



## Enterprise Best Practices for Apple Devices on Cisco Wireless LAN

[Scope](#) 2

[Background](#) 2

[Wireless LAN Considerations](#) 2

[Quality of Service](#) 12

[Application Visibility and Control](#) 19

[Roaming Enhancements for Apple Devices](#) 22

[Wi-Fi Calling with Apple Devices on Cisco WLAN](#) 29

[Apple Bonjour on Cisco WLAN](#) 30

[Knowing your Wireless Environment](#) 31

[Apple Devices on Cisco WLAN Best Practices Summary](#) 37

[Additional Information](#) 38

Revised: May 23, 2016,

## Scope

This document is intended for IT professionals responsible for designing, deploying, and managing Cisco Wireless LANs (WLAN). This reference design guide is updated to account for Cisco and Apple's joint recommendations focused on the centralized (local) mode configuration for a controller based Cisco Wireless LAN. It assumes the reader has a working knowledge of Cisco WLAN components and features, basic IP networking and Voice over IP (VoIP). The best practices cover design considerations, recommended network setup, and configuration guidelines in order to provide best possible services for Apple devices on a Cisco Wireless LAN, while maintaining the infrastructure security.

This document highlights general best practices, and controller configurations for different use cases, and specific guidance for Apple iOS based devices like iPhone, iPad, iPod which are running iOS 9.0 operating system and above.

As per established enterprise best practices, and both Cisco and Apple's joint recommendation, the use of the 2.4 GHz band is not considered suitable for use for any business and/or mission critical enterprise applications. Cisco and Apple strongly recommends a 5 GHz-only (802.11a/n/ac) wireless network for Apple devices. This document focuses completely on a 5 GHz network layout as a best practice for all Apple Devices, and there are no recommendations for a 2.4 GHz-only or dual-band networks.

## Background

Today's Bring Your Own Device (BYOD) era has positively encouraged the end users to carry personal devices which can connect to a Wi-Fi network, with the majority of workplaces now seeing a minimum of 2-3 wireless capable devices per user. It has become necessary for IT administrators to design and develop the Wi-Fi infrastructure in order to rightly balance and accommodate an open access network environment, without reducing the security of network resources.

In addition to security concerns, these environments present a number of challenges in regards to quality of service, 2.4GHz vs 5GHz radio coverage, client roaming across an AP scenario, and the presence of legacy client devices on the wireless network. With more business critical applications being used by employees on personal devices, there is a high demand for a pervasive wireless connectivity in parallel to responsive application performance.

Apple iOS based smartphones and tablets constitute a significant presence in today's Enterprise environments. In order to ensure the best possible service for Apple devices, a number of different factors have to be considered including RF conditions, client connectivity, network visibility, quality of service, and network monitoring. This document includes important guidelines on how to configure the Cisco Wireless LAN Controller (WLC) with respect to these factors.

## Wireless LAN Considerations

Deploying real-time applications, such as Voice over WLAN (VoWLAN), on a shared medium like Wi-Fi in a production environment requires careful planning, consideration, and design. Many administrators are asked to add VoWLAN onto an existing wireless infrastructure originally designed to meet very different needs. Others have the benefit of starting from scratch and taking VoWLAN into consideration in the original design. Either path raises an important question for the administrator: how can I ensure the best possible end-user experience in my Cisco environment?

Apple continually adds support for industry-standard technologies that enhance the connectivity as a VoWLAN client; however, some of these enhancements are only supported on specific Apple devices and iOS software releases. It is important to learn which Apple device (and iOS release) are expected to be used on your wireless network in order to tune your network to its maximum potential. To assist in this process, Apple maintains a series of knowledge base articles that list which devices support the various technologies as described in the [Apple Roaming on iOS](#) document.

Although many of the enterprise feature like 802.11r and 802.11k were introduced starting with Apple iOS 6.0 update, Apple recommends upgrading all the devices to the latest iOS 9 or above.



---

**Note** Refer to Device Classification Chart for details on 802.11 & Enterprise Features for Apple Devices: [http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/device\\_classification\\_guide.pdf](http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/device_classification_guide.pdf)

---

## RF Design Guidelines for Apple Devices on Cisco WLAN

The first step in a wireless LAN (WLAN) deployment is to ensure that desired operation begins with a site survey to assess the Radio Frequency (RF) behavior in a specific environment. Many issues can arise in a wireless network due to poor planning and resulting poor coverage. While analyzing existing wireless deployments, it's often discovered that site surveys are not performed properly or the site survey has been omitted altogether.

One key factor for continued success is to make sure that the site survey takes into account the current and future needs of the wireless devices and applications in use. This must include use cases and account for various device types that you plan on using and deploying on the wireless network in the foreseeable future. Different use cases have different site survey methodologies. For instance, a general use (data or voice) only site survey can vary significantly from a mission critical network that requires voice, video, data and location based services.

Different devices such as laptop and smart phones, have different wireless characteristics that must be taken into account during the design and site survey of the wireless network. It also helps to understand what the transmit power characteristics of the wireless client devices to ensure that access points and associated devices transmit at a similar RF power level. Cisco finds that the typical max transmit power for most iOS devices fall in the range of 9 dBm to 14 dBm, depending on the model and AP Channel.

## RF Design Recommendations for Apple Devices on Cisco WLAN

- 1 The use of 802.11a/n/ac 5GHz based design for all Apple devices
- 2 Optimal Cell edge recommendation for Apple Devices is -67 dBm or better (-65 dBm is better for typical high density enterprise deployments). An optimal WLAN deployment will require minimum of 2 APs in 5 GHz at -67 dBm as measured by the Apple client
- 3 Average Channel Utilization should be less than 40%
- 4 Maintain a minimum Signal to Noise Ratio (SNR) of 25 dB
- 5 802.11 retransmissions should be kept under 15%
- 6 Packet Loss should remain under 1 percent and jitter should be kept to less than 100 ms

These are general recommendations and may not fully address any potential transmit power changes in some situations like full and low battery levels, along with possible attenuation when the device is actively being covered with hands while in use, or passively stored when not in direct use (in the pocket)

**Table 1: Basic steps to a successful RF design**

Step	Description	Purpose
1	Definition	Define what applications and clients will be deployed and who the stakeholders are.

Step	Description	Purpose
2	Coverage areas and project phases	Define what areas within the campus will support only general applications, and voice plus general applications on the wireless network.
3	Plan approval	Gain buy-in of all key stakeholders.
4	RF audit and site survey	Validate and adjust design.
5	Deploy infrastructure	Implement design.
6	RF test	Test implementation on deployed infrastructure.
7	Final adjustments	Adjust access point settings.
8	Ongoing operation support	Transition to sustaining support with adaptation to usage changes.



**Note**

---

Refer to Site Survey RF Design Validation Guide for more details:<http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html>

---

## Wi-Fi Channel Coverage

Cisco and Apple recommend a 5 GHz only coverage design when designing for Apple devices on a Cisco wireless network. The channel utilization of the 5 GHz channels is generally much lower than the 2.4 GHz channels, and there are more channels available for the network to reuse.

**Figure 1: Configuring Radio Policy to 5GHz (802.11a only)**

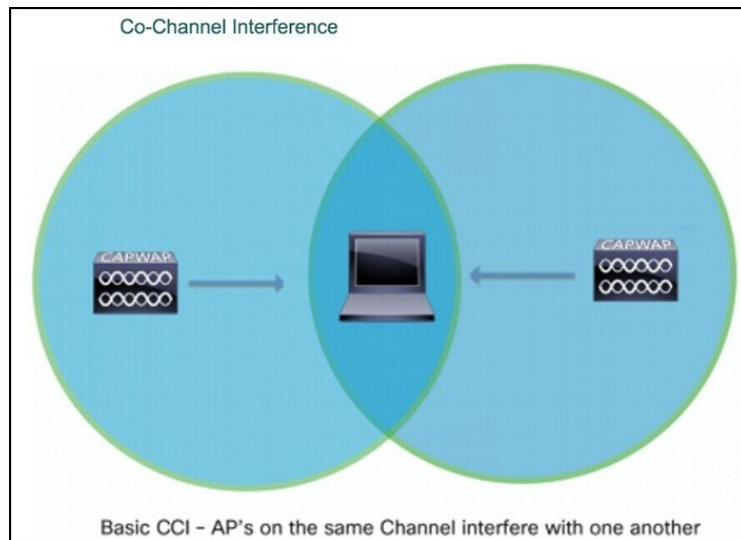
The screenshot displays the Cisco WLAN configuration interface. The top navigation bar includes tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows a tree view with 'WLANs' expanded, containing 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > Edit 'Cisco-Apple'' and features five tabs: General, Security, QoS, Policy-Mapping, and Advanced. The 'General' tab is active, showing the following configuration details:

Profile Name	Cisco-Apple
Type	WLAN
SSID	Cisco-Apple
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	802.11a only
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	Cisco_5508_1

The 'Radio Policy' field is highlighted with a green border, indicating the selection of '802.11a only'.

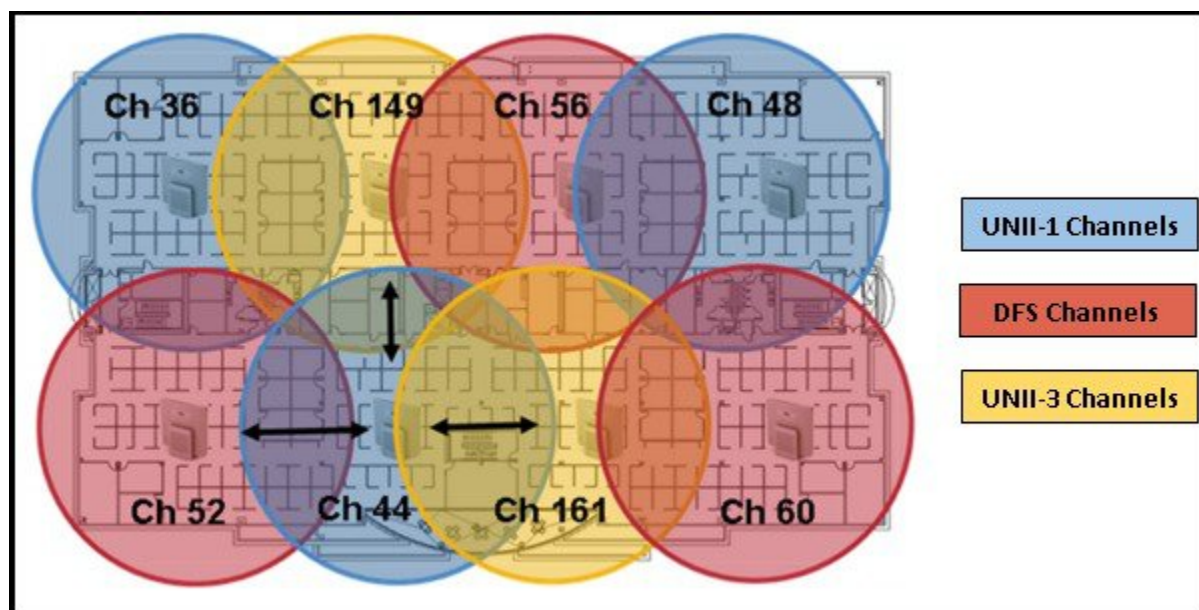
The 5 GHz channels are free of common devices operating on 2.4GHz frequency such as Bluetooth interference, video cameras, and microwave ovens. With more channels being available as compared to 2.4GHz, the channel utilization on the 5 GHz band is generally lower due to the reduced channel re-utilization (co-channel interference) and channel overlap.

