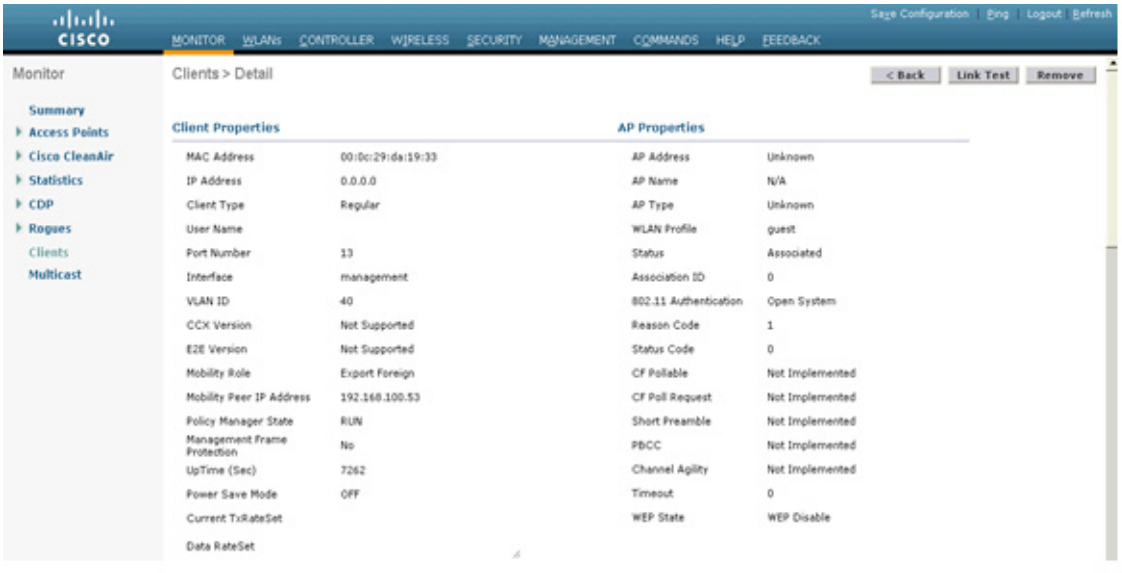
To determine if the current 5 GHz AP coverage is sufficient for the applications running on iPhone5 and iPads, the WLC provides a user-friendly link test tool.

To check for 5 Ghz AP coverage:

Step 1 With the iPhone associated to an AP, and from the MAC address that matches the client, select **WLC > Monitor > Clients**. The Client Details are displayed (See Figure 1)

Step 2 Run the link test by selecting the **Link Test** button. This action performs a bi-directional link test to determine the current coverage of the client. If there are no missing packets, then try moving the client away from the AP to determine if there is additional range available while maintaining enough signal to have quality application performance.

Figure 1 Client Details with Link Test Option



One coverage goal is to have a signal of -67 dBm Received Signal Strength Indicator (RSSI) or better to the AP. When doing coverage testing on 2.4 GHz it is recommended to have the lower data rates disabled. This is because the -67 dBm RSSI coverage area is much larger at 1 Mbps data rate than 12 Mbps. This is a range versus bandwidth design consideration. Dense 2.4 GHz networks may have high channel utilization. The most effective way to reduce channel utilization is to remove lower data rates.

Current iPhones and iPads with 802.11n radio technology support one spatial stream. One spatial stream means on a 20 MHz wide Wi-Fi channel the 802.11n supported data rates are from 6.5 Mbps to 72 Mbps. On the 5 GHz band this is better than 802.11a data rates, which are from 6 Mbps to 54 Mbps. The 11n technology allows use of 40 MHz wide Wi-Fi channels by the client and, when the client is operating as an 802.11a client, it allows sharing the usage of the primary 20 MHz of the 40 MHz wide channel.

The client iPhones and iPads with 802.11n radios support 802.11n beam forming. Cisco terms the 802.11n beam forming technology as ClientLink 2.0. Cisco provides ClientLink for 802.11g on 2.4 GHz and 802.11a on 5 GHz. The benefit of ClientLink is it improves the quality of the Wi-Fi signal between the client devices and the AP. Each high quality link between the client devices and the APs improves the bandwidth and the quality of coverage on those Wi-Fi channels.

Note For more information about ClientLink 2.0, refer to the *Cisco Wireless ClientLink 2.0 Technology at a Glance* document:
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps11983/at_a_glance_c45-691984.pdf

Cisco recommends the use of 802.11n on the 5 GHz band because beam forming (ClientLink) provides a better quality link and better call quality than 802.11a. ClientLink 2 improves the bandwidth in the Wi-Fi channel and the coverage area, thereby improving the performance of all the devices in the coverage area.

Cisco also recommends enabling the WLAN setting, “BandSelect”. While the iPhone5 does exhibit in some cases a bias to the 5 GHz band, enabling BandSelect can improve the percentage of connections on 5 GHz when a phone has appropriate signal strength to both bands.

Wi-Fi 802.11e/WMM QoS

There are different use cases for the WLAN setting of Wireless Multimedia (WMM). When WMM is set to disabled, WMM QoS is not used to queue or mark the packets. All packets on the WLAN are forwarded at the WLAN QoS setting. Therefore, a ping sent to the iPhone will be sent at a voice priority when the WLAN QoS setting is voice or platinum. This includes a ping packet that is marked with a best effort Differentiated Services Code Point (DSCP) value going into the WLC.

For these reasons, the recommended setting for WMM is “allowed” or “required” depending on the use case. With an 802.11e/WMM QoS capable client and a WMM WLAN, each transmitted packet by the AP has a QoS value in the 802.11 header. Likewise, the WMM client is going to send all packets with a QoS value in the 802.11 header. A non-WMM client is not capable of sending or receiving packets with a WMM header. Packets without the WMM header have no channel priority or control. Their traffic is best effort.

The 802.11e/WMM specification has been around as long as the cellular phone has been using Wi-Fi as an alternate wireless media and as long as tablets have been using Wi-Fi. These devices should be capable of connecting to a WLAN that has WMM set as required. When the WLAN is set to WMM required, a device that is not WMM will not associate to the WLAN even if the WLAN has no security. A WLAN with security will not pass the authentication requests of a non-WMM client. A WMM setting of ‘allowed’ needs to be considered for legacy devices like handheld transaction computers and single-purpose laptops of considerable age, which are not WMM capable. Apple devices with iOS 4.0 and later do support the WMM required configuration.

In the configuration graphic example shown in Figure 5 in the “802.11n” section on page 13 under **WLANs > Edit 11nSSID > QoS**, the graphic shows a configuration for WMM. Depending on the use case for the WLAN, this setting may be changed. For example, it may be a company policy to have guest access WLAN configured to allowed with a WMM QoS value of silver or best effort. In such a case the AP will forward all traffic as best effort if there are no specific policies in place.

Recommended for an Enterprise WLAN for iPhones and iPads is a QoS value of platinum or voice with WMM set to required. This allows the Ethernet traffic from the AP to connect to the switch port with a QoS value representative of the priority on the Wi-Fi channel. If corporate policy requires, the need to re-mark the header then can be done at the edge switch on the port that is connected to the AP. As of Release 7.4 of the WLC code, by enabling Application Visibility and Control (AVC) such policies can be activated on the WLC. The AP will do the deep packet inspection on the upstream packets and re-mark the upstream packets matching the policies set on the WLC.

How QoS Markings are Handled

When the packet QoS marking does not match the WLAN setting for QoS, the WLAN setting has forwarding precedence over the packet marking. If the iPhone transmits a voice packet at a voice priority over the Wi-Fi channel, then it has voice priority queuing and voice priority media access (channel access) with voice expedited retry priority in the case of packet collisions. This happens even if the WLAN that the phone is connected with has the QoS set as best effort or silver.

If the phone is connected to a WLAN with a WMM priority of voice or platinum, that packet will be forwarded over the Ethernet upstream into the infrastructure with priority of voice - that is, unless there is an overriding network policy in place to change the QoS value in the wired side header of that packet. If that iPhone is connected to a WLAN with a best effort or silver WLAN, then the AP forwards those packets to Ethernet with a best effort marking.

In the case of the audio packet from the Cisco softphone application called Jabber, the Jabber application marks the audio (G711/722) packet with a DSCP value of expedited forwarding value of 46. But iPhone WMM/iOS does not mark the WMM user priority (UP) field to a voice value. Instead, it uses a value

with a video priority. The WMM value for voice is UP=6. The WMM value of video is UP=5. Therefore, the Jabber audio packet has the Wi-Fi queuing, retry, and media access value behavior of a video packet when sent to the Wi-Fi channel. This happens regardless of whether the WLAN setting is voice, video, or best effort.

If the destination WLAN of that packet is set to voice and there are no overriding policies, then that packet will be sent from that WLAN with a WMM UP value of 6 or voice. This WLAN/WMM behavior helps the quality of the call without invoking extra policies. The iPhone's marking of the audio packet will hurt the audio call's Mean Opinion Score (MOS) value by marking down the QoS value on the first network hop of the call. But with a source WLAN set to a WMM value of platinum, the Jabber audio packet will have voice priority on the last hop if not changed by a network policy.

If the Jabber application had set the DSCP value of the audio packet to best effort, then the iPhone would have sent the audio packet with a WMM UP=0 or best effort. Then, if that packet has a destination of another phone on the same WLAN, the AP will forward that packet with a WMM UP=0 even with a WLAN WMM setting of platinum/voice.

