

Enterprise Best Practices for iOS devices and Mac computers on Cisco Wireless LAN



Updated: January 2018

Contents

SCOPE	4
BACKGROUND.....	4
WIRELESS LAN CONSIDERATIONS	5
RF Design Guidelines for iOS devices and Mac computers on Cisco WLAN.....	5
RF Design Recommendations for iOS devices and Mac computers on Cisco WLAN	6
Wi-Fi Channel Coverage.....	7
ClientLink Beamforming.....	10
Wi-Fi Channel Bandwidth	10
Data Rates	12
802.1X/EAP Authentication.....	14
QUALITY OF SERVICE	15
Wireless Quality of Service	16
Wi-Fi Multimedia.....	19
WLAN Quality of Service Profiles.....	20
Cisco Fast lane Configurations	22
Optimized Enhanced Distribution Channel Access	26
Wired Switch Port Configurations	26
APP VISIBILITY AND CONTROL	27
AVC Configuration Example for iOS devices or Mac computers with Cisco Jabber	28
CISCO WI-FI OPTIMIZATION FOR IOS DEVICES.....	32
802.11r - Fast Transition.....	33
Adaptive 802.11r	35

802.11k - Radio Measurement & Neighbor Reporting	37
802.11v – Basic Service Set (BSS) Transition Management	38
Cisco Wi-Fi Analytics for iOS	40
WI-FI CALLING WITH IOS DEVICES ON CISCO WLAN	41
BONJOUR ON CISCO WLAN	42
KNOWING YOUR WIRELESS ENVIRONMENT	43
ASSOCIATED DEVICE MONITORING	44
CHANNEL UTILIZATION	45
PEER-TO-PEER ACTIVITY MONITORING	47
IOS DEVICES AND MAC COMPUTERS ON CISCO WLAN BEST PRACTICES SUMMARY	48
ADDITIONAL INFORMATION	50

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 iOS 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 iOS devices running iOS 9 or later and Mac computers running macOS High Sierra 10.13 or later. Some sections in the document are relevant to iOS devices running iOS 10 or above, or iOS 11 or above. These sections will clearly be marked to indicate Cisco AireOS 8.3 (or later) and iOS 10 (or later), and Cisco AireOS 8.5 (or later) and iOS 11 (or later) as the recommended software code version to be compatible.

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 as best suiting the needs for business and/or mission critical enterprise apps. Cisco and Apple strongly recommends a 5 GHz-only (802.11a/n/ac) wireless network for iOS devices and Mac computers. This document focuses completely on a 5 GHz network layout as a best practice for all iOS devices and Mac computers.

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 apps being used by employees on personal devices, there is a high demand for a pervasive wireless connectivity in parallel to responsive app performance.

Apple devices constitute a significant presence in today's Enterprise environments. In order to ensure the best possible service for iOS devices, a number of different factors have to be considered including RF conditions, client connectivity, network visibility, quality of service, and network monitoring. Coexistence also has to be ensured with larger mobile devices, such as the MacBook. These laptops also require optimized service. 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 apps, 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 for my Cisco wireless environment?

Apple continually adds support for industry-standard technologies that enhance the connectivity as a Wi-Fi client; however, some of these enhancements are only supported on specific iOS devices and Mac computers and operating system releases. Some other enhancements are solely targeted for iOS devices, which are expected to be more mobile and more susceptible to sudden RF changes than Macs running macOS. It is important to learn which iOS devices (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 features like 802.11r and 802.11k were introduced starting with iOS 6 update, Apple recommends upgrading all iOS devices to the latest version of iOS. Similarly, Apple recommend updating all Mac computers to the latest version of macOS.

Note: Refer to Device Classification Chart for details on 802.11 & Enterprise Features for iOS devices: http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/device_classification_guide.pdf.

RF Design Guidelines for iOS devices and Mac computers 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. In most cases, designing the network for expected client devices that are most sensitive to changes in RF conditions is a sound principle. Smartphones, because of their small form factor, and because they are moved in multiple directions and held close to the human body (a source of RF absorption) are usually more susceptible to sudden RF changes than larger computers. 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 iOS devices and Mac computers on Cisco WLAN

- The use of 802.11a/n/ac 5GHz based design for all iOS devices and Mac computers
- Optimal Cell edge recommendation for iOS devices is -67 dBm or better (-65 dBm is better for typical high density enterprise deployments). Mac computers can accept a cell edge at -72 dBm. An optimal WLAN deployment will require, at the cell edge, a minimum of 2 APs in 5 GHz at -67 dBm **as measured by the iOS client.**
- Average Channel Utilization should be less than 40%
- Maintain 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

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.
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.