**Figure 2: Access Points on the same channel causes co-channel interference**



For reasons of channel capacity and co-channel interference situations, you may need to use Dynamic Frequency Selection (DFS) channels. DFS is the process of detecting radar signals used by departments such as military and weather, which must be protected against interference from 5 GHz radios running over the Wi-Fi networks. Upon detection, the AP must switch the operating channel of the 5 GHz radio, and move to a channel that is not interfering with the radar systems.

**Figure 3: Channel distribution example in a 5GHz network design**



Cisco and Apple recommends to carefully monitor the DFS Channels for radar activity via the controller traps in order to plan and avoid frequent DFS events causing periodic channel changes across APs.

Considering optimal application performance, a wireless network typically reaches capacity when the utilization reaches between 40 to 50% on an average. For latency sensitive and real time applications like VoWLAN, channel utilization over 30% may potentially impact the end-user experience. 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 that customers create a baseline measurement of their existing client count, number of clients per Access Point, configured channel numbers and current channel utilization prior to deploying additional devices.

Cisco's Radio Resource Management (RRM) is enabled on the controller by default, and was designed to manage the RF environment in a dynamic way with little to no user intervention. RRM calculates and assigns the best channels and power combinations using measured, over-the-air metrics. RRM keeps track of high utilizations on all channels, and will mitigate co-channel assignments and balance power. If there are no open channels available, or the AP's are simply too close together the only choice remaining is sharing the channel with an existing user. This happens in congested environments and two different networks may have to share the same bandwidth.

Cisco recommends to carefully monitor the 5 GHz Wi-Fi channels that are affected by continuous high channel utilization conditions, and be added to the Dynamic Channel Allocation (DCA) exclusion list in case the interference is recurring or cannot be managed. Excluding a channel from the DCA list should be utilized as a last resort measure. Cisco recommends channel exclusion with the use of [RF profiles](#) to effectively apply the removal of the channels to only the affected APs, and not globally across all APs.



---

**Note** Refer to RRM guidelines in Enterprise Mobility Design Guide for more details: [http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise\\_Mobility\\_8-1\\_Deployment\\_Guide.pdf](http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide.pdf)

---

To estimate if the current 5 GHz AP coverage is sufficient for the applications running on iOS devices, Cisco Wireless LAN Controller (WLC) provides a friendly link test tool to determine the Access Point's view of the client signal; in addition to this, Apple also provides a wireless network scanner for iOS in their [AirPort Utility](#) app. A Signal to Noise (SNR) of 25 or higher should be maintained at all times.

Performing a Link Test from the controller interface

- 1 On the controller GUI, choose **Monitor > Clients** to open the Clients page.
- 2 Hover your cursor over the blue drop-down arrow for the desired client and choose Link Test. A link test page with results will pop up.



Link Test Results

Client MAC Address00:1c:58:cd:46:fe

AP MAC Addressb0:aa:77:85:11:30

Packets Sent/Received by AP20/20

Packets Lost (Total/AP->Client/Client->AP)0/0/0

Packets RTT (min/max/avg) (ms)4/48/9

RSSI at AP (min/max/avg) (dBm)-60/-58/-58

RSSI at Client (min/max/avg) (dBm)-58/-56/-56

SNR at AP (min/max/avg) (dB)31/39/36

SNR at Client (min/max/avg)(dB)0/0/0

Transmit retries at AP (Total/Max)1/1

Transmit retries at Client (Total/Max)0/0

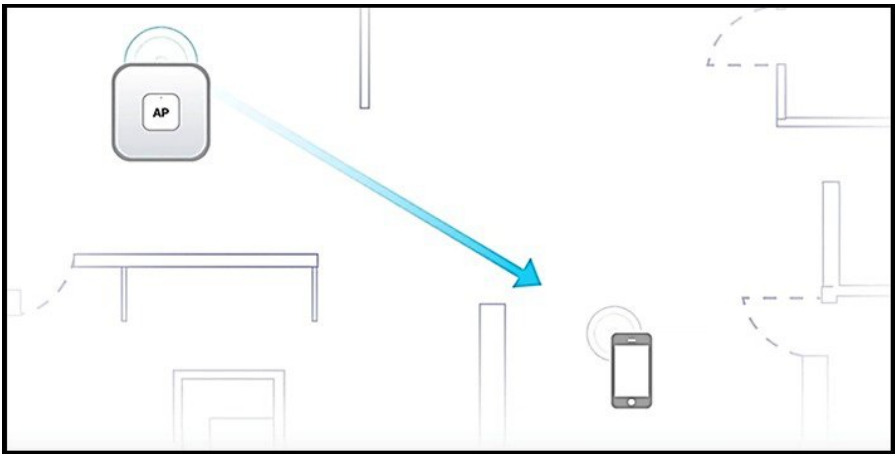
Packet rate	1M	2M	5.5M	6M	9M	11M	12M	18M	24M	36M	48M	54M						
Sent count	0	0	0	0	0	0	0	0	0	0	0	20						
Receive count	0	0	0	0	0	0	0	0	0	0	0	20						

Packet rate(mcs)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
Sent count	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
Receive count	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		

## ClientLink Beamforming

Cisco's patented beamforming technology – **ClientLink** functions to optimize the connection reliability for mobile devices like Apple iPhone and iPad. This technology is based on signal processing enhancements to the access point chipset and does not require changes to network parameters. Most of the newer Apple devices now support beamforming, but ClientLink benefits all wireless client devices – old and new, regardless of the client beamforming capabilities since its functionality is independent of any assistance from the client device. ClientLink uses algorithms to calculate estimates of the wireless channel conditions so the access point can adjust the RF for the transmitter and receiver antennas accordingly in order to benefit the client connectivity. It is enabled on the Cisco AP by default, and continuously operates in the background at all times.

**Figure 4: Cisco ClientLink technology improves connectivity by optimizing signal to each Apple device**



The core benefit of ClientLink technology is improved quality of Wi-Fi signal between the AP and the wireless client devices. The resulting high quality link between the AP and the client device increases the chances of the client to remain connected at a higher data rate, and promotes the quality of coverage for all wireless clients across the Wi-Fi network. In addition to providing gain in an



indoor multipath environment, ClientLink also provides increased SNR at the client in line-of-sight environments such as outdoors or large open indoor spaces.

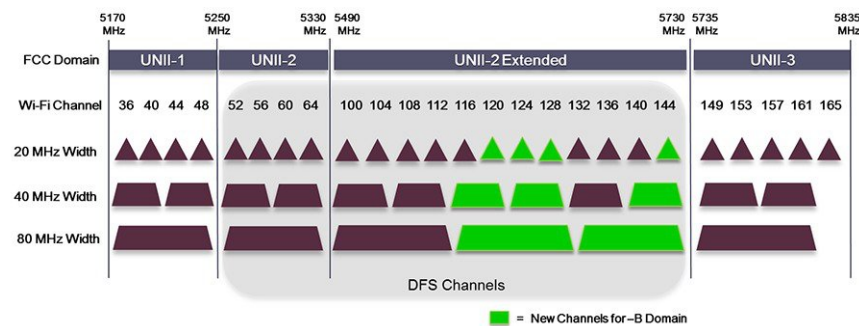


**Note** Refer to ClientLink 3.0 Whitepaper for more details: <http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3700-series/white-paper-c11-731150.html>

## Wi-Fi Channel Bandwidth

In 802.11a, a 5GHz channel uses channel width of 20 MHz. With the adoption of 802.11n and 802.11ac, channel bonding capability was added to allow multiple 20MHz channels to bond together and form a single channel with a larger width. By doubling the channel bandwidth from 20 to 40 MHz, a single transmission can carry twice as much data at the same time, effectively doubling the throughput of the wireless network. With 802.11ac, 5 GHz offers you a choice of 20 MHz, 40 MHz and 80 MHz (160 MHz with 802.11ac - wave 2) channel width modes.

**Figure 5: Channel bonding example for 20 MHz, 40 MHz and 80 MHz channel widths on a 5GHz network**

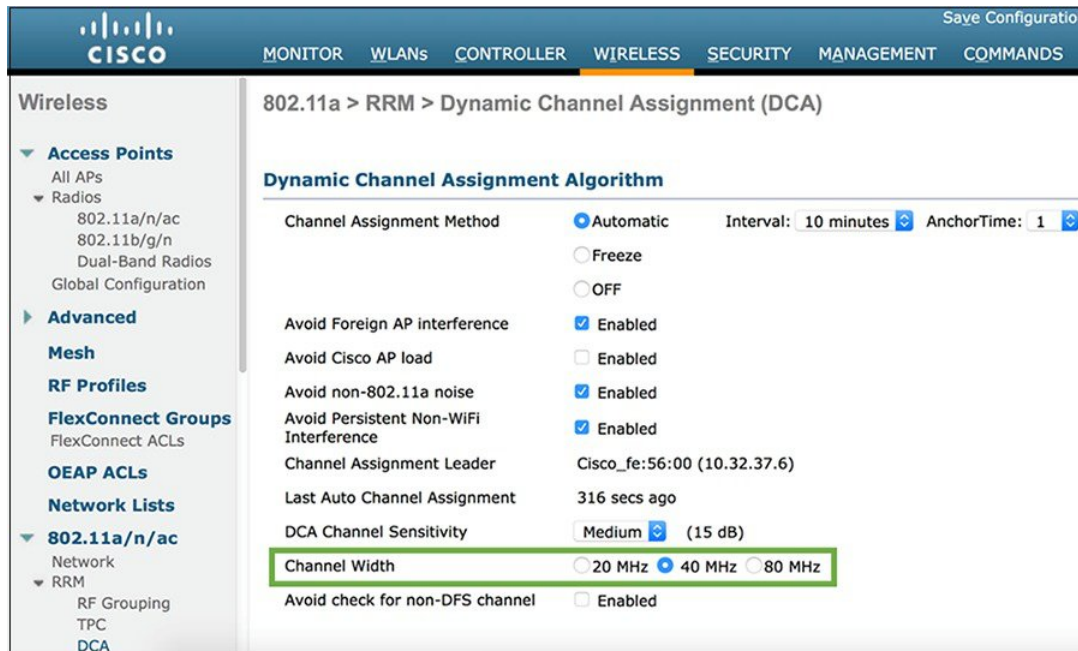


Cisco and Apple recommends the use of 40 MHz channel widths in environments where performance is required and 20 MHz for high AP density deployment environments. To allow for an efficient 40-MHz wide deployment the use of DFS channels becomes necessary in order to achieve optimal frequency re-use, and reduce the likelihood of co-channel Interference. Without DFS channels enabled in an FCC regulated domain, 4 - 40MHz channels are available. By enabling DFS channels, the number of 40MHz channels available increases to 10.

Although using 80 MHz wide channel bonding may at first seem to boost an individual client performance, in a high AP density environment, the co-channel interference due to limited spectrum availability can potentially reduce the overall network performance.

It is therefore not yet recommended to use 80 MHz channel width design. If necessary, it should only be considered for low AP density deployments where co-channel interference can be easily avoided.

**Figure 6: Configuring channel width from the controller user interface**



Navigate to **Wireless > 802.11a/n/ac > RRM > DCA** and specify the width of the channel to be used.



**Note**

Refer to DCA guidelines in Enterprise Mobility Design Guide for more details: [http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise\\_Mobility\\_8-1\\_Deployment\\_Guide.pdf](http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide.pdf)

## 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. Two possible paths can be taken:

- **Maximizing range:** If the requirement is to increase the range, consider enabling low data rates. 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. Going with the maximize range approach may impact application performance for the client devices especially for time-sensitive voice-video type of applications. Lower data rates typically require more air time and overall cell capacity (user experience) can potentially be reduced.
- **Maximizing 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 on the minimum data rates as this could prevent a client device from establishing a reliable connection and actually result in decreasing the performance.