WMM QoS logic supports DSCP values. When the Wi-Fi channel is not over-utilized and therefore has adequate bandwidth, then quality application performance can be expected.

This does place a degree of trust that the applications used maintain a proper QoS behavior. An application like Cisco's softphone application, Jabber, does mark audio, video and other frame types to the Cisco Architecture for Voice, Video and Integrated Data (AVVID) QoS standard.

Note Refer to the chart in "Addendum A: IEEE IP DSCP - AVVID Values & 802.11e WMM" section on page 33

For Jabber and other business applications Cisco recommends platinum QoS so that application QoS levels can be obtained for packets that have a degraded WMM QoS value due to the device's WMM driver or QoS policy. If iPhones, iPads and other similar devices only have guest access or by policy are restricted from Enterprise level access, then configure the WLAN through which they authenticate to a WMM QoS setting that reduces their priority.

An iDevice that is authenticated into a WLAN and that has WMM enabled sends packets at WMM QoS levels set by that device's Wi-Fi radio driver and QoS policies. When this happens, these devices are not required to send packets with the QoS values set on the WLC for the WLAN. Nor are the devices required to send the packets with the DSCP IP value set in the packet by the application. The WLAN QoS value is more of a high-level mark that the AP uses to forward upstream and downstream traffic. In addition to the WLAN WMM setting there are numerous QoS configuration options. Please review a current WLC configuration guide for those options.

To summarize, the general QoS behavior of the iPhone and iPad is that upstream and downstream packets will be sent with a WMM value that is representative of the DSCP value. If additional management of the Wi-Fi iPhone and iPad traffic is desired, Cisco recommends using Application Visibility and Control (AVC). AVC is included on the WLC as of Cisco WLAN Release 7.4.

Note For additional recommendations, refer to the *Voice over Wireless LAN Design Guide* at http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html and the *Wireless LAN Controller Configuration Guide* appropriate to your version of code, available on cisco.com.

Note For a summary of the various iDevices capabilities supported, refer to "Addendum B: Summary Matrix" section on page 34.

Roaming

Overview of Roaming

IEEE 802.11k and 802.11r are the key industry standards now in development that will enable seamless Basic Service Set (BSS) transitions in the WLAN environment. As of Cisco WLAN Release 7.4, the recommended Enterprise roaming configuration for iPhones and iPads with Apple iOS6 is 802.11k Neighbor List. The IEEE 802.11k specification was ratified in June 2008.

Note For a brief description of 802.11k on Wikipedia go to http://en.wikipedia.org/wiki/IEEE_802.11k-2008

Note For the IEEE 802.11k specification go to http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4544755

Note For 802.11k references, see the "Radio Resource Management" section on page 8 of this document.

To facilitate roaming an iPhone associated with an AP sends a request for a list of neighbor APs. The request is in the form of an 802.11 management frame known as an action packet. The AP responds with a list of neighbor APs on the same WLAN with their WiFi channel numbers. The AP response is also an action packet.

From the response frame the iPhone knows which APs are candidates for the next roam. The use of 802.11k radio resource management (RRM) processes allows the iPhone to roam efficiently and quickly, a requirement for good call quality in an Enterprise environment where on-call roams are common.

The recommended WLC 802.11k configuration is to enable the radio resource management to provide both 2.4 GHz and 5 GHz AP channel numbers in the neighbor list response packets. Cisco recommends the use of 5 GHz band Wi-Fi channels for not only Voice over WLAN calls but for all applications and devices. The dual-band iPhone5 and iPads do show a bias to the 5 GHz band.

With the neighbor list information, the iPhone does not need to probe all of the 2.4 GHz and 5 GHz channels to find an AP it can roam to. Not having to probe all of the channels reduces channel utilization on all channels, thereby increasing bandwidth on all channels. It also reduces roam times and improves the decisions made by the iPhone or iPad. Additionally, it increases battery life of the device because it is neither changing the radio configuration for each channel nor sending probe requests on each channel. It avoids the device having to process all of the probe response frames.

Listed below are the recommended WLC configuration commands for 802.11k using CLI.

Note The WLC does not have a GUI configuration for 802.11k.

- WLAN neighbor list Enable/Disable: This is to enable or disable the neighbor list from the WLC and also the RRM and Power Constraint Information Elements (IEs) on the APs.

  config wlan assisted-roaming neighbor-list {enable|disable} *wlanId*

- WLAN neighbor list dual-band response Enable/Disable: This is to enable or disable the neighbor list including entries for both radio bands. Default is the band in which the client is currently associating.

  config wlan assisted-roaming dual-list {enable|disable} `wlanId`

- Prediction list based assisted roaming Enable/Disable: This is to enable or disable the assisted roaming capabilities with a roaming optimization predict list. A warning will be printed out, and load-balancing will be disabled for the WLAN if load balancing is already enabled on the same WLAN.

  config wlan assisted-roaming prediction {enable|disable} *wlanId*

Note Save the configuration once the command is executed.

Radio Resource Management

The 802.11k standard provides information to discover the best available AP.

Note For 11r references, refer to the "Roaming" section on page 7 of this document.

The iPhone4s with iOS6 code and the iPhone5 use the 802.11k radio management information to determine which APs they may need for roaming. As part of the process defined in the 802.11k specification, the phone can send a request for neighbor information to the AP that has a current association. That AP then returns the neighbor information, which includes the nearest AP and the Wi-Fi channel number of that AP. This allows the iPhone5 to find that AP without taking time to scan all of the Wi-Fi channels on the 2.4 GHz band and all of the channels in the 5 GHz band. This is a savings of several seconds in time and battery drain.

802.11k is intended to improve the way traffic is distributed within a network. In a WLAN, each device normally connects to the AP that provides the strongest signal. Depending on the number and geographic locations of the clients, this arrangement can sometimes lead to excessive demand on one AP and under-utilization of others, resulting in degradation of overall network performance. In a network conforming to 802.11k, if the AP having the strongest signal is loaded to its full capacity, a wireless device is connected to one of the under-utilized APs. Even though the signal may be weaker, the overall throughput is greater because more efficient use is made of the network resources.

The following steps demonstrate how a possible 802.11k Neighbor List Protocol Operation is performed before switching to a new AP:

1. The AP determines that the client is moving away from it.
2. The AP informs the client to prepare to switch to a new AP.
3. The client requests a list of nearby APs.
4. The AP gives a site report.
5. The client moves to the best AP based on the report.

The iPhone5 and iPad with iOS6 exhibits a similar use of the 802.11k neighbor list function. They request a neighbor list from the AP that they just associated with shortly after they associated. That neighbor list report contains the Basic Service Set Identifier (BSSID) and the channel number of the neighboring APs.

Fast Roaming

Overview of Fast Roaming

The recommended enterprise security configuration for devices with Apple iOS6 is 802.11r Fast Transition (FT). The IEEE 802.11r specification was ratified in July 2008, and it follows the 802.11i specification of June 2004.

802.11r introduces standards-based fast transition:

- Allows a client to establish security and QoS state to target AP prior to (or during) re-association
- Method 1: Over-the-Air (client to new AP)
  - 4 packets are changed over the Wi-Fi channel
- Method 2: Over-the-Distribution System (through the old AP)
  - 2 packets are exchanged over the Wi-Fi channel and 2 via Ethernet

802.11r reduces the number of packets exchanged between an AP and an 11r client whose credentials are already cached.

Note For a brief description of 802.11r on Wikipedia go to http://en.wikipedia.org/wiki/IEEE_802.11r-2008.

Note For the IEE 802.11r specification go to http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04573292

Note For iPhone and iPad model numbers go to http://support.apple.com/kb/HT3939

Apple iOS prior to 6.0 does not support fast transition. The Apple iOS5 supports Sticky Key Caching (SKC). Both iOS5 and iOS6 support the 802.11e authentication types, EAP-FAST, LEAP, EAP-TLS, EAP-TTLS, EAP-SIM, and PEAP versions 1 and 2.

This security option allows the iPhone to authenticate securely to an AP in an exchange of only four packets. Two of the packets can be sent on the Ethernet wires that connect APs to each other. The other two packets are sent on the Wi-Fi channels of each AP. This allows the iPhone to be authenticated securely to the AP that it is going to roam to before it actually roams. The result is the iPhone can be sending and receiving data, video, and audio packets after the roam without the delay of the authentication process.

The following are guidelines and limitations currently affecting 802.11r FT:

- 802.11r FT is not supported on Mesh APs.
- For APs in FlexConnect mode:
  - 802.11r FT is supported only in centrally and locally switched WLANs in Release 7.3 and later.
  - 802.11r FT is not supported for the WLANs enabled for local authentication.