The IEEE 802.11a/n/ac standard provides data rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps, with 54 Mbps being the maximum data rate.

**Figure 7: Configuring the Data Rates for the 5GHz network**

**802.11a Global Parameters**

**General**

802.11a Network Status	<input checked="" type="checkbox"/> Enabled
Beacon Period (milliseconds)	100
Fragmentation Threshold (bytes)	2346
DTPC Support	<input type="checkbox"/> Enabled
Maximum Allowed Clients	200
RSSI Low Check	<input type="checkbox"/> Enabled
RSSI Threshold (-60 to -90 dBm)	-80

**802.11a Band Status**

Low Band	Enabled
Mid Band	Enabled
High Band	Enabled

**Data Rates\*\***

6 Mbps	Disabled
9 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Mandatory
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

**CCX Location Measurement**

Mode ☐ Enabled

\*\* Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies

Navigate to **Wireless > 802.11a/n/ac > Network** to specify the rates at which data can be transmitted between the AP and the client.

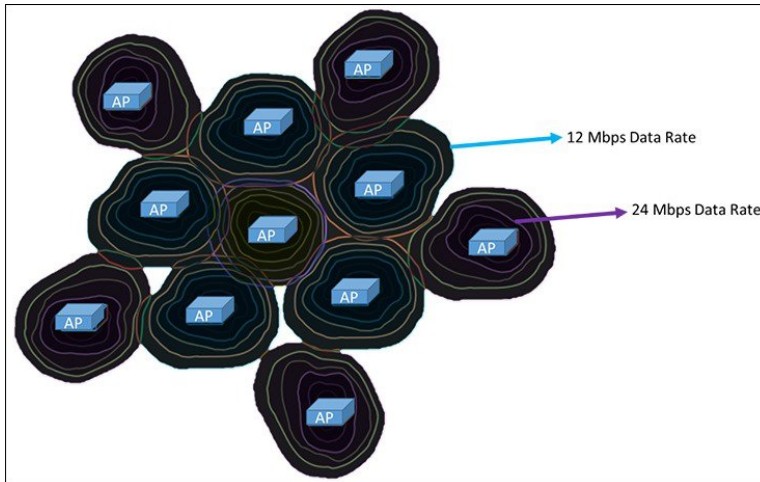
You can set each data rate to one of three modes:

- **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.

Configuring low data rates as mandatory 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. Although this increases the cell size of the access

points, and in a site with few APs this may be desirable, but if the density of mobile clients is high, this will likely rob the site of bandwidth and lead to poor application performance.

**Figure 8: Example to show how data rates impact the cell size for the APs in client's perspective**



Cisco and Apple recommends a minimum data rate of 12 Mbps, and enabling 12 Mbps and 24 Mbps as the two mandatory data rates as a general best practice for Apple devices on Cisco Wireless LAN. If the 5GHz coverage is marginal, setting 6 Mbps as the lowest mandatory rate could potentially resolve issues.

It is advisable to keep a check on the administration logs, traps, and alerts using controller dashboard and [Cisco Prime Infrastructure](#), in order to monitor and verify that client devices are connecting to the network at the configured data rates. Indications that data rates are not set properly may include:

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

## Quality of Service

In order to achieve optimal results for applications running on Apple devices associated to Cisco WLAN, it is crucial to implement the correct end-to-end quality of service (QoS). Wi-Fi traffic can display a prioritization value, expressed through a User Priority (UP) tag present in the 802.11 header and defined by the 802.11e amendment. This User Priority is also known as the Traffic Identifier (TID). It can receive any value from 0 to 7. Traffic with higher UP typically receives a more expedited over-the-air treatment. The Wi-Fi Alliance ensures interoperability between vendors applying 802.11 QoS marking and prioritization through the Wi-Fi Multimedia (WMM) certification. The SSID configuration on Cisco controller defines the highest priority allowed for traffic forwarded to and from the WLAN.

## Wireless QoS

Different vendors may use different translation mechanisms and values between Wi-Fi QoS marking and Wired QoS marking. Cisco uses DSCP marking downstream, and can use Layer 2 or Layer 3 marking upstream. Cisco follows the IETF marking translation recommendations (for example: [RFC 4594](#), which is the latest IETF guidelines on DSCP traffic marking) and the 802.11e mapping.

**Table 2: Applied QoS marking for the main categories of traffic**

<b>Cisco 802.1p User Priority Traffic Type</b>	<b>IP DSCP (PHB Value)</b>	<b>IEEE 802.11e/WMM User Priority</b>	<b>Designative (Informative)</b>	<b>Cisco Designative</b>
Reserved	56 - 63	7 (unused)	—	—
Reserved	48 - 55	6 (unused)	—	—
Voice	46 (EF)	6	Voice	Platinum
Interactive Video	34, 36, 38 (AF4x)	5	Video	Gold
Streaming Video	26, 28, 30 (AF3x)	4	Video	Gold
Voice Control (Signaling)	24 (CS3)	4	Video	Gold
Background (Transactional/Interactive Data)	18, 20, 22 (AF2x)	3	Best Effort	Silver
Background (Bulk Data)	10, 12, 14 (AF1x)	2	Background	Bronze
Best Effort	0 (BE)	0	Best Effort	Silver
Scavenger	8 (CS1)	1	Background	—



**Note**

IEEE 802.11e UP value for DSCP values that are not mentioned in the table is calculated by considering 3 MSB bits of DSCP. For example, the IEEE 802.11e UP value for DSCP 32 (100 000 in binary), would be the decimal equivalent of the MSB (100) which is 4. The 802.11e UP value of DSCP 32 is 4.

In AireOS controller code 8.1 and prior, the above mentioned translation uses a static mapping table and UP value for upstream mapping. From AireOS 8.1MR release, users can decide custom DSCP values for upstream mapping using the QoS Mapping option.

**Figure 9: Applying custom UP to DSCP mapping values with AireOS 8.1MR**

**QoS Map Config**

Qos Map: Enable

Trust DSCP UpStream: ☐

**UP to DSCP Map**

User Priority: 0

DSCP Default: 0

DSCP Start: 0

DSCP End: 0

Modify

**Add DSCP Exception**

DSCP Exception: 0

User Priority: 0

Add Clear All

**DSCP Exception List**

	DSCP	UP
0	255	255
1	255	255
2	255	255
3	255	255
4	255	255
5	255	255
6	255	255
7	255	255

Navigate to **Wireless > QoS > QoS Map** to implement the UP to DSCP mapping values.

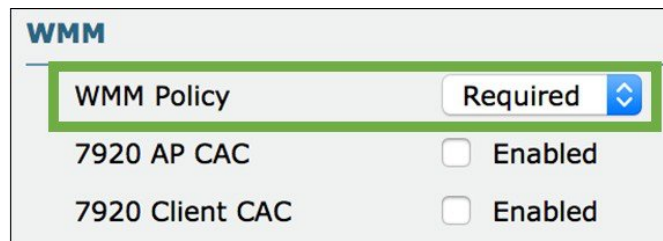
## Wi-Fi Multimedia

Wi-Fi Multimedia (WMM) is the standardized form of Quality of Service for wireless networks, and is based upon the 802.11e amendment. Cisco and Apple both provide robust support for WMM at the network and application layers.

There are different use cases for the WLAN setting of WMM. When WMM is set to disabled, WMM QoS is not used to queue or mark the packets. With QoS being disabled, there is no marking for any packet. Therefore, if a ping sent to an Apple iPhone device will be sent at a Best Effort (BE) priority even when the WLAN QoS setting is voice or platinum. For these reasons, the recommended

setting for WMM is 'allowed' or 'required' depending on the use case. If the WLAN or SSID is for Apple devices only, then it is recommended to go with the 'required' setting.

**Figure 10: Configuring WMM on the WLAN**



WMM	
WMM Policy	Required
7920 AP CAC	<input type="checkbox"/> Enabled
7920 Client CAC	<input type="checkbox"/> Enabled

Navigate to **WLAN > QoS** and choose **Required** as the WMM setting.

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.



**Note** Non-WMM clients will not be able to connect to a WLAN which is set to have WMM Policy as 'Required', even if the WLAN has no security. To support Non-WMM clients, a separate SSID/WLAN is recommended to allow connectivity to the network.

Administrators should be aware that the WMM controls at the controller can only guarantee that downstream packets to the client are marked as defined. The client and application has to appropriately support WMM for the upstream traffic. Fortunately, Apple's iOS devices can support the network-level WMM settings (e.g. platinum or voice) in addition to application-layer support. Apple provides application developers the ability to mark their packets at the application layer that ensure specific packets queued to appropriate WMM level. Application developers should [ensure that the iOS application tags](#) the appropriate WMM marking so client's upstream traffic is properly tagged.

## WLAN QoS Profiles

From the Cisco WLAN Controller user interface, you can assign a QoS profile (Platinum, Gold, Silver, and Bronze) to each SSID. This profile determines the highest QoS level expected and allowed to be used on this SSID. The role of a QoS profile is to set the ceiling (the maximum level of QoS that clients are allowed to use). For example, if you set a silver profile on a WLAN, clients can send lower priority traffic such as background. Any traffic marked with a higher QoS value (say Voice or Video) will be down-marked to Silver (BE, DSCP 18).

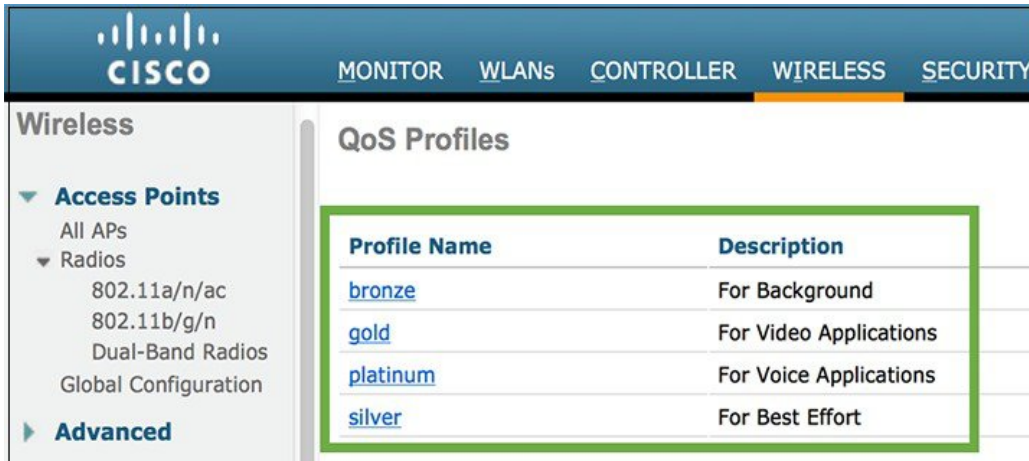
The profile also determines what marking behavior should be used for incoming non-WMM traffic, traffic without a DSCP marking, and for multicast traffic. When incoming traffic exceeds the maximum QoS value of the profile, the traffic is remarked to match the maximum QoS value assigned to the profile.

Similarly, if you set platinum, the clients are allowed to use the highest QoS tag/class (Up to UP6/DSCP EF). This does not mean that all traffic is considered as voice traffic. It means that, if for example an iPad sends voice traffic, it is treated as such, and, if it sends best effort traffic (as the majority of non-real-time applications send), it is treated as best effort.



Setting the WLAN QoS parameters allows additional configuration to granularly handle non-WMM or unknown traffic on the WLAN where the Apple devices communicate.

**Figure 11: Verifying QoS Profile configurations**



Wireless	
MONITOR   WLANS   CONTROLLER <b>WIRELESS</b> SECURITY	
QoS Profiles	
Profile Name	Description
<a href="#">bronze</a>	For Background
<a href="#">gold</a>	For Video Applications
<a href="#">platinum</a>	For Voice Applications
<a href="#">silver</a>	For Best Effort

The individual QoS profile settings are available on the **Wireless > QoS** tab.

The unicast default priority is allotted to any incoming unknown traffic marking. This setting decides on what should be done for traffic for non-WMM traffic or traffic with unknown marking. Setting the unicast default priority and multicast default priority to best effort will prevent the undesired prioritization on the WLAN.

**Figure 12: Configuring the QoS Profile Parameters for unicast and multicast Traffic**

The screenshot shows the Cisco Wireless configuration interface. The left sidebar contains a navigation menu with options like Access Points, Radios, Advanced, Mesh, ATF, RF Profiles, FlexConnect Groups, OEAP ACLs, Network Lists, 802.11a/n/ac, 802.11b/g/n, Media Stream, Application Visibility And Control, Lync Server, and Country. The main content area is titled 'Edit QoS Profile' and shows the configuration for the 'platinum' profile. The 'Description' is 'For Voice Applications'. There are sections for 'Per-User Bandwidth Contracts (kbps) \*' and 'Per-SSID Bandwidth Contracts (kbps) \*', each with a table for DownStream and UpStream rates. The 'WLAN QoS Parameters' section is highlighted with a green box and contains three settings: Maximum Priority (voice), Unicast Default Priority (besteffort), and Multicast Default Priority (besteffort).

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

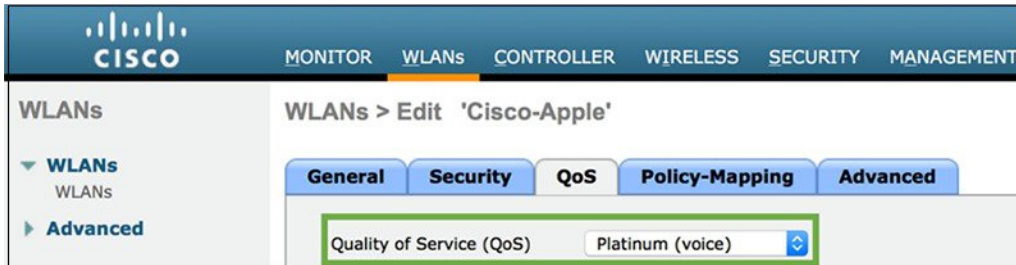
	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WLAN QoS Parameters	
Maximum Priority	voice
Unicast Default Priority	besteffort
Multicast Default Priority	besteffort

Navigate to **Wireless > QoS > Profiles > Platinum** tab, choose best effort for Unicast Default Priority and Multicast Default Priority. Based on the QoS profile assigned to the WLAN for the apple devices, you will need to make the parameter changes accordingly.

To honor the traffic marked as voice for all apple devices, it is recommended to make the WLAN QoS set to 'Platinum'.

**Figure 13: Configuring the QoS Profile on the WLAN**



Navigate to **WLANs > QoS** tab of the WLAN SSID to assign the Quality of Service profile to the WLAN.

## Wired Switch Port Configurations

The wired side of the infrastructure also needs to be compatible with the DSCP honoring to allow a complete end to end priority structure. The QoS configuration of the switch port connecting the access point should trust the DSCP of the packets exchanged between the access point and the controller.

Following 3750X and 2960 switch port configuration examples addresses the classification and queuing commands that can be added depending on local QoS policy.

### Cisco 3750X and 2960 Example

#### Wireless LAN Controller EtherChannel Switch Port:

```
interface GigabitEthernet1/0/1
  description Wireless LAN Controller Connection port 1
!
interface GigabitEthernet2/0/1
  description Wireless LAN Controller Connection port 2

interface range GigabitEthernet 1/0/1, GigabitEthernet 2/0/1
  switchport
  mls qos trust dscp
  srr-queue bandwidth share 1 30 35 5
  priority-queue out
  channel-group 1 mode on

interface Port-channel 1
  description EtherChannel to Wireless LAN Controller
  switchport trunk allowed vlan 116, 120, 275
  switchport mode trunk
  spanning-tree portfast trunk
```

#### Access Point Switch Port Example:

```
interface GigabitEthernet1/0/2
  description Access Point Connection Centralized Switching
  switchport mode access
  switchport access VLAN 100
  switchport host
  mls qos trust dscp
  srr-queue bandwidth share 1 30 35 5
  priority-queue out
```

In trusting the access point DSCP values, the access switch trusts the policy set for that access point by the WLC. The maximum DSCP value assigned to client traffic is based on the QoS policy applied to the WLAN on that access point.

**Note**

Refer to QoS guide for wired switch port configuration examples: [http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2015/CVD-Campus\\_LAN\\_L2\\_Access\\_Simplified\\_Dist\\_Deployment-Oct2015.pdf](http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2015/CVD-Campus_LAN_L2_Access_Simplified_Dist_Deployment-Oct2015.pdf)

## Application Visibility and Control

Cisco's Application Visibility and Control (AVC) classifies applications using deep packet inspection techniques with the Network-Based Application Recognition (NBAR) engine, and provides application-level visibility and control into Wi-Fi networks. Using AVC, the controller can detect more than 1000 applications including voice/video, email, file sharing, gaming, and peer-to-peer applications. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.

The recognition of business applications is supported from AVC protocol pack 6.4 and above, operating with next-generation Network-Based Application Recognition (NBAR2) engine 13 and above. With this capability, you can correctly identify all the applications running on the apple devices and also sub-classify how much of your traffic is data, audio, video, and apply different policies on those.

**Note**

Refer to the Application Visibility Control FAQ page for more info on AVC and Protocol packs: [http://products.mcisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/qa\\_c67-722538.pdf](http://products.mcisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/qa_c67-722538.pdf)

After the applications are recognized, the AVC feature enables you to either drop, mark, or rate-limit (by direction) the data traffic. Even if DSCP is already set, there is a value of AVC providing visibility to the traffic that it classifies. AVC integration with QoS allows you to create a policy to mark traffic using a DSCP value based on application knowledge

When traffic from the Apple Devices reach the wireless controller, the controller performs deep packet inspection to recognize the flow. If the flow is recognized as an application that is part of the AVC profile, the traffic is marked according to the AVC policy. For example, in situations where a wireless client sends application traffic, this traffic upon reaching from the AP to the WLAN Controller would get immediately recognized by the NBAR2 engine, and get correctly remarked according to the configured AVC profile.

## AVC Configuration Example for Apple Devices with Cisco Jabber

Cisco Jabber is available on all apple devices as a collaboration application. It offers several types of services: File transfer, application sharing, SIP signaling, real time audio, and real time video communications. Cisco recommends DSCP 46 for real time voice, DSCP 34 for video, and 24 for signaling.

This section focuses on configuring AVC for Jabber traffic as an example. This configuration section is targeted only towards the Jabber traffic for the WLAN profile to be used for Apple devices. The rest of the traffic could of course be allowed on the WLAN (and prioritized similarly), but assuming the marking for rest of the traffic is untouched and do not exceed the QoS profile maximum.

To configure Application Visibility and Control for Cisco Jabber traffic, perform the following steps:

**Figure 14: Creating an AVC profile for Jabber application**

The screenshot shows the Cisco Wireless configuration interface. The left sidebar has a tree view with 'All APs', 'Radios', '802.11a/n/ac', '802.11b/g/n', 'Dual-Band Radios', and 'Global Configuration'. The 'Advanced' option is selected. The main content area is titled 'AVC Profile Name' and contains a text input field with the value 'Jabber' and a dropdown arrow.

Navigate to **Wireless > Application Visibility And Control > AVC Profiles** and click on New

**Figure 15: Adding rules to mark the application traffic types to the AVC Profile**

The screenshot shows the 'AVC Profile > Rule Edit > 'Jabber'' configuration page. The left sidebar is the same as in Figure 14. The main content area has a form with the following fields: 'Application Name' (cisco-jabber-audio), 'Application Group Name' (voice-and-video), 'Action' (Mark), 'Dscp (0 to 63)' (Platinum(voice)), and 'Direction' (Bidirectional). A green box highlights the 'Action', 'Dscp', and 'Direction' fields.

Navigate to **Wireless > Application Visibility And Control > AVC Profiles** and click on the profile to add a rule for the application to be marked

**Figure 16: Verifying all the rules for the application traffic type associated to the AVC Profile**

The screenshot shows the 'AVC Profile > Edit > 'Jabber'' configuration page. The left sidebar is the same as in Figure 14. The main content area displays a table of rules. A green box highlights the 'Application Name', 'Application Group Name', 'Action', 'DSCP', and 'Direction' columns.

Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps
cisco-jabber-audio	voice-and-video	mark	46	Bidirectional	NA
cisco-jabber-video	voice-and-video	mark	34	Bidirectional	NA
cisco-jabber-control	voice-and-video	mark	24	Bidirectional	NA

Make sure you have the right DSCP markings associated to the application traffic types. AVC will prioritize the traffic according to the action, DSCP value and direction of the traffic flow.

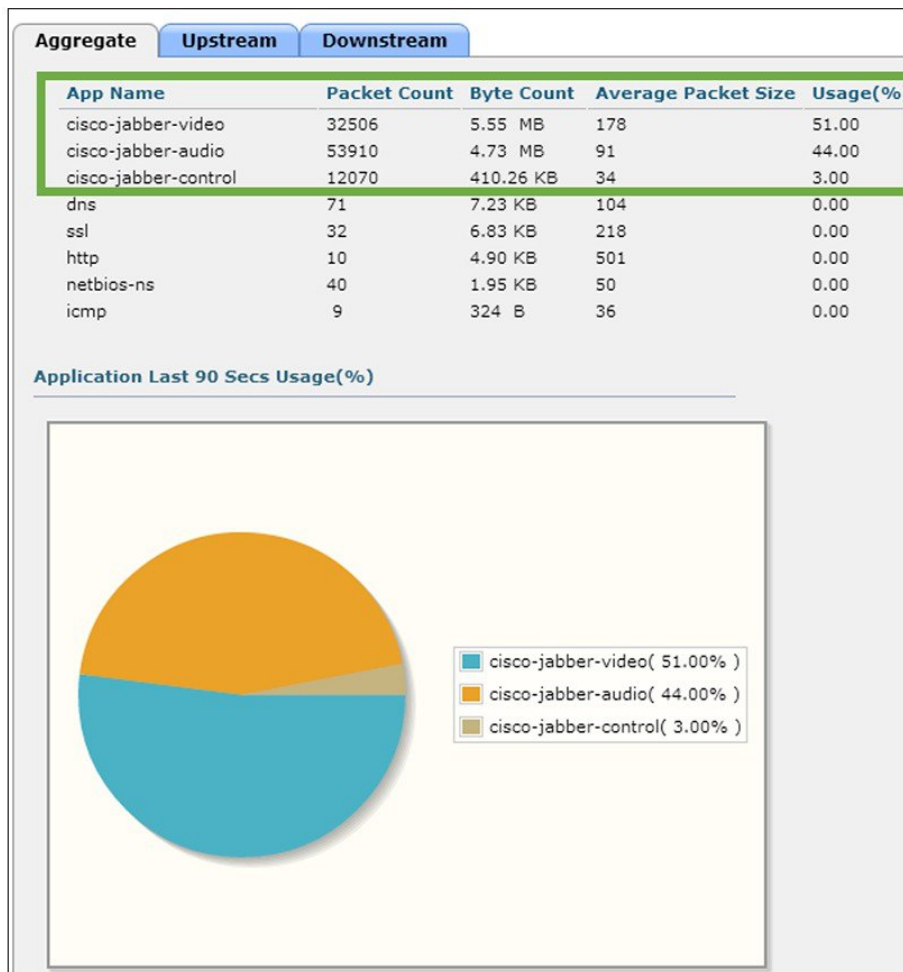
**Figure 17: Enabling AVC on the WLAN, and applying the AVC Profile**



Navigate to **WLANs > QoS** tab for the WLAN SSID. Check to enable Application Visibility and select the created AVC profile to assign it to this WLAN.