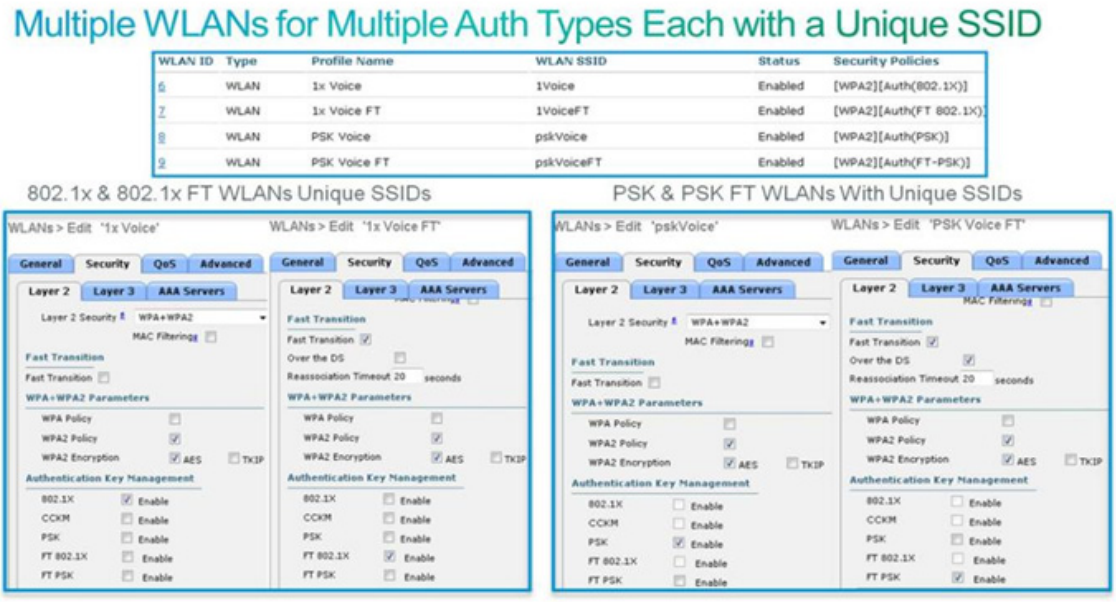
- 802.11r FT is not supported on Cisco 600 Series OfficeExtend Access Points.
- 802.11r client association is not supported on APs in standalone mode.
- 802.11r fast roaming is not supported on APs in standalone mode.
- 802.11r fast roaming between local authentication and central authentication WLAN is not supported.
- 802.11r fast roaming is not supported if the client uses over-the-DS pre-authentication in standalone mode. Over-the-Distribution System (DS) is when packets are sent on the wired infrastructure.
- The service from a standalone AP to a client is only supported until the session timer expires.
- Traffic Specification (TSpec) is not supported for 802.11r fast roaming. If a WLAN link latency exists, fast roaming is also delayed. Voice or data maximum latency should be verified.
- The WLC handles 802.11r fast transition authentication requests during roaming for both over-the-air and over-the-DS methods.
  - Over-the-DS is recommended because two of the required packets are sent on the wired connection of the APs, with two packets sent on Wi-Fi. If the DS option is not selected, then all four packets are sent on WLAN.

Recommended WLC Configuration for Fast Transition

The following are the WLAN configuration recommendations for adding 802.11r FT clients to the WLAN network. Figure 2 provides an example of these configurations. The best practices recommendation listed below is the result of cooperative work between Apple and Cisco.

- Configure an additional WLAN for fast transition 802.1x clients.
- Configure an additional WLAN for fast transition PSK clients.
  - The reason for this recommendation is legacy radio drivers will not understand the added information in the association response packets of a WLAN with fast transition configurations. Although the 802.11r specification was ratified in 2008, not all client radio drivers have been updated to handle the changes in management packets with respect to 802.11r. This includes several Apple products.
  - Apple recommends using separate WLAN and SSIDs for legacy clients.

Figure 2 WLAN Configuration Recommendations for adding 802.11r FT Clients



Note Please refer to the *Cisco Wireless LAN Controller Configuration Guide* specific to your installed version of WLC code for the complete CLI or GUI configuration options regarding fast transition.

Sticky Key Caching (SKC)

SKC has not been widely adopted. Cisco added support in the WLC Release 7.2. The client limitation with SKC is that the client only caches information from the last 8 APs with which it has associated. Each roaming to a new AP will cause a full authentication, and roaming to the same AP will be using the cached entry.

The WLC limitations are:

- Caching will not work across WLCs in mobility.
- Caching will work only for WPA2 Robust Security Network (RSN) configured WLANs.
- Caching is applicable only for Local Mode APs.

SKC is configurable on the WLC CLI. The command used is:

`config wlan security wpa wpa2 skc-cache {enable|disable}` *`wlan-id`*

Note For more information on SKC refer to the *Wireless LAN Configuration Guide, Release 7.2* at http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html

Note Save the configuration once the command is executed.

Data Rates

Overview of Data Rates

You can use the data rate settings to choose which data rates the wireless devices can use for data transmission. There is a direct correlation between data rates, performance, range, and reliability. When working with Apple devices, the strategy needs to be comprehensive and include all possible devices that will connect to the network and should take into account the AP density of the deployment.

For selecting data rates two paths can be taken:

- Maximize range — If the requirement is to increase the range, consider enabling low data rates. The reason for this is that lower data rates require lower signal levels and SNR at the receiver in order to decode the signal, and this allows client devices to maintain a reliable connection to an AP from a farther distance. Just be sure to try to keep data rates high enough to still provide adequate levels of performance.
- Maximize performance — If the objective is to deploy a high-performance WLAN, improve roaming, and help mitigate the effects of co-channel interference by reducing the cell coverage, consider configuring higher data rates. Be sure to avoid being too aggressive as this could prevent a client device from establishing a reliable connection and actually result in decreasing the performance.

Selection of Data rates is based on the following guidelines:

- The enabling of low data rates increases the range of packets sent by the APs. The lower you set the lowest configured mandatory data rate, the greater the range of beacons and other packets from the AP. In a site with few APs this may be desirable if there is a large number of legacy clients. Current client devices have better radios than those from the 802.11b era. Current clients have range capabilities at 802.11g rates that equal their range at 802.11b rates. So, the slow and bandwidth-robbing rates of 802.11b may have no value.
- In a site with many APs low data rates will likely rob the site of bandwidth and lead to poor application performance. The degradation of bandwidth due to AP density is more likely at 2.4 GHz than at 5 GHz. The degradation in this case is due to the channel utilization increase from co-channel interference. A side effect of co-channel interference is higher packet error rates from packet collisions. Collisions mean retries, and retries add to the channel utilization.

Therefore, the best practice recommendation is to manage data rates to fit the data rates to provide coverage suitable to the number of clients needed in the coverage of a channel with bandwidth needed in the coverage of the channel.

Note For more information refer to the *Enterprise Mobility 4.1 Design Guide* at http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html

You can set each data rate to one of three modes:

- Mandatory — Allows transmission at this rate for all packets, both unicast and multicast. At least one data rate needs to be set to mandatory on the APs, and all clients that associate to the AP must be able to physically support this data rate on their radio to use the network. Additionally, for the wireless clients to associate to the AP, they must be able to currently receive packets at the lowest

mandatory rate and their radios must physically support the highest mandatory data rate. If more than one data rate is set to mandatory, multicast and broadcast frames are sent at the highest common mandatory transmission rate of all associated clients.

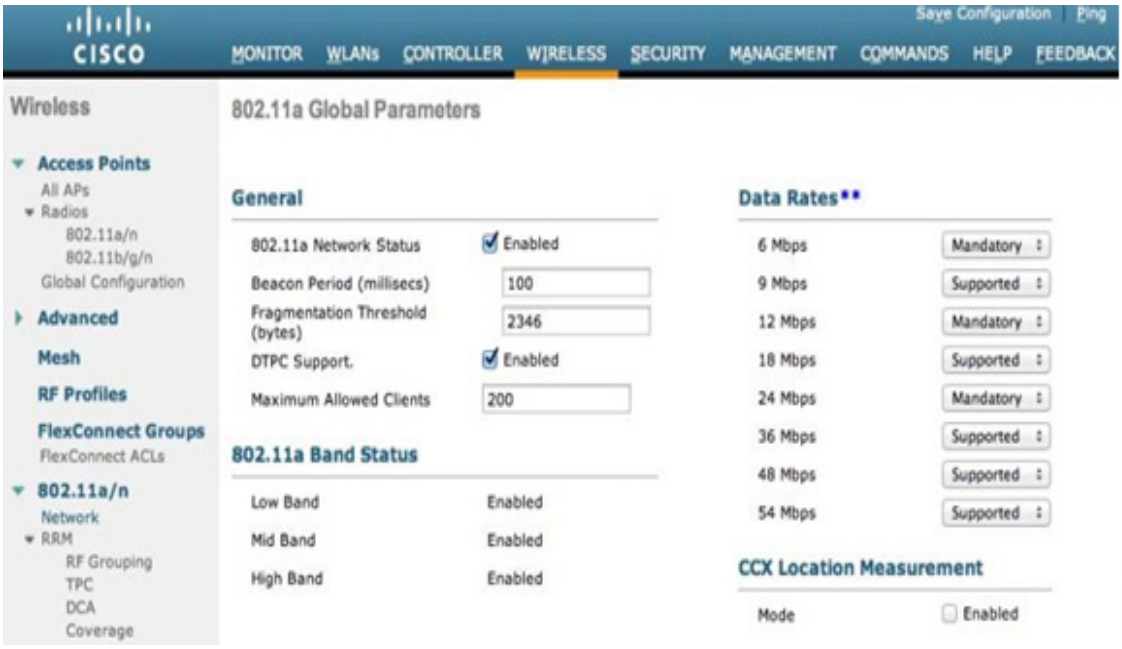
- Supported — Allows transmission at this rate for unicast packets only. The wireless clients always attempt to transmit and receive at the highest possible data rate.
- Disabled — The AP does not transmit data at this rate.

To configure the data rate settings using the controller GUI, go to **Wireless > 802.11a/n** or **802.11b/g/n > Network**, as shown in Figure 3, to specify the rates at which data can be transmitted between the AP and the client.