Now with AVC enabled and the Jabber AVC profile set, the Cisco controller has complete visibility and traffic control for all Jabber traffic in this WLAN. To test your configuration, associate your Apple devices to the WLAN, and initiate Jabber voice and video calls on the network.

**Figure 18: Verifying application traffic being correctly recognized by AVC**



Verifying application traffic being correctly recognized by AVC.

Other applications can also be included in the same Jabber profile and then have their QoS priorities managed in a similar fashion in order to control the priority of multiple applications over the same WLAN. In a very high density environment enabling AVC for multiple applications on single WLAN may have a performance impact.

## Roaming Enhancements for Apple Devices

Roaming is an integral part of an enterprise wireless network. Smartphones and tablets are bound to roam from one AP to another to remain connected to the Wi-Fi at all times as the user moves. Enterprise roaming enhancements mainly imply enabling of IEEE standards based 802.11r, 802.11k, and 802.11v optimizations on both the wireless infrastructure as well as the client devices.



**Table 3: Support for Roaming Enhancement Standards on Cisco and Apple**

Roaming Enhancement Standard	Cisco Implementation	Apple Implementation
802.11r – Fast Transition (FT)	<a href="#">AireOS v7.2</a>	iOS 6.0
802.11k – Neighbor Reporting	<a href="#">AireOS v7.4</a> (Suggested v8.0 MR3)	iOS 6.0 (Suggested iOS 8.0)
802.11v – BSS Transition Management	<a href="#">AireOS v8.0</a>	iOS 7.0

Additional roaming behavior tweaks were introduced in iOS 8 to further improve the roaming efficiency in enterprise environments. These optimizations allow the clients to potentially roam between APs within the same network with minimum application disruption.

Cisco and Apple recommends enabling 802.11r, 802.11k, and 802.11v on the Cisco Wireless LAN infrastructure for supporting Apple devices in order to implement an enterprise environment configured for efficient roaming. However, this recommendation should only be considered for a WLAN where all expected devices have support for at least the 802.11r roaming enhancement. Any client which does not support the roaming enhancement standards may not be able to associate to that wireless network. See [Apple's device list](#) to check whether your Apple device supports 11r, 11k, and 11v or not.

In the Wi-Fi world, the Received Signal Strength Indicator (RSSI) is a critical measurement of the RF signal. The RSSI value is typically shown as a negative dBm value (e.g. -72 dBm). The Wi-Fi signal is considered to get stronger as the RSSI value gets closer to 0. An RSSI measurement of -65 dBm is weighed stronger than a value of -73 dBm, therefore a client associated at -65 dBm has a better Wi-Fi signal strength than if it was connected at -73 dBm. However, this does not necessarily imply higher performance or higher throughput as there are a number of other factors associated to performance.

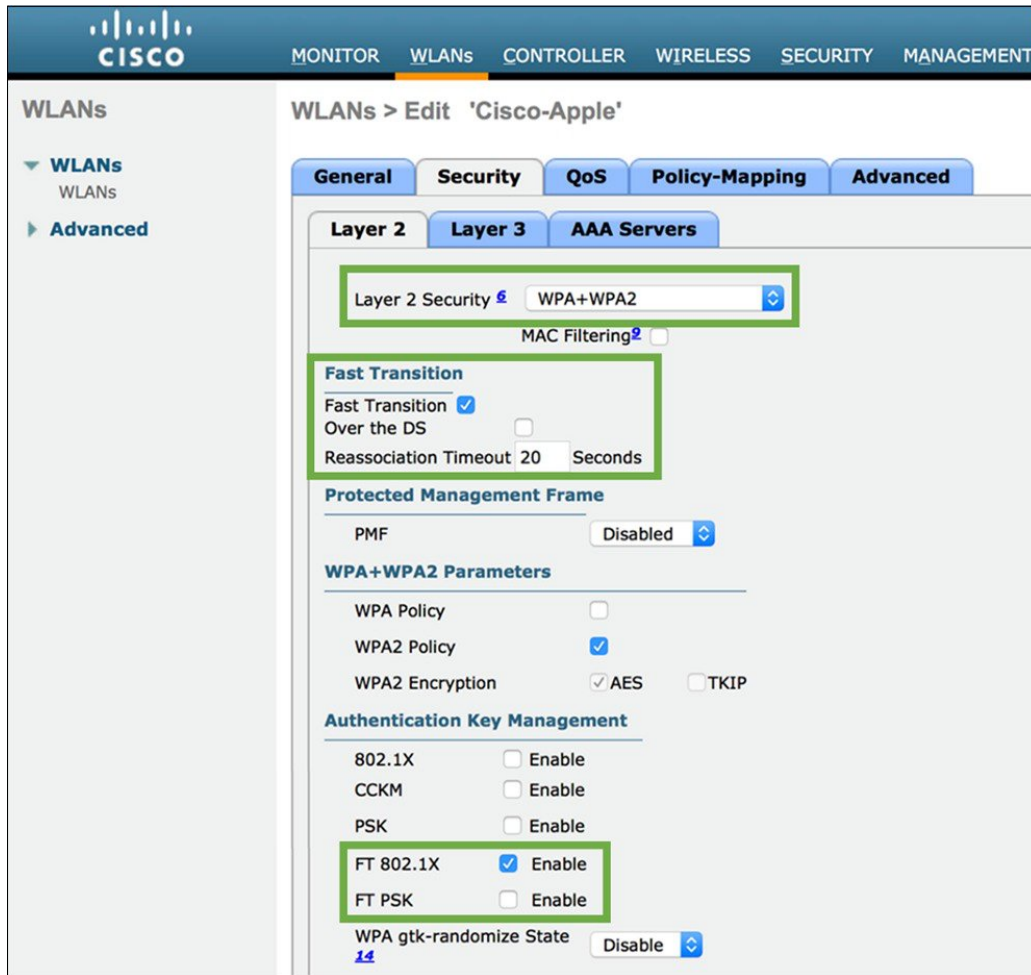
Apple devices make use of a certain RSSI thresholds to trigger the roam scanning mechanism. This trigger threshold is the minimum signal level a client requires to maintain the current connection. Apple clients monitor and maintain the current Wi-Fi connection until the RSSI crosses the -70 dBm threshold. Once crossed, iOS initiates a scan to find a suitable AP that can be roamed to. Apple details this roaming logic for iOS devices in the Wireless Roaming Reference for Enterprise document.

## 802.11r - Fast Transition (FT)

802.11r is an enhancement which allows for the Client-AP handshake with the new AP to be done even before the client roams to the new AP, which is called Fast Transition (FT). With this method, the wireless client performs just one initial authentication against the WLAN infrastructure when a connection is established to the first AP, and performs fast-secure roaming while roaming between APs of the same FT mobility domain. This eliminates much of the handshaking overhead while roaming, thus reducing the handoff times between APs while maintaining security and QoS. Since 802.11r helps reduce latency while roaming, it is useful for client devices running real-time applications such as voice and video over Wi-Fi.

## Configuring 802.11r on Cisco Controller

Figure 19: Enabling 802.11r - FT on the WLAN



Navigate to **WLANs > Security** tab of the WLAN (Layer 2 security can be WPA+WPA2 or Open) Check to enable Fast Transition. Uncheck Over the DS mode, and choose FT 802.1X or FT PSK depending on the desired security authentication for the WLAN.

802.11r reduces the number of packets exchanged between an AP and an 11r client whose credentials are already cached. With 802.11r, client device can establish security and QoS state prior to re-association in two modes:

- Over the Air – Client exchanges packets directly with the new AP
- Over the Distribution System – Client exchanges packets via the current AP

Unchecking Over-the-DS implies FT uses over-the-air mode. For a high density enterprise environment, Cisco and Apple recommend to use 802.11r with Over the air transition for optimal 11r-FT performance.

### Configuring 802.11r for Mixed Mode

When you enable Fast Transition on the WLC, you will notice a warning pop-up saying "Client that do not support 802.11r will be unable to join the network". This is true for some laptop and legacy clients that don't support 802.11r as they are unaware of how to

process the Fast Transitions Information Elements (IEs) during authentication. So there is likelihood that such devices will not be able to see or join an 802.11r enabled WLAN.

This led to the development of 'mixed-mode', which allows both non-FT and FT versions of authentication modes to be enabled on the same WLAN. This mixed mode support was officially introduced in [AireOS 8.0](#), which allows to remove the restriction of creating a separate SSID for 802.11r enabled devices.

**Figure 20: Enabling 802.11r mixed-mode to allow non-FT clients to join the same network WLAN**



Navigate to **WLANs > Security** tab of the WLAN and check both FT and non-FT authentication. Example 802.1X and FT 802.1X, or PSK and FT-PSK.

Non-802.11r clients which have the updated wireless LAN drivers for '802.11r-compatibility' can now join this 802.11r-mixed-mode WLAN. It is important to note that laptop clients with newer wireless LAN chipsets and updated chipset drivers with **11r-compatibility**, both are equally important when trying to use the 11r mixed-mode SSID configuration. For example, Apple introduced the 11r-compatibility drivers for the MacBook Laptops with their Mavericks 10.9 OS, which allowed the MacBook to correctly identify and associate to a mixed mode SSID (e.g. FT-PSK + PSK). Any MacBook laptop running an older OS (even with the same chipset) might be able to see the 11r mixed mode SSID, but may fail to associate to it.

**Note**

Cisco and Apple recommend performing lab test for 11r-mixed-mode WLAN before enabling it on the network. You can avoid unexpected behavior by using a newly created WLAN with mixed-mode enabled. If you try to edit a previously known WLAN from regular mode or FT only mode to a mixed mode, you may see an unexpected result where the '11r compatible' clients (e.g. Apple MacBook) are still not able to associate, as they might be using the cached information from its previous association. If you do choose to edit a known Wi-Fi network's configuration from regular mode to mixed mode, then the workaround is to make the 11r compatible clients "forget" that wireless network, and then try re-joining.

It is recommended to check multiple vendor devices to ensure the 11r compatibility driver is present before using the mixed mode SSID. If you cannot predict what clients will try to join your 802.11r enabled WLAN, then creating a separate SSID for non-802.11r clients is advisable. Please note that 11r -compatibility does not mean that those devices are 802.11r enabled, it simply means they have the ability to correctly identify and associate to a mixed mode SSID.

## 802.11k - Radio Measurement & Neighbor Reporting

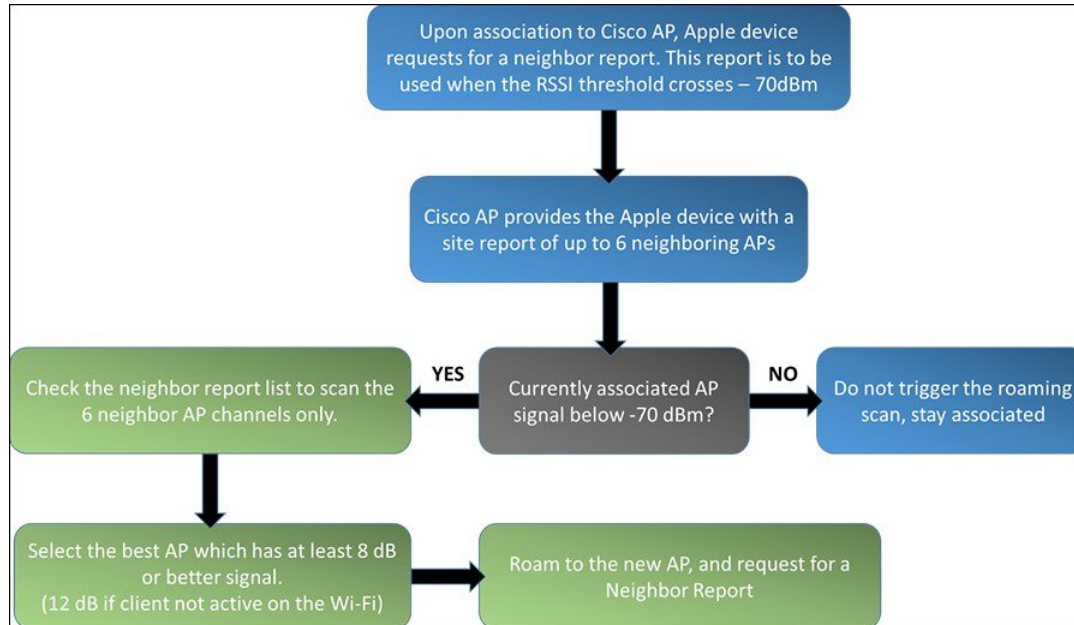
The 802.11k standard allows clients to request reports containing information about known neighbor APs that are candidates for roaming. The request is in the form of an 802.11 management frame known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with their Wi-Fi channel numbers. The AP response is also an action frame. With the 802.11k response frame coming from the AP, the client becomes aware of the best channel candidates that should be scanned before the next roam. Having this handy neighbor list allows the client to strategically probe these reported channels first when approaching the next roaming opportunity, thus reducing its scanning time and expeditiously decide which AP should it roam to.

Although 802.11k support was officially introduced by Cisco in AireOS 7.4 and Apple in iOS 6.0, there were design changes that were implemented by Apple in iOS 8.0 in order to improve the neighbor list request process. These changes were integrated by Cisco in AireOS v8.0 MR3 and v8.1 MR1 releases. For 802.11k, Cisco and Apple recommend using AireOS v8.0 MR3 or above controller code, and iOS 8.0 or above updates for the Apple devices.

On Cisco infrastructure, 802.11k algorithm uses RRM to determine neighbors to the AP to which client is associated, check which APs heard the client, and the AP then returns list of best 6 APs to the client. With the neighbor list information, the 11k capable client does not need to scan all channels to find which AP it can roam to. Not having to scan all the channels also reduces channel utilization, thereby potentially saving air-time on the channels. Additionally, the battery life of the Apple devices is also benefited since the devices are not frequently changing the radio configuration for scanning each channel, or sending probe requests on each channel.

This prevents the device from having to process all of the probe response frames. This also reduces interruption of connectivity due to off channel passive scanning through listening for beacons.

**Figure 21: Neighbor Report processing flow for Apple devices supporting 802.11k (iOS 8.0 and above)**



**Note** : Refer to Apple iPhone roaming behavior and optimization guide for more details: [http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/iPhone\\_roam/b\\_iPhone-roaming.html](http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/iPhone_roam/b_iPhone-roaming.html)

Using 802.11k to discover and zero in on the new AP to roam to is only part of the process - post this, Apple device also needs to swiftly complete the authentication process, so the users experience minimal disruption in service. This process involves the Apple devices authenticating with the new AP and de-authenticating from the current AP. Enabling 802.11r and 802.11k on the WLAN together is a good way to quicken the roaming process. Implementing 11r and 11k together would allow the Apple devices to not only reduce the scan times, but also pre-authenticate against the potential access points, thus reducing the authentication time and briskly complete the roam to the new AP.

## Configuring 802.11k on Cisco Controller

Figure 22: Enabling Neighbor Report on the WLAN

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, and MANAGE. The left sidebar shows a tree view with 'WLANs' expanded, showing 'WLANs' and 'Advanced' sub-items. The main content area is titled 'WLANs > Edit 'Cisco-Apple''. It features several tabs: General, Security, QoS, Policy-Mapping, and Advanced. The 'Advanced' tab is selected. Under the 'Advanced' tab, there are sections for 'Lync' and '11k'. The '11k' section contains three items: 'Assisted Roaming Prediction Optimization' (unchecked), 'Neighbor List' (checked and highlighted with a green box), and 'Neighbor List Dual Band' (unchecked). The 'Neighbor List' checkbox is checked, indicating that 802.11k neighbor reporting is enabled.

Navigate to **WLANs > Advanced** tab of the WLAN and scroll down to the 11k section. Check the Neighbor List box to enable 802.11k neighbor reporting. Since this is a 5GHz only WLAN, dual band neighbor list is not necessary. Assisted roaming prediction optimization does not apply to Apple devices as they offer 802.11k support.

## 802.11v – Basic Service Set (BSS) Transition Management

802.11v Basic Service Set (BSS) Transition Management is part of the Wireless Network Management (WNM) feature which acts as a platform for the clients and the infrastructure to potentially exchange operational information so that both sides have additional awareness of the WLAN conditions.

802.11v offers a network assisted roaming enhancement for the client devices, where the AP will try to assist in the roaming decision making by providing an unsolicited recommendation in the form of a request to the client. This request will contain the suggestion for the best available AP that the client could potentially roam to. Client devices and infrastructure may both use WNM to exchange operational information to gain additional awareness of the WLAN conditions. Although the client always has the freedom to choose whether to accept or reject the advice offered by the AP, the additional awareness can assist to build a firm foundation for self-correcting events and actions to be implemented. 802.11v BSS Transition Management functions with three set of frames:

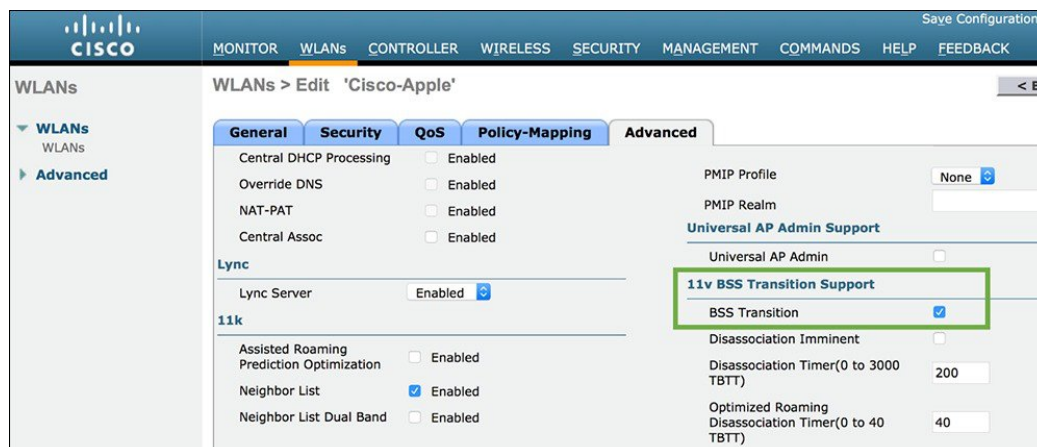
- BSS Transition Management Query – Transmitted from a client to the AP
- BSS Transition Management Request – Transmitted from AP to the client
- BSS Transition Management Response – Transmitted from a client to the AP but is only done so following a BSS Transition Management Request

Apple devices supporting 802.11v can respond to the BSS transition management query from the AP and utilize the provided list of preferred APs to make roaming decisions. Note that this preferred list of APs could be different than the neighbor AP list acquired with the 802.11k exchange. Unlike 802.11k where the Apple device will request for a neighbor list only upon association or re-association, the BSS transition management query can be sent out at any time. First, in a solicited way by the client asking for a



recommendation for a good AP to roam to (via BSS Transition Management Query), or the AP can respond or offer an unsolicited request to the client asking to roam to a particular AP if the client is experiencing bad connectivity (via BSS Transition Management Request). The trigger of the BSS Transition Management Request from Cisco AP can also occur for other reasons including a load balancing event. Accepting/rejecting this request is the primary function of the BSS Transition Management Response. The client can also include a reason code for acceptance or rejection. It is important to note that the response to the request is optional.

**Figure 23: Enabling 802.11v BSS Transition Management on Cisco Controller**



Navigate to **WLANs > Advanced** Tab of the WLAN and scroll down to the 11v section. Check BSS Transition to enable 11v BSS Transition Management support on the Cisco APs.

The Disassociation Imminent is an optional add-on for the BSS Transition support feature. It is used to inform the client that it will be disconnected from the AP after the time indicated in the Disassociation Timer field. The Disassociation Timer is expressed in number of beacon intervals. Once the Disassociation Timer reaches zero, then the AP can forcefully disassociate the client any time thereafter.

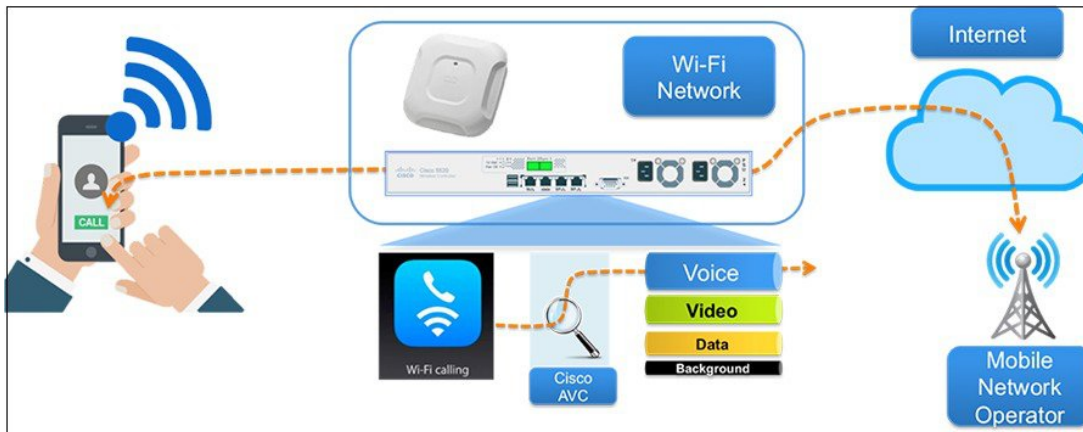
## Wi-Fi Calling with Apple Devices on Cisco WLAN

Apple introduced Wi-Fi Calling across multiple iPhone models (iPhone 5c and above) in September 2014 with its iOS 8.0 update, and has since been adding major network carriers who offer Wi-Fi calling service. With the [iOS 9.0 update](#), more network carriers have been added to the list on which Apple iPhones support Wi-Fi calling. With extended Wi-Fi calling services where you can add an iPad or Macbook via the iPhone, and make Wi-Fi calls directly from the added device, it has become important to ensure an optimized wireless network for Wi-Fi calling in an enterprise.



When Wi-Fi Calling is enabled, the iPhone device establishes an IPsec connection with the carrier network server. This initial connection traffic goes out in Best Effort mode. Following this, all the voice traffic from the iPhone is sent within an Encapsulated Security Payload (ESP) in Voice priority (UP6).

**Figure 24: Optimizing Wi-Fi Calling over Cisco WLAN with Cisco AVC**



The downlink traffic to the iPhone comes on a best effort priority with default controller settings. Using a Platinum QoS, and AVC for the WLAN, you can effectively classify and prioritize all Wi-Fi calling voice traffic. Wi-Fi calling is one of the new applications that will be classified in AVC Protocol Pack 15.