Check administration logs to verify that client devices are connecting to the network at desired rates. Indications that data rates are not set properly can include:

- Coverage hole alarms
- High levels of channel utilization
- Excessive retransmissions
- Clients not able to connect
- Clients not roaming properly

Figure 3 Configure Data Rates



802.11n

The 802.11n standard can increase the wireless network's performance, reliability, and predictability for most Apple devices (iPhone 4, iPod Touch 4, iPads and newer versions).

For best practice, use the following guidelines when you deploy 802.11n:

- Aggregated MAC Service Data Unit (A-MSDU) — Packet Aggregation does provide faster throughput for applications like File Transfer Protocol (FTP). But it takes away channel fairness. Several FTP processes in the same coverage area will create jitter for voice applications. Therefore Cisco recommends disabling packet aggregation in an enterprise network.
- Channel bonding — While 802.11n in 2.4 GHz will be restricted to use only 20 MHz channels, in 5 GHz both 20 MHz and 40 MHz modes are supported. Use 20 MHz when channel density (e.g., high density environment) is needed, and consider 40 MHz when client traffic uses heavy bandwidth (e.g., video). To configure channel bonding from the controller GUI, go to **Wireless > 802.11a/n > RRM > DCA** and specify the width of the channel to be used as shown in Figure 4.
- WLANs that the 802.11n clients use must have the correct security and QoS enabled. The 802.11n Standard requires either no security or WPA2 with Advanced Encryption Standard (AES) encryption. It also requires that Wi-Fi WMM be allowed or required. This is shown in Figure 5.
- Modulation Coding Schemes (MCS) — Although WLC code 7.3.101.0 and older allows the possibility to enable/disable specific MCS data rates, it is highly recommended to leave them all enabled as shown in Figure 6. Per the 802.11n standard, MCS 0 to 15 are mandatory in 20 MHz with 800 ns Guard Interval (GI) at the AP and MCS 0 through 7 are mandatory in 20 MHz with 800 ns GI at all stations (all other MCSs and modes are optional). Disabling some of those rates could potentially break compatibility with some versions of the 64-bit drivers on Mac OS 10.7 and 10.8.

Figure 4 DCA

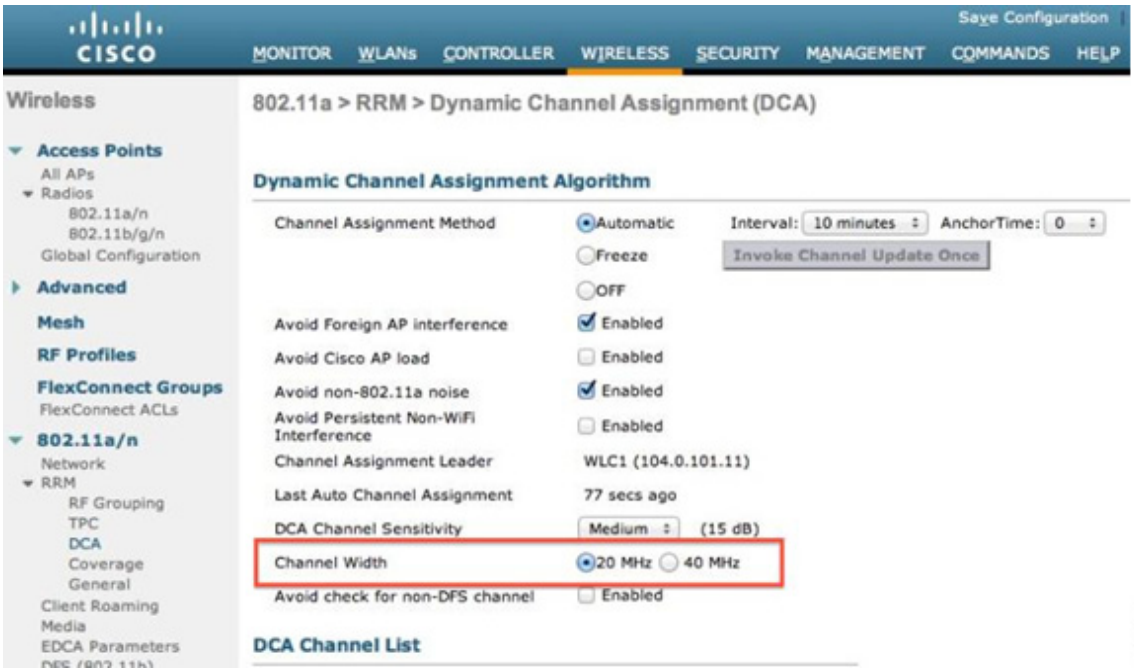


Figure 5 Security

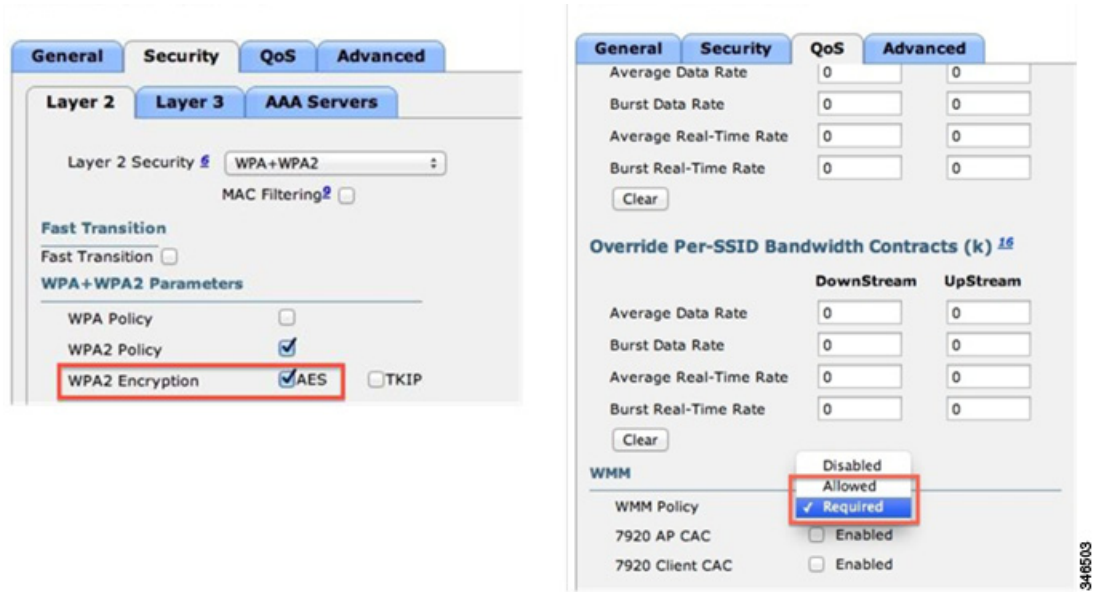
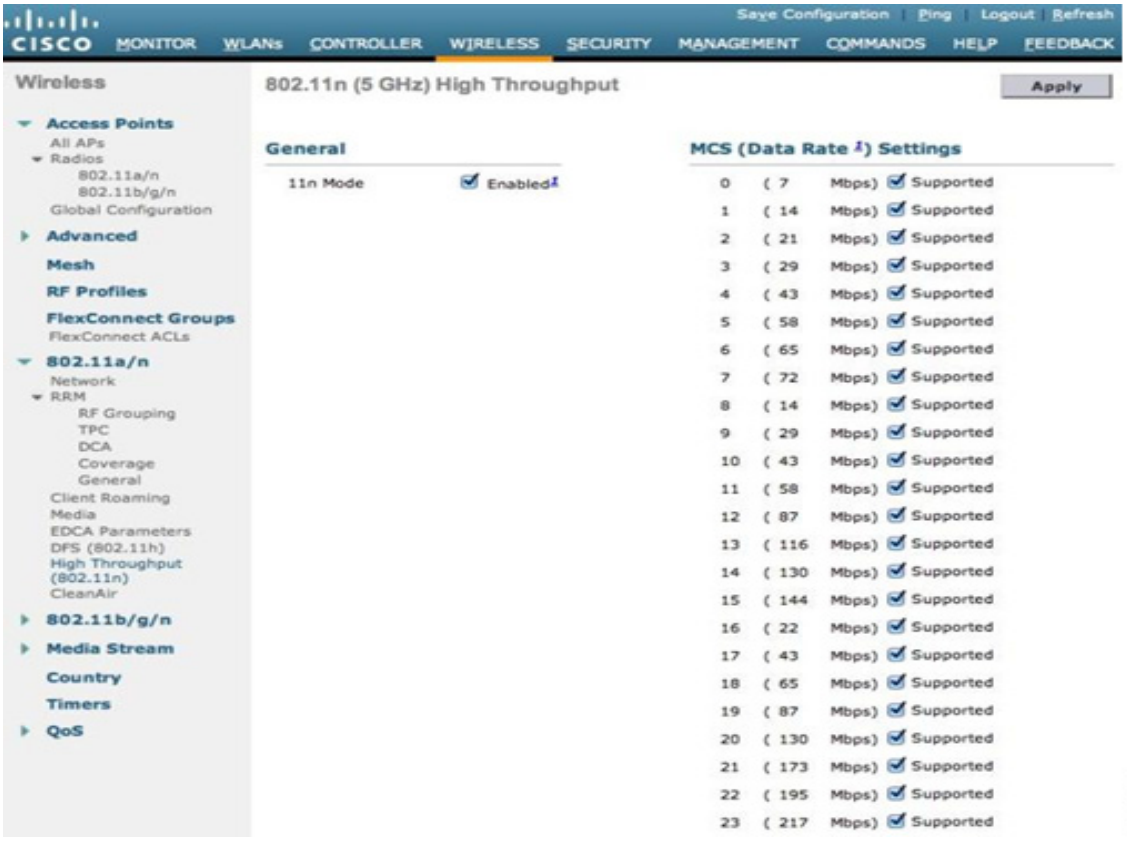


Figure 6 High Throughput



WebAuth for iOS Devices

WebAuth for Guest Access

One of the most common usage scenarios for Enterprise wireless networks is guest access for visitors. Guest access allows easy wireless access without the complexity of setting up a more secure method like 802.1x EAP authentication.

This section covers the details applicable for a WLC and iDevices guest solution. The WLC provides an interesting set of features for guest support, which are covered in several Cisco documents, for example:

- Creating a Lobby Ambassador Account:

  http://www.cisco.com/en/US/docs/wireless/controller/7.3/configuration/guide/b_wlc-cg_chapter_01011.html#ID26

- Create a Dynamic Interface for Guest User access:

  http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008076f974.shtml#c3

- Configure the WLC for External Web Authentication:

  http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008076f974.shtml#c5

Note For more information on Identity Services Engine (ISE) / BYOD scenarios and topics such as ISE, see the *Wireless BYOD with Identity Services Engine* information at http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bba10d.shtml

Note For more information on refer to the Cisco Bring Your Own Device (BYOD) Smart Solution Design Guide at http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byoddg.html

Guest access has several security implications that need to be taken into account and are normally misunderstood:. These are provided in the following list:

- It is a “layer 3” policy, so as such, by itself it will not protect from any layer 2 attacks, like MAC/IP address spoofing, eavesdropping, etc. If layer 2 protection is needed by your security policies, please consider combining WebAuth + WPA/PSK or WebAuth + WPA2/802.1x (Release 7.4 and higher). For guest access, customers normally are OK with the layer 2 security implications, so this evaluation needs to be done on a case by case scenario.

- The session timeout marks the “maximum” time a client will be allowed before the security of the WLAN has to be validated again (re authentication). This means that seating a long session timeout, for example, 24 hours, does not mean that the client will not have to authenticate again during that time. Other factors, like DHCP activity, idle timeout, etc., may cause the client to be removed.
- Proper certificate setup - As will be explained later, client devices may reject HTTPS connections towards untrusted servers. It is important to ensure that, depending on the guest access solution implemented, the client devices have a proper trust set for the certificates installed on the “server” infrastructure (WLC, ISE, external web server, etc.).

Captive Portal Detection

iDevices have a mechanism to detect if there is a WebAuth required on the current wireless connection (Internet access detection). This is done using a WiSPR request over HTTP to an apple.com address.

By default on WebAuth, this connection is intercepted by the WLC, and a login page is presented to the user as soon as the phone starts this captive portal detection. This allows the user to get a quick credential prompt, authenticate directly, and get access to the network.

The captive portal request process has a different handling on the device side than a normal web client triggered by a user on the device. This leads to implications for features like splash page support, login redirection, or untrusted certificate handling.

Starting with Release 7.2, the redirection can be disable with the **config network web-auth captive-bypass enable** command.

This allows the WLC to “spoof” the answer expected by the device, and it marks the wireless connection as having Internet access without any credential prompt as shown in Figure 7:

Figure 7 ‘Spoof’ Internet Access

There is no traffic allowed, but the device can mark this connection as usable.
The main implications for captive bypass enabled are:

- Client device "believes" it is already having access, but no traffic is allowed until client authenticates.
- The exception to this captive by-pass feature is that you can explicitly allow traffic before authentication by adding permit rules to the pre-auth Access Control List (ACL).
- For the device to be fully authenticated (RUN state), the user has to open Safari, and navigate to any HTTP page to get the login page.
- Client is deleted every 5 minutes, as it is on "WEBAUTH_REQ" state, meaning, it is associated and has an IP address, but it has never completed a full authentication. Normally the client will reassociate quickly after this event.

You should use captive bypass if you are using any of the following features:

- Splash page redirection — sending **url-redirect** AVP from RADIUS for either WebAuth or conditional WebAuth scenarios).
- External server WebAuth — hosting your page on an external server, doing local WebAuth on the WLC.
- Using HTTPS for WebAuth, **without** a trusted certificate — By default, the WLC will use a self-signed certificate, which is not trusted unless manually added to the client device. The handling of the untrusted certificate is not complete under the captive redirection on the client, so it is possible that the authentication will fail; thus, it is recommended that for WebAuth, the captive bypass redirection is bypassed and done through full user request on Safari.

Trusted Certificates

In most scenarios, WebAuth is done over HTTPS to prevent sniffing of the user's username and password over-the-air. This leads to an important requirement that there should be a proper "trusted chain" between the client and the presented certificate by the server.

By default, iOS devices trust several well-known certificates, as documented by Apple. For more information refer to *iOS 5 and iOS 6: List of available trusted root certificates* at http://support.apple.com/kb/HT5012?viewlocale=en_US&locale=en_US

An Untrusted certificate example is shown in Figure 8:

Figure 8 Untrusted Certificate Example

If a certificate is installed on the WLC from one of the certificate authorities, it is automatically trusted by the client device. This prevents any HTTPS redirection inter operability issues.

One alternative mechanism, which makes sense only if the devices are fully managed by the Enterprise, or very useful for lab testing, is to add a trusted authority into the device list using the Apple Enterprise Configuration tool available at http://www.apple.com/support/iphone/enterprise/.

If the Enterprise organization has a Public Key Infrastructure (PKI) system in-house, the tool can be used to add a CA cert into the trusted list as shown in Figure 9 and Figure 10:

Figure 9 Adding a CA Cert

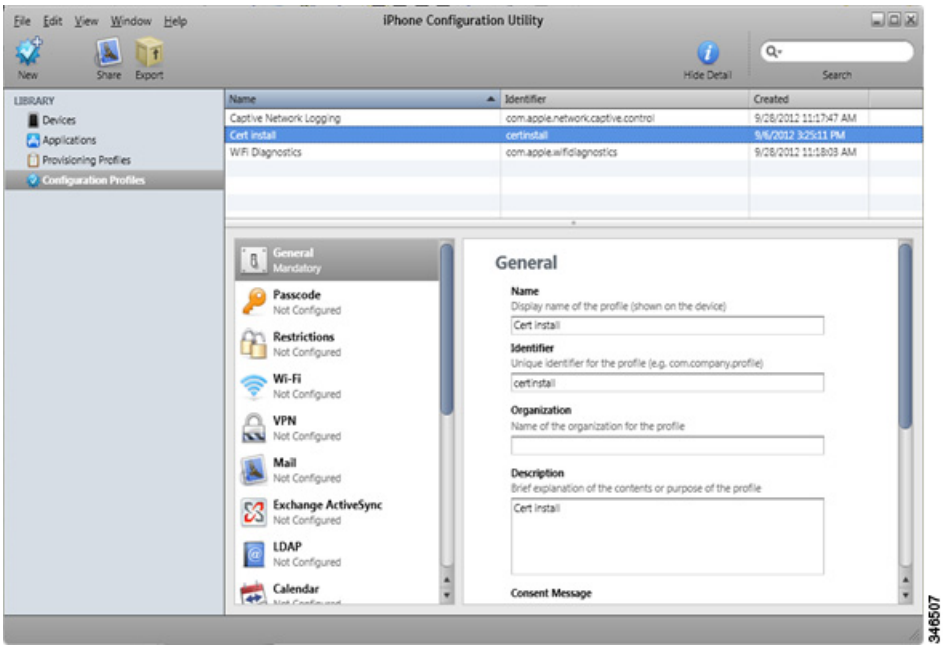
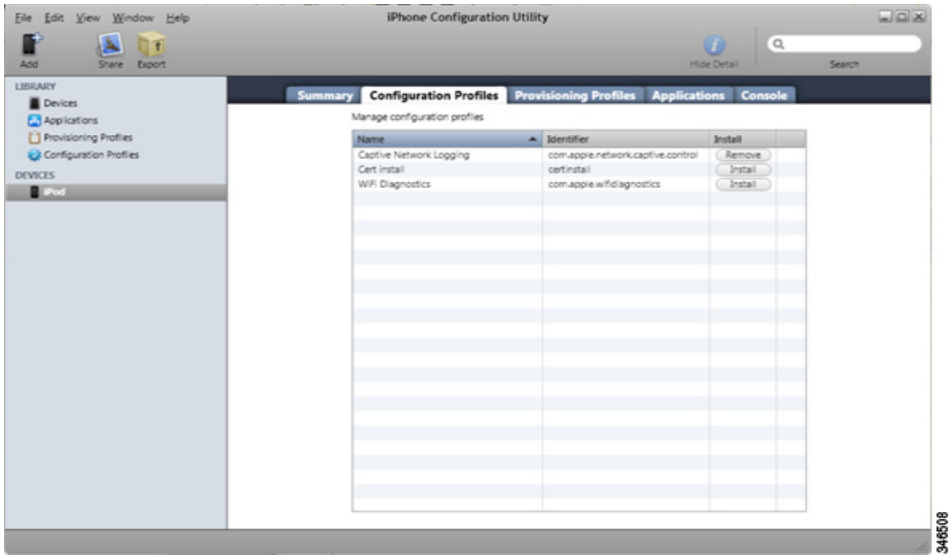


Figure 10 Trusted Certs Installed



When added to the trusted list, it can be seen as an installed profile on the device as shown in Figure 11:

Figure 11 Trusted Profile Installed

Webauth Session Time

As mentioned previously, the user will remain authenticated for the maximum duration of the session timeout, but other factors can affect how long a user will be allowed into the network before a new authentication process is needed. In general, the session timeout can be seen as the maximum time before the user has to authenticate, but other factors can trigger an earlier authentication request:

- **Idle timeout** — In case the user is no longer active, for example, the device is in sleep state, out of coverage, or turned off, the controller will remove the client after 5 minutes by default. This timer can be increased in case longer inactivity times are needed, but it will translate into a larger user count on average, as non-active users are kept for a longer time.
- **DHCP activity** — WebAuth state is tied to the IP / MAC address relationship. If due to DHCP renew process, or DHCP discovery attempts from the client, the WLC may trigger a WebAuth state remove if the client changes IP addresses during the process.
- **Roaming** — This is a very critical process for any 802.11 network. If during the roaming event the client fails to complete the full roaming to the new AP and/or WLC, it is possible that the client state will be removed, ending on a new WebAuth authentication step needed.
- **L2 policies** — For scenarios with a mix of layer 2 policy, like WPA2-PSK, and layer 3, like WebAuth, the client must comply with all requirements or it must be terminated. This provides an additional layer of security, but has the side effect that it may trigger client deletion on additional conditions. In particular, we should be aware of failed roam scenarios, where Extensible Authentication Protocol over LAN (EAPoL) exchange is not completed, or during broadcast key rotation, which by default happens every 60 minutes. The client must be able to answer to the EAP request from the AP, which triggers the group key rotation notification; it will be de-authenticated.

For scenarios of WebAuth and WPA2-PSK, it may be desirable to increase the EAP retries and the broadcast key rotation from the default in order to avoid client WebAuth state removal, if the devices are going to sleep. The command to change webauth session time configuration is **config advanced eap bcast-key-interval X**.

The default interval is 60 minutes.

Note Longer timers are not desirable from a strict security point of view.

For EAP requests, the command is **config advanced eap request-retries X**.

The default is two retries. This normally does not have any side effect, except for a longer time in the case of EAP errors, before a client is de-authenticated.

Troubleshooting

Using the WLC to Diagnose iPhone Issues

The Cisco APs are local to iPhone/iPad connection issues. They are sharing the same Wi-Fi conditions. Therefore, the WLCs, in conjunction with the APs, are an excellent source and a real-time source for a first-level debug.

What the APs see can be examined remotely and graphically. The WLC reports the Wi-Fi channel conditions surrounding the iPhone, and the WLC allows for remote testing of the iPhone. It reports the link connection quality of the phone. The WLC also reports the real-time quality of Wi-Fi, current interference devices, number of devices connected to the AP, number of calls on the AP, and what percentage of the Wi-Fi channel is utilized. This information is important for determining what is the source of a problem. And it can be done without engaging the end user directly.

Several documents on the Apple website reference using the WLC for low-level troubleshooting. Below are Cisco's recommendations, which provide environment and configuration insight on issues that may be hampering quality connections and quality application performance.

In Enterprise deployments it is not uncommon to have so many devices on a Wi-Fi channel that additional devices trying to make Wi-Fi network connections do not connect because of the lack of bandwidth. The iPhone may be blocked from a connection by parameters configured on the WLC. The WLC is the best tool to determine these types of conditions.

Several models of Cisco APs provide full spectrum analysis. Cisco provides a PC tool to examine in real-time from any remote location the spectrum analysis of those APs local to phone connections. The tool assists in the diagnostic process and may lead to a problem resolution related to Wi-Fi channel conditions without having to engage the phone and end user.

The WLC monitoring also provides a listing of rogue APs and adhoc rogue clients that may be the source of connection problems. Monitoring can be pushed to syslog servers, which can be added for a case. The logging can be configured to typical level and facilities.

Knowing the Wi-Fi Environment

The call quality and roaming performance of iPhones are proportional to the amount of AP coverage and Wi-Fi channel bandwidth. The WLC graphic interface as shown in Figure 12 provides data relative to those two conditions: **WLC > Monitor > Access Points > Radio(bands) > Statistics** is a link to a particular AP. On that page are numerous rows of information about the AP and Wi-Fi conditions in the coverage area of that AP. The data includes the Wi-Fi channel number, interference on that channel, current channel load statistics, number of Voice over IP (VoIP) calls, and other information.

Also shown on this window are the “Client Count vs RSSI” and “Client Count vs SNR”. This information provides insight as to the speed at which packets for the iPhone can be sent by understanding the data rate capabilities of the phone and what data rates might be in actual use during the phone call because of RSSI and SNR.

Following this information about the clients is the “Rx Neighbors Information” as shown in Figure 13. The neighbor information can be used to get a quick understanding of how much coverage overlap there is between the APs that neighbor the AP with which the phone is associated. The neighbor information is used in the 802.11k specification. This IEEE specification deals with radio management information.

Figure 12 AP and WiFi Conditions

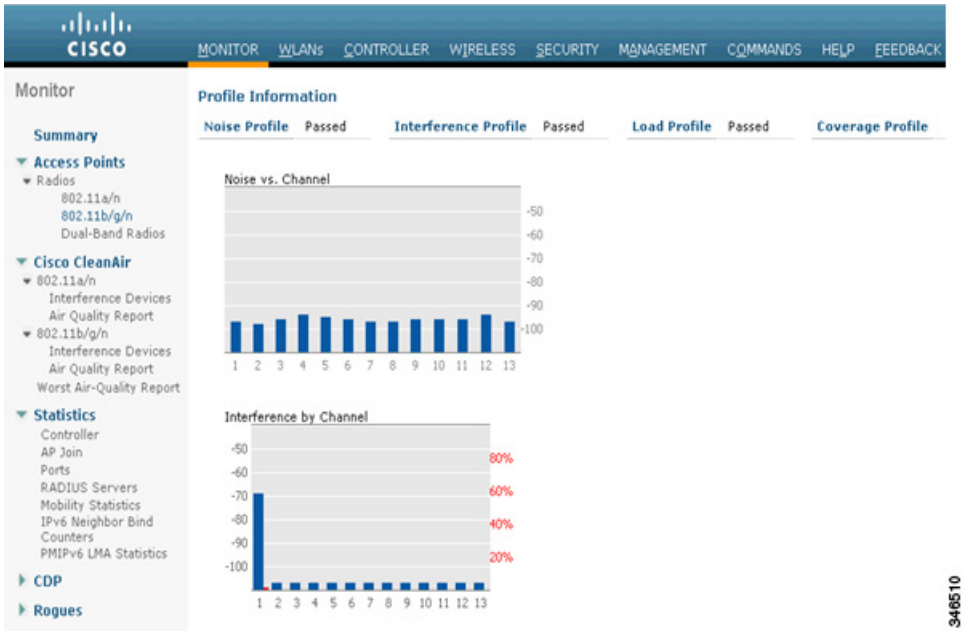
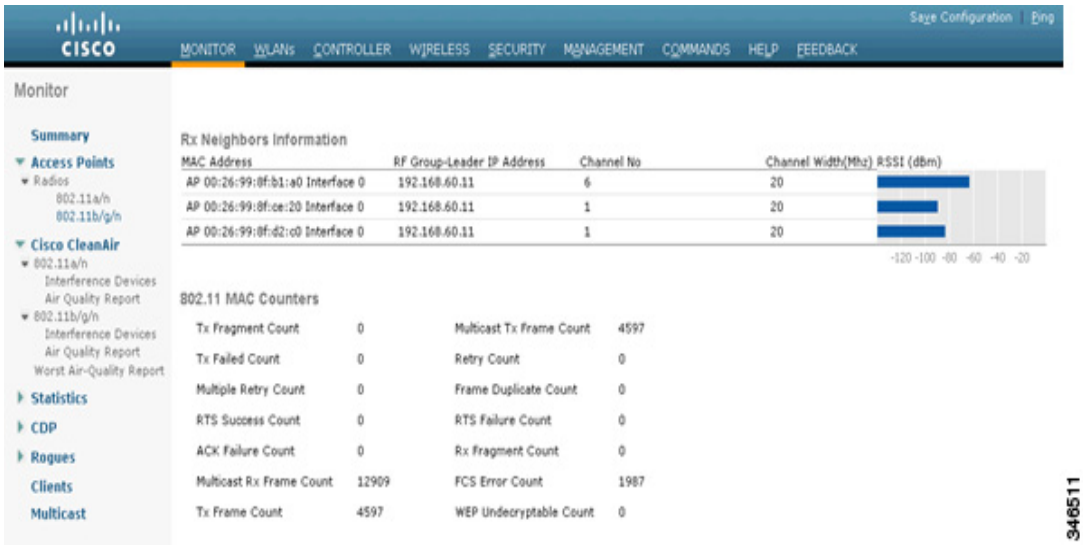


Figure 13 Rx Neighbors Information



Note Cisco's recommendation is that the overlap of Wi-Fi signals between AP neighbor cells is 15%. Please see the section in this document on "Wi-Fi Channel Coverage" section on page 2.

To view further information on WLC client statistics click the **Band Select Statistics** tab. This data shows how many dual-band devices like the iPhone5 are connected to the AP.

The next aspect of knowing the Wi-Fi environment of the iPhone is connection status. Again, the WLC provides a window of information about each individual phone. This information is in a database that is accessed by the Wi-Fi MAC address of the phone. To access that value form the phones own menu facilities choose **Settings > General > About > Wi-Fi Address**.