There are several key design considerations to keep in mind when designing Cisco wireless network for optimized Wi-Fi Calling support:

- Optimal RF conditions: AP Cell Size, Data Rates, Deployment density, and Roaming enhancements (802.11r/k/v)
- WLAN Configuration: Set WMM on your WLAN, QoS to Platinum, and AVC for classification



**Note** Refer to Cisco VoWi-Fi Network Design document for more details: <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/service-provider-wi-fi/white-paper-c11-733914.html>

## Apple Bonjour on Cisco WLAN

Bonjour is an Apple service discovery protocol, which locates devices such as printers, other computers, and the services that those devices offer on a local network using multicast Domain Name System (mDNS) service records.

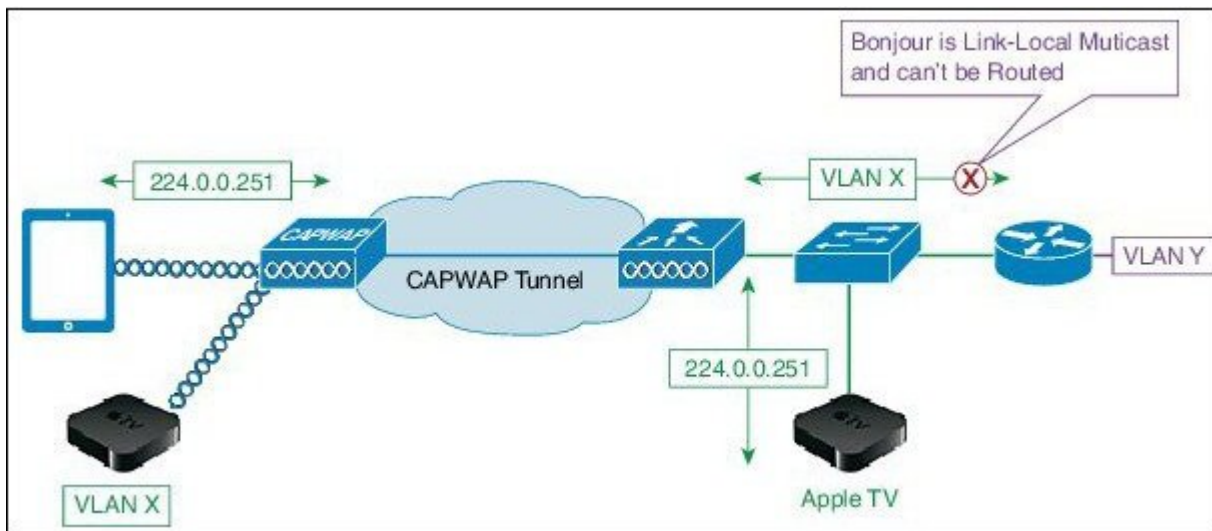
The Bonjour protocol operates on service announcements and service queries which allow devices to ask and advertise specific applications, such as:

- Printing services
- File sharing services
- Remote desktop services
- iTunes file sharing
- iTunes Wireless iDevice Syncing (in Apple iOS v5.0+)

- AirPlay, which offers these streaming services:
  - Music broadcasting in iOS v4.2+
  - Video broadcasting in iOS v4.3+
  - Full screen mirroring in iOS v5.0+ (iPad2, iPhone4S or later)

Each query or advertisement is sent to the Bonjour multicast address for delivery to all clients on the subnet. Apple's Bonjour protocol relies on Multicast DNS (mDNS) operating at UDP port 5353 and sends to the reserved group addresses.

**Figure 25: Apple Bonjour services for Apple TV on Cisco WLAN**



**Note** Refer to Cisco v8.0 Bonjour Deployment Guide document for more details: <http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/WLAN-Bonjour-DG.html>

## Knowing your Wireless Environment

In addition to designing your Cisco WLAN around the best practices for the Apple devices, network maintenance and monitoring helps to keep track of the overall network health. The application and roaming performance for the Apple devices are largely dependent

on AP coverage and Wi-Fi channel bandwidth. Cisco's controller user interface provides relevant data to granularly track important statistics for the APs and the RF environment.

**Figure 26: Checking AP Statistics to monitor the RF environment**

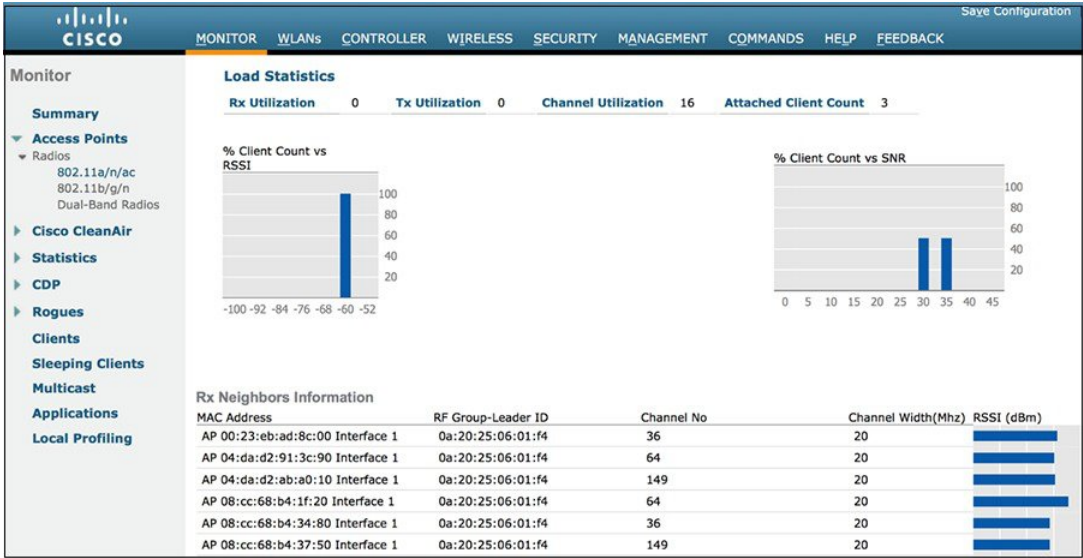


Navigate to **Monitor > Access Points > Radios > 802.11a/n/ac** and click on the radio button on the right side, and select details to access stats like noise profile, interference and coverage.

The data includes the Wi-Fi channel number, interference on that channel (red), current channel load statistics (blue), number of Voice over IP (VoIP) calls, and other client related information like 'Client Count vs RSSI' and 'Client Count vs SNR'. Using this

information, users can get insight to the data rate capabilities of the Apple devices, and what data rates might be in actual use because of RSSI and SNR for the associated clients.

Figure 27: Monitoring for Client count against RSSI/SNR, and AP neighbors RSSI



The information about the clients is the 'Rx Neighbors 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 Apple devices are associated.

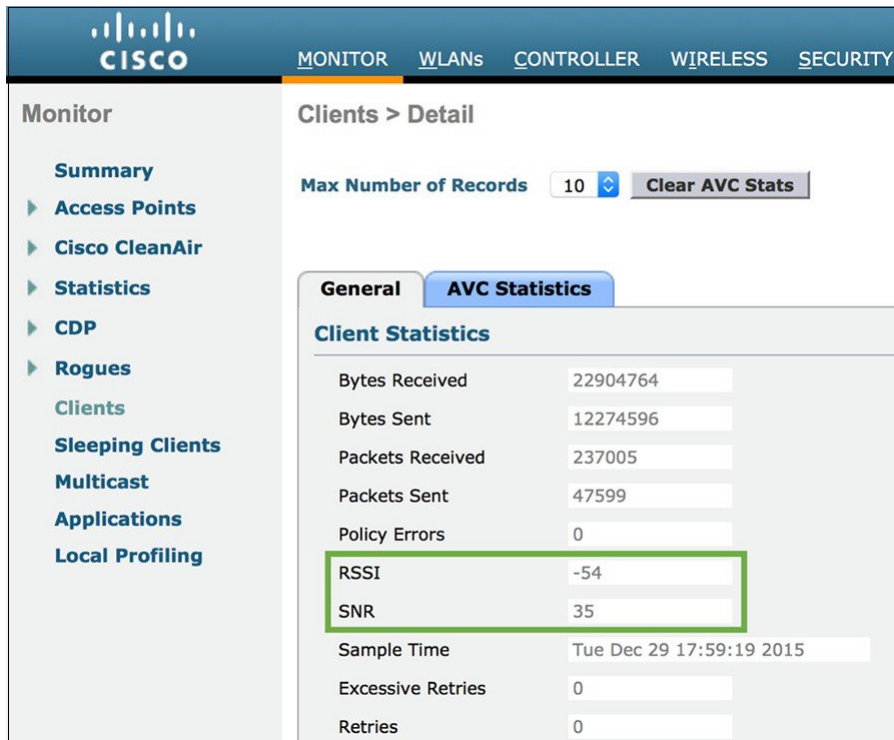
### Associated Device Monitoring

The next aspect of knowing the Wi-Fi environment is the connection status for the Apple devices. Cisco controller user interface provides a window of information for each individual device. This information is in a database that is accessed by the Wi-Fi MAC address of the devices. To [determine the MAC address for an Apple device](#), tap on Settings on the Apple device and navigate to **General > About > Wi-Fi Address**.

Individual client info page shows 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 Apple device. The information includes client and AP properties. Client properties include the IPv4 and IPv6 addresses, VLAN ID, current data rate set, security information, and QoS properties.

Other important Wi-Fi statistics can be gathered from the client page. The RSSI field reports the signal strength of the packets received at the AP indicates how well the client packets are being seen at the AP.

**Figure 28: Monitoring Client RSSI and SNR statistics**



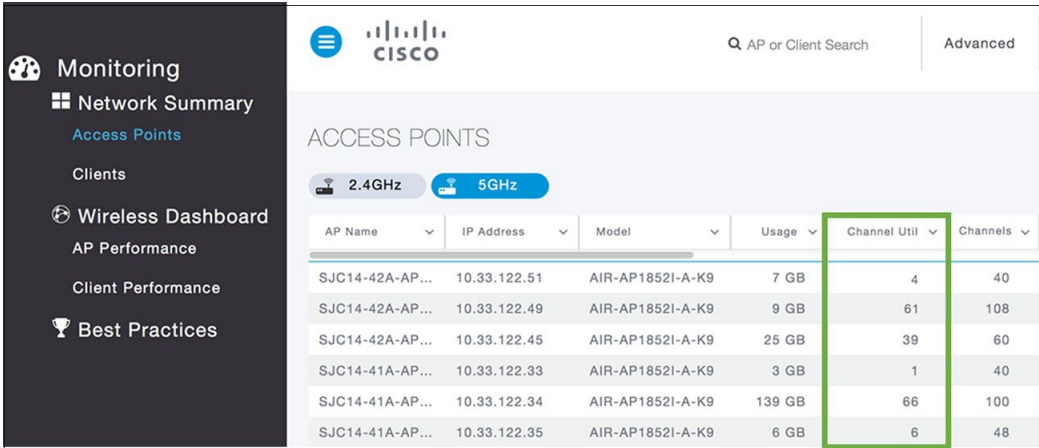
For example, an RSSI value of -45 dBm shows the AP can see the client at a stronger signal than a value of -67 dBm. The RSSI value is also important for knowing the coverage quality. If the value is too low, it could be an indication for poor connectivity. It is also an indicator of whether there is a need for more APs or a need for a better AP.