The MAC address of all phones currently associated to APs connected to the WLC are listed on the WLC at **Monitor > Clients**. Shown by row is the MAC address of the client, the AP name associated with the client, the WLAN SSID, and the 802.11 protocol. At the end of each row is a drop-down menu button. When you select this menu button, it displays a new window showing the current connection status of the iPhone. The information includes client properties and the properties of the AP to which the client is associated. Client properties include the IPv4 and IPv6 addresses, VLAN ID, current data rate set, security information, and QoS properties.

There are important Wi-Fi statistics in this window. The most important is the RSSI value. The RSSI field reports the signal strength of the packets received at the AP. This value indicates how well the client packets are being seen at the AP. An RSSI value of -45 dBm is a stronger signal than a value of -67 dBm. The RSSI value is important for knowing the coverage quality. If the value is too low then the phone will have poor call quality. It is also an indicator of whether there is a need for more APs or a need for a better AP. This RSSI value is an important indicator of a client's Wi-Fi performance. It should be used for product comparisons and site designs.

If the phone's audio packets are not being received at the AP, then the call will have one-way audio behavior. Packets with RSSI values that are in the range of -45 to -67 dBm will most likely be sent at the faster data rates. That is because these are both strong Wi-Fi signals. As the phone gets farther away from the AP the RSSI value will drop.

To compensate for the signal strength drop as the phone moves away from an AP, the data rates of each packet are slowed. This then provides a more reliable packet delivery but reduces the throughput of the phone and increases the bandwidth used by the phone. The increase in bandwidth required by the phone in turn reduces the available bandwidth in the Wi-Fi channel used by the phone and the AP. As bandwidth usage in the Wi-Fi channel increases, another Wi-Fi channel performance indicator increases. This indicator is channel utilization.

Channel utilization is one of the channel load statistics shown on the AP's radio statistics page. RSSI and channel utilization are two principle media factors in the quality of a call. The media is the Wi-Fi channel shared by the phone and the AP by way of their association. The Wi-Fi channel is also shared by other APs, other phones, and other devices, both Wi-Fi and non-Wi-Fi. The other Wi-Fi devices sharing the channel are contributors to the channel utilization as co-channel interferers. Non-Wi-Fi interferers are contributors to the channel utilization. Non-Wi-Fi interferers include Bluetooth devices, microwave ovens, surveillance cameras or any other device using the same radio frequency as the Wi-Fi channel but not using the 802.11 protocol. Rogue Wi-Fi devices and non-Wi-Fi interferers should be managed as best as possible to guard the channel utilization.

Another aspect of channel utilization management is to manage the number of valid devices and valid applications used in a Wi-Fi channel. The WLC can be configured to limit the number of audio calls, video calls and applications allowed on an AP and therefore the AP's Wi-Fi channel. The WLC configurations to manage this function include call admission control (CAC) and AVC.

Note These configuration options are covered in depth in the *Cisco Wireless LAN Controller Configuration Guide* at http://www.cisco.com/en/US/docs/wireless/controller/7.3/configuration/guide/b_cg73.html

For further information, note following content and sections of Cisco Validated Design (CVD) documents:

- The principles of Wi-Fi design for voice are covered in depth in the *Cisco Voice over Wireless LAN 4.1 Design Guide*: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html
- High Density Wi-Fi Deployments - review the sections labeled 'Design Points': http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10981/design_guide_c07-693245.html
- Bring Your Own Device - review the sections labeled 'User Experience' for 'Apple iOS devices and Cisco Jabber Clients':

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byoddg.html

Debugging a Wireless Client on the WLC

The command **debug client** <*MAC_Address*> is a macro that enables eight debug commands, plus a filter on the MAC address provided so that only messages that contain the specified MAC address are shown. The eight debug commands show the most important details on client association and authentication. The filter helps with situations where there are multiple wireless clients.

Note In Release 7.2 and later, the **debug client** command supports up to three clients simultaneously: **debug client** <*MAC_Addr1*> <*MAC_Addr2*> <*MAC_Addr3*>

The following debugs are enabled when **debug client** is executed:

```
(Cisco Controller) > show debug

MAC address.........................00:00:00:00:00:00
Debug Flags Enabled:
  dhcp packet enabled
  dot11 mobile enabled
  dot11 state enabled
  dot1x events enabled
  dot1x states enabled
  pem events enabled
  pem state enabled
```

These commands cover address negotiation, 802.11 client state machine, 802.1x authentication, Policy Enforcement Module (PEM), and address negotiation (DHCP).

The following **debug** commands can be added to **debug client** when troubleshooting various situations:

- 802.1x Authentication:
  - **debug aaa events enable**
  - **debug aaa detail enable**
- Web Authentication (as of Release 7.2 and later):
  - **debug web-auth redirect enable IPOFCLIENT**

The following are **debug** commands to use for 802.11k:

- (Cisco Controller) > **debug 11k ?**

- **errors** Configures debug of 802.11k errors
- **detail** Configures debug of 802.11k detail
- **history** Configures debug of 802.11k roam history
- **all** Configures debug of all 802.11k events
- **>debug 11k {all/event/errors/detail] [enable|disable]**

The following are **debug** commands to use for 802.11r:

- **11r / FT Debug**:
- (Cisco Controller) **>debug FT ?**
- **Events** Configures debug of 802.11k events
- **>debug ft events{enable|disable}**

Note For more information on debugging clients on the WLC, visit Understanding Debug Client on Wireless LAN Controllers (WLCs), or watch the video Troubleshooting Client Connection Issue on Cisco Wireless Controllers

Performing a Remote Packet Capture on Apple iOS Devices

In iOS5 and later releases you can remotely capture packets sent over the wireless adapter on an Apple iOS device. This capability adds a new dimension to troubleshooting on these platforms. Mac OS X running Xcode 4.2 or later is required. A remote virtual interface (RVI) will have to be configured on your Mac, which will create an interface allowing for capturing via Wireshark or other preferred OS X capturing utility.

To begin capturing on your iOS device:

Step 1 Connect the iOS device to a Mac via the USB cable.

Step 2 Download, and install Apple Xcode 4.2 or later at http://developer.apple.com/xcode/

Step 3 Locate your iOS Unique Identifier (UDID): Launch iTunes, and select your iPhone under **Devices** in the left column. Once selected, click on the **Serial Number** text to view your UDID. This value will be used in step 5.

Step 4 Launch the Terminal by choosing **Utilities > Terminal**.

Step 5 Create the RVI by using your iOS device's UDID:

```
MacBookPro:~ client$ rvictl -s UDID of iOS device

Starting device UDID of iOS device
SUCCEEDED
```

Note Use **ifconfig –l** to view a list of current devices.

Step 6 Begin capturing on the new rvi# interface via Wireshark or preferred capturing tool.

Step 7 Once finished, remove the RVI by issuing the following:

```
MacBookPro:~ client$ rvictl -x UDID of iOS device

Stopped device UDID of iOS device
SUCCEEDED
```

Note For more information on capturing packets on iOS devices, visit the Mac Developer Library: http://developer.apple.com/library/mac/#qa/qa1176/_index.html

Performing a Wireless Sniffer Capture

In order to understand how and why 802.11 Wi-Fi devices behave as they do, it is invaluable to perform a wireless packet capture, or "sniffer" action. This can be especially important when working with Cisco Technical Assistance Centre (TAC) to resolve a technical problem. The following articles will help you to choose and use a wireless sniffer:

- Fundamentals of Wireless Sniffing - Some Important Guidelines: https://supportforums.cisco.com/docs/DOC-19136
- Wireless Sniffing using a Mac with OS X 10.6 and Above: https://supportforums.cisco.com/docs/DOC-19212
- Wireless Sniffing in Windows 7 with Netmon 3.4: https://supportforums.cisco.com/docs/DOC-16398
- Collecting a Wireless Sniffer Trace using the Cisco Lightweight AP in Sniffer Mode: https://supportforums.cisco.com/docs/DOC-19214
- OmniPeek Remote Assistant: http://www.wildpackets.com/products/omnipeek_remote_assistant

Note The Linksys USB600N does not reliably collect 802.11n packets with short guard interval, for example, missing 20% to 30% of short guard interval packets. If necessary the WLC configuration can be changed only to use the slower long guard interval. This should be only a temporary configuration change. The command used is **config 802.11{a | b} 11n support guard-interval {any | long} .**

Additionally, there are several commercially available wireless sniffer products, for example:

- OmniPeek from WildPackets
- AirMagnet Wi-Fi Analyzer from Fluke
- CommView for Wi-Fi from TamoSoft
- AirPcap from Riverbed (formerly CACE)

Debugging and Logging on Apple iOS Devices

The iPhone Configuration Utility (IPCU) enables you to collect a series of enhanced logs from an iPad, iPhone, or iPod Touch:

- For Mac OS X - http://support.apple.com/kb/DL1465
- For Windows - http://support.apple.com/kb/DL1466

To begin collecting enhanced logs from your iOS device:

Step 1 Download and install the IPCU to a computer being used with the iPhone, iPad, or iPod Touch.

Step 2 Run the following Shell commands to enable debug logging options in the iPhone Configuration Utility:

In the Mac OS X:

Launch Terminal **Utilities > Terminal** and type the following:

- `defaults write com.apple.iPhoneConfigurationUtility`
- `EnableDebugLoggingInterface YES`

In the Windows OS:

Via the command line type the following:

- `cd c:\Program Files\iPhone Configuration Utility\`
- `ipcu.exe –enableDeviceLogCapture`

Step 3 Launch iPhone Configuration Utility and select the iPhone, iPad, or iPod Touch under Devices (left sidebar).

Step 4 Export a Device Profile under **File > Export >** (Mobile Device Profile), and save to a local directory.

Step 5 Click on the Console tab and choose "Save Log As" to save the console output to the same location used in Step 4.

For additional VPN, 802.1X, and/or Network output, continue with the steps below:

Step 1 Click on the Logging tab and check the appropriate options (VPN, 802.1X and/or Network).

Step 2 Click on the Summary tab and then disconnect the iPhone from the computer.

Step 3 Reproduce the failure condition under investigation.

Step 4 Reconnect the iPhone, iPad, or iPod Touch to the computer running iPhone Configuration Utility, and select the iPhone, iPad, or iPod Touch again under Devices.

Step 5 Under the Logging tab, click on **Download Logs**, and save to a local directory.

Note Before disconnecting the device, disable the appropriate logging options that were enabled in step 1 above.

Note For additional information on troubleshooting iOS devices, visit Enterprise iOS Support: http://www.apple.com/support/iphone/enterprise/

Debugging and Logging on Apple Mac OS X Supplicant

For OS X 10.6 and earlier:

Step 1 Launch Terminal **Utilities > Terminal**

Step 2 Collect get-mobility-info data:

```
MacBookPro:~ client$ sudo
/System/Library/Frameworks/SystemConfiguration.framework/Resources/get-mobility-info
Password: <Enter Password>
Please wait, collecting statistics
Network data collected to "/Users/client/Desktop/mobility-info-...tar.gz"
```

For OS X 10.7 and later:

OS X 10.7 (Lion) introduces a Wi-Fi Diagnostics Utility for additional Wi-Fi troubleshooting. The Wi-Fi Diagnostics Utility allows you to perform the following tasks:

- Monitor performance (signal, noise, BSSID, and so forth.)
- Record Wi-Fi events (associations, reassociations, deauthentications, and so forth.)
- Preform a wireless sniffer capture
- Enable debug logging

To open the Wi-Fi Diagnostics Utility:

Step 1 From the Finder, choose **Go > Go to Folder.**

Step 2 Type: */System/Library/CoreServices/*, and choose **Go**.

Step 3 Open **Wi-Fi Diagnostics.**

Logging 802.1x Authentication Failures on the OS X Supplicant

Step 1 Launch Terminal **Utilities > Terminal**

Step 2 Enable 802.1x logging:

```
MacBookPro:~ client$ sudo defaults write
Library/Preferences/SystemConfiguration/com.apple.eapolclient LogFlags -int -1
Password: <Enter Password>
```

Step 3 Restart the computer (to apply the setting).

Step 4 From the Finder, choose **Go > Go to Folder…**

Step 5 Type: */var/log/*, and choose **Go**.

Step 6 The supplicant logs will be titled “eapolclient.<interface>.log”.

Step 7 Once finished, to disable logging enter the following in Terminal:

```
MacBookPro:~ client$ sudo defaults write
/Library/Preferences/SystemConfiguration/com.apple.eapolclient LogFlags -int 0

Password: <Enter Password>
```

Step 8 Restart the computer (to apply the setting).

Summary of Recommendations

Several recommendations are made in this document, and these are summarized now:

- Cisco recommends a 5 GHz coverage design for dual-band devices. The channel utilization of the 5 GHz channels is generally much lower than the 2.4 GHz channels.
- Cisco recommends closely monitoring the channel utilization provided through the WLC reports. High channel utilization values may be an indication of new sources of interference, AP outages, or an influx of new Wi-Fi devices.
- Cisco recommends monitoring for APs changing channels frequently, and adding the identified 5 GHz Wi-Fi channels that are affected by known sources of interference to the DCA exclusion list.
- When doing coverage testing on 2.4 GHz it is recommended to have the lower data rates disabled. This is because the -67 dBm RSSI coverage area is much larger at 1 Mbps data rate than 12 Mbps. This is a range versus bandwidth design consideration.
- Cisco recommends the use of 802.11n on the 5 GHz band because beam forming (ClientLink) provides a better quality link and better call quality than 802.11a.
- Cisco recommends enabling the WLAN setting, “BandSelect”. While the iPhone5 does exhibit in some cases a bias to the 5 GHz band, enabling BandSelect can improve the percentage of connections on 5 GHz when a phone has appropriate signal strength to both bands.
- Cisco recommends iPhones and iPads be connected to a WLAN with a QoS value of platinum or voice and with WMM set to required. This allows the Ethernet traffic from the AP to connect to the switch port with a QoS value representative of the priority on the Wi-Fi channel.
- For Jabber and other business applications Cisco recommends platinum QoS so that application QoS levels can be obtained for packets that have a degraded WMM QoS value due to the device’s WMM driver or QoS policy.
- Cisco recommends configuring the WLC to enable RRM to provide both 2.4 GHz and 5 GHz AP channel numbers in the neighbor list response packets (802.11k). Cisco recommends the use of 5 GHz band Wi-Fi channels for not only Voice over WLAN calls but for all applications and devices.
- Cisco and Apple recommend that you configure an additional WLAN for fast transition 802.1x clients.
- Cisco and Apple recommend that you configure an additional WLAN for fast transition PSK clients.
- Apple recommends using separate WLAN and SSIDs for legacy clients.
- Cisco recommends managing data rates to provide the coverage that is suitable for the number of clients needed in the coverage of a channel, with bandwidth needed in the coverage of the channel.
- Cisco recommends for Channel Bonding use 20 MHz when channel density (e.g., high density environment) is needed, and consider 40 MHz when client traffic uses heavy bandwidth (e.g., video).
- Cisco highly recommends leaving all MCS rates enabled. Disabling some of the rates could potentially break compatibility with some versions of the 64-bit drivers on Mac OS 10.7 and 10.8.
- Cisco recommends that the overlap of Wi-Fi signals between AP neighbor cells is 15%.

For more information, see the following additional resources on Apple-related services and Cisco WLAN:

- Cisco Wireless LAN Apple Bonjour Deployment Guide:
  - http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_tech_note09186a0080bb1d7c.shtml

- Cisco Wireless LAN Controller System Management Guide, Release 7.4:
  - http://www.cisco.com/en/US/docs/wireless/controller/7.4/configuration/guides/system_management/config_system_management.html
- Mac Wi-Fi Update 1.0: http://support.apple.com/kb/DL1620

Note Cisco recommends periodically checking the reference links in this document and on Apple websites as well as general Cisco documentation for updates that may occur after publication of this best practices document.

Addendum A: IEEE IP DSCP - AVVID Values & 802.11e WMM

AVVID 802.1pUP based Traffic Type	AVVID 802.1pUP	AVVID IP DSCP	IEEE IP DSCP	IEEE 802.eUP	Comments
Reserved (Network Control)	7	56?	56	7	TBD
Reserved	6	48?			TBD
Voice	5	46(EF)	48	6	
Voice	4	34(AF41)	40	5	
Voice Control	3	26(AF31)	32	4	
Background(Gold)	2	18(AF21)	16	2	
Background(Gold)	2	20(AF22)	16	2	
Background(Gold)	2	22(AF23)	16	2	
Background(Silver)	1	10(AF11)	8	1	
Background(Silver)	1	12(AF12)	8	1	
Background(Silver)	1	14(AF13)	8	1	
Best Effort	0	0(BE)	0,24	0,3	
Background	0	2	8	1	
Background	0	4	8	1	
Background	0	6	8	1	
Unknown DSCP from wired	Access Port	D	Don’t care	D>>3	On the AP

Addendum B: Summary Matrix

	Wi-Fi Radios	11r Fast Transition Authentication	11k Neighbor Lists	Webex Client Available	Jabber Client Available
iPhone iPhone3G iPhone 4 iPad	11g 20Mhz wide channels only	No	No	Yes	Yes
iPhone 4S iPad2	2.4Ghz 11g & 11n MCS 0-7 20Mhz wide channels only	With iOS6 --Yes Yes	With iOS6 - Yes Yes	Yes	Yes
iPhone 5 iPad Retina iPad Mini	2.4 and 5 Ghz 11n MCS 0-7 20mHz wide on 2.4Ghz 20 or 40 Mhz on 5 Ghz	Yes	Yes	Yes	Yes

Addendum C: Acronyms

A-MDSU	Aggregated MAC Service Data Unit
ACL	Access Control List
AP	Access Point
AVC	Application Visibility and Control
AVVID	Architecture for Voice Video and Integrated Data
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certification Authority
CAC	Call Admission Control
CVD	Cisco Validation Design
DCA	Dynamic Channel Allocation
DS	Distribution System
DSCP	Differentiated Services Code Point
FT	Fast Transition
FTP	File Transfer Protocol
GHz	Gigahertz
GI	Guard Interval
IEs	Information Elements
IPCU	iPhone Configuration Utility
MAC	Medium Access Control
Mbps	Megabits per second
MCS	Modulation Coding Schemes
MOS	Mean Opionion Score
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
QoS	Quality of Service
RF	Radio Frequency
RRM	Radio Resource Management
RSSI	Received Signal Strenght Indicator
RToWLAN	Real-Time over Wireless LAN
RVI	Remote Virtual Interface
SKC	Sticky Key Caching
SNR	Singal-to-Noise Ratio
SSID	System Set Indentifier

TAC	Technical Assistance Centre
TSpec	Traffic Specification
UDID	Unique Identifier
VoWLAN	Voice over Wireless LAN
VPN	Virtual Private Network
WiSPR	Wireless Internet Service Provider Roaming
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller
WMM	Wireless Multimedia
WPA	Wi-Fi Protected Access