## Channel Utilization

To compensate for the signal strength drop, as the phone moves away from an AP, the data rates shift down to a lower value. This helps to provide a more reliable packet delivery but reduces the throughput of the device and increases the air-time used by the device. More air-time consumed reduces the overall available bandwidth in the Wi-Fi cell for other devices. Available channel bandwidth

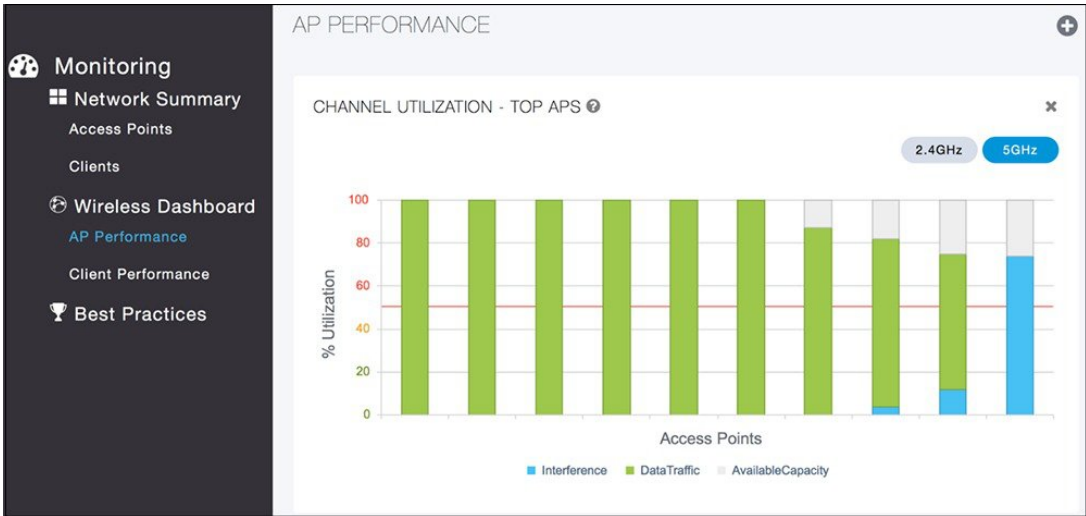
can be determined by monitoring the channel utilization. RSSI and channel utilization are two of the principle factors in assessing the overall connectivity for the Apple devices. The Wi-Fi channel is shared by the devices and the AP by way of their association.

Figure 29: Accessing Channel Utilization for all APs using monitor dashboard with AireOS v8.1 and above



Channel utilization is one of the channel load statistics shown on the AP's radio statistics page.

Figure 30: Accessing Channel Utilization to identify the APs with the highest channel utilization



In AireOS 8.1 or above, navigate to **Monitoring > Wireless Dashboard > AP Performance** to access the channel utilization graphs. The Wi-Fi channel is also shared by other APs (both your own and others operating on the same channel), and other devices, including 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 to the degree that an AP on the same channel can hear them. Non-Wi-Fi interferers are contributors to the channel utilization. Non-Wi-Fi interferers include Bluetooth devices, microwave ovens, DECT like phones, surveillance video cameras or any other device using the same radio frequency as the Wi-Fi channel but not using the 802.11 protocols. Rogue Wi-Fi devices including personal hotspots and non-Wi-Fi interferers should be managed as best as possible to guard the channel utilization.



## Peer-to-Peer Activity Monitoring

Besides RF channel layout, planning and associated enterprise wireless network design, another factor to consider is the role and potential impact of newer Apple devices and their peer-to-peer behavior in your enterprise network. As of the 3rd generation of Apple TVs running Apple TV software version 7.0 or later, a new peer-to-peer methodology for AirPlay is introduced. Whereby [compatible iOS and OS X](#) devices can establish direct wireless communication with an Apple TV using Airplay. This peer-to-peer AirPlay feature is enabled by default on compatible devices, and is the preferred data path for Apple devices regardless of the availability of an established network connection.

This peer-to-peer capability between compatible Apple TV and other Apple endpoints is possible even if the respective devices are on different wireless networks, or if there is no network connectivity whatsoever. This is accomplished using a variety of methods, such as Bluetooth Low Energy (BTLE) for initial discovery of an available Apple TV, and thereafter a direct communication path using an 802.11 channel is established between the two peer devices (i.e. AirPlay sender to AirPlay receiver). As such, this can also affect either channels 149+1, or 153-1 (Ch. 44 outside US) accordingly when a peer-to-peer AirPlay connection involving a compatible Apple TV is in use. If peer-to-peer AirPlay is not supported on either the AirPlay sender or receiver, then the established network infrastructure connection is used instead for AirPlay communication.

A compatible iOS or Macbook (OS X) device has discovered a 3rd generation or later Apple TV using its Bluetooth adapter, and all involved endpoints support peer-to-peer AirPlay functionality. The next phase of the associated discovery process will lead to the compatible Apple end device and the Apple TV to directly communicate in a peer-to-peer fashion using 802.11 channel 149+1 in the 5 GHz band.

Following the discovery phase being completed, the end user can select the applicable Apple TV to start AirPlay communication. This causes the 802.11 radios to timeshare or balance between channel 149+1 for AirPlay, and the infrastructure wireless channel used for the active connection to the wireless network infrastructure. If possible, the AirPlay sender (i.e. iOS or OS X device) will roam to the same infrastructure channel currently used by the Apple TV in question. If neither device is currently connected to the wireless network, the devices will use channel 149+1 for AirPlay functionality. Wireless peer-to-peer AirPlay communications adhere to 802.11 standards.

Airdrop is an Apple feature which is used to share content between iOS and MacBook devices using Bluetooth and Wi-Fi simultaneously. Similar to Airplay, Airdrop also uses 802.11 channel 149+1 or 153-1 in the 5 GHz band to transfer the content between the devices. During Airdrop activity, the devices time slice the Wi-Fi connectivity and content sharing by jumping back and forth between the Wi-Fi connectivity with the associated AP, and the peer-to-peer connectivity to complete the transfer of the content.

Cisco recommends monitoring the UNII-3 Band for high channel utilization with regards to peer-to-peer activity against regular Wi-Fi activity. If a lot of Apple devices are expected to use continuous peer-to-peer connections on a daily basis, a last resort potential solution could be removal of the channels 149, 153 from the DCA list to avoid congestion. Cisco strongly recommends channel exclusion with the use of [RF profiles](#) to effectively apply the removal of the channels to only the affected APs, and not globally across all APs.



**Note** Refer to guidelines in Enterprise Mobility Design Guide for more details on how to configure DCA:[http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise\\_Mobility\\_8-1\\_Deployment\\_Guide.pdf](http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide.pdf)

Apple Watch is another portable device which uses peer-to-peer communication to function. It supports both Bluetooth and Wi-Fi connections for communicating with the paired iOS device. Although there are two modes of communication, the Apple watch's primary mode of connectivity is Bluetooth to transfer data back and forth between watch and iPhone. If the Bluetooth is off, the watch switches to Wi-Fi to stay connected to the paired iPhone. Currently the Apple watch only supports 802.11b/g/n in the 2.4 GHz band, with Open or Pre-Shared-Key security authentication.

With the latest WatchOS2 update, Apple Watch can also use Tetherless Wi-Fi to connect to the Internet independently. It means that even without the iPhone, the watch will be able to connect to the Wi-Fi network. Since Apple watches are 2.4 GHz only, there should not be any impact on the 5 GHz networks even if multiple Apple Watches are simultaneously communicating with the Wi-Fi network.



# Apple Devices on Cisco WLAN Best Practices Summary

Recommendations for Apple Devices on Cisco WLAN are summarized as follows:

- Cisco recommends a 5 GHz only network and coverage design for all apple devices. The 5 GHz band is typically less affected by non-802.11 sources of interferences than the 2.4 GHz band
- Cisco recommends closely monitoring the channel utilization provided through the WLC dashboard. 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 take action to resolve identified 5 GHz Wi-Fi channels that are most affected by known sources of interference on a regular basis.
- Cisco recommends all Apple devices to be connected to a WLAN with a QoS value of platinum (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
- Cisco and Apple recommend that you configure an 802.11r mix mode WLAN for fast transition 802.1X or WPA2 PSK capable clients and 802.11r-compatible clients to join the same network
- For high density enterprise environments, Cisco and Apple recommend to use 802.11r with Over the air transition for optimal 11r-FT performance.
- Cisco recommends configuring 802.11k on the WLAN to provide Apple devices with a neighbor list response. Cisco v8.0MR3 and v8.1.120.0 and Apple iOS 8.0 is the minimum version recommended for 802.11k
- Cisco and Apple recommend the use of 802.11v BSS Transition Management to help balance client load across access points
- 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 number of APs in environment) is needed, and consider 40 MHz when client traffic uses heavy bandwidth (e.g., video) and DFS Channels are available
- Cisco recommends using DSCP 46 for voice traffic based applications, translates to 802.11e – UP 6
- Cisco and Apple recommends a minimum data rate of 12Mbps and 24 Mbps as the mandatory rate as a general best practice for Apple devices on Cisco Wireless LAN. If the 5GHz coverage is marginal, set 6Mbps as the lowest mandatory rate, and make sure that 12 and 24Mbps are enabled as well
- Cisco highly recommends leaving all MCS rates enabled
- Cisco recommends that at all times an Apple client device observes a minimum of 2 APs with an RSSI measurement of -67 dBm
- Cisco recommends monitoring for peer-to-peer communication activity on UNII-3 band channels in a high client density environment. If high number of Apple devices are expected to perform peer-to-peer activity, excluding channels 149, 153 from DCA can be considered as a last resort measure
- Apple recommends upgrading all devices to the latest iOS 9 or above operating system
- RF design and monitoring recommendation summary:
  - Over all Channel Utilization should be less than 40%.
  - A minimum Signal to Noise Ratio (SNR) of 25 dB.
  - 802.11 retransmissions should be kept under 15%.
  - Packet Loss should remain under 1 percent and jitter should be kept to less than 100 ms.

The best practices for WLANs also includes deploying highly-available WLCs, in conjunction with high-density of access points to promote always-available WLAN infrastructure. In addition, Cisco's HDX suite of technologies such as Cisco CleanAir, ClientLink, Optimized Roaming, and Radio Resource Management automatically allows to optimize your network performance while simultaneously reducing coverage holes and bypassing interference.

## Additional Information

### **Cisco Wireless LAN Controller Deployment Guide v8.1**

[http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise\\_Mobility\\_8-1\\_Deployment\\_Guide.pdf](http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide.pdf)

### **Cisco Wireless LAN Controller Configuration Best Practices**

<http://www.cisco.com/c/en/us/td/docs/wireless/technology/wlc/8-1/82463-wlc-config-best-practice.html>

### **Detailed overview on how 802.11r works on Cisco WLAN**

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html#anc24>

### **Cisco Device Classification Guide**

[http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/device\\_classification\\_guide.html](http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/device_classification_guide.html)

### **Cisco Application Visibility and Control (AVC) Q & A**

[http://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/qa\\_c67-722538.html](http://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/qa_c67-722538.html)

### **Configuring Application Visibility and Control (WLC 7.6 or later)**

<http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/115756-avc-guide-00.html>

### **Wi-Fi network roaming with 802.11k, 802.11r, and 802.11v on iOS**

<https://support.apple.com/en-us/HT203068>

### **iOS 9.0 Deployment Reference Guide**

<https://help.apple.com/deployment/ios/>

### **Apple Voice Over IP (VoIP) Best Practices Guide**

<https://developer.apple.com/library/ios/documentation/Performance/Conceptual/EnergyGuide-iOS/OptimizeVoIP.html>

### **IEEE 802.11r/k/v standards**

<http://ieeexplore.ieee.org/servlet/opac?punumber=4544752>

<http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=4573290>

<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5716530>



**Americas Headquarters**

Cisco Systems, Inc.  
San Jose, CA 95134-1706  
USA

**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](http://www.cisco.com/go/offices).