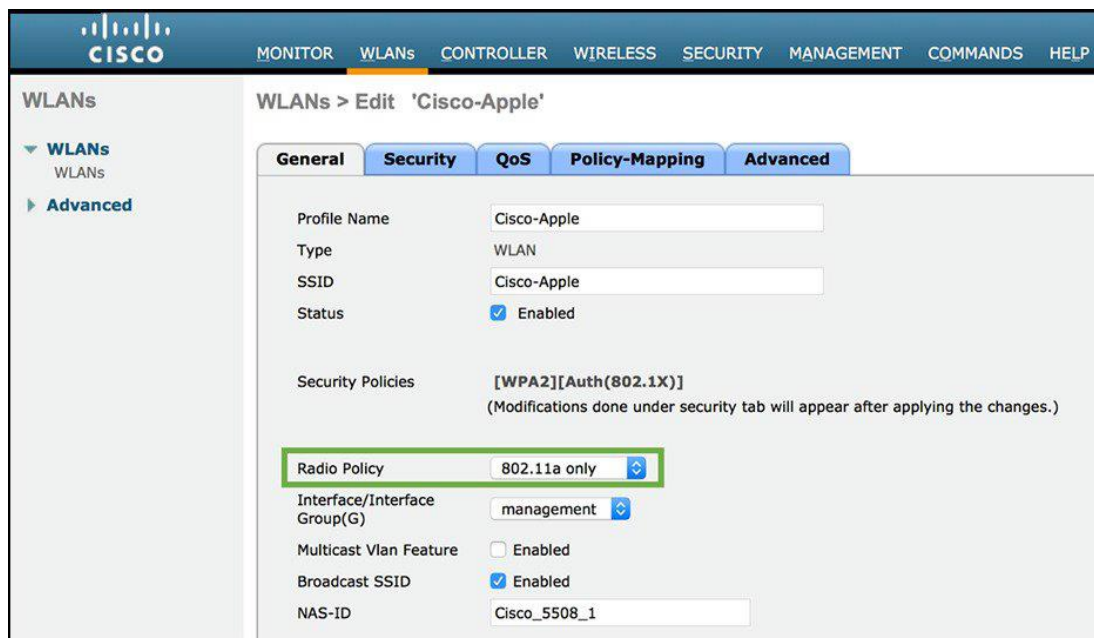
Note: Refer to Site Survey RF Design Validation Guide for more details:

<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 iOS devices and Mac computers on a Cisco wireless network. For environments where 2.4 GHz-only devices are present, a separate wireless network could be potentially added to allow the 2.4 GHz devices to connect to the network.

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

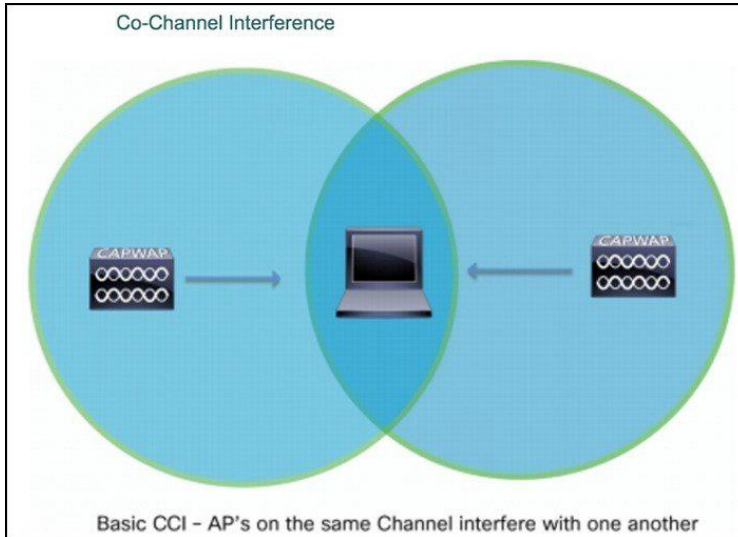


The screenshot displays the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The main content area is titled 'WLANs > Edit 'Cisco-Apple''. The 'Advanced' tab is selected, showing the following 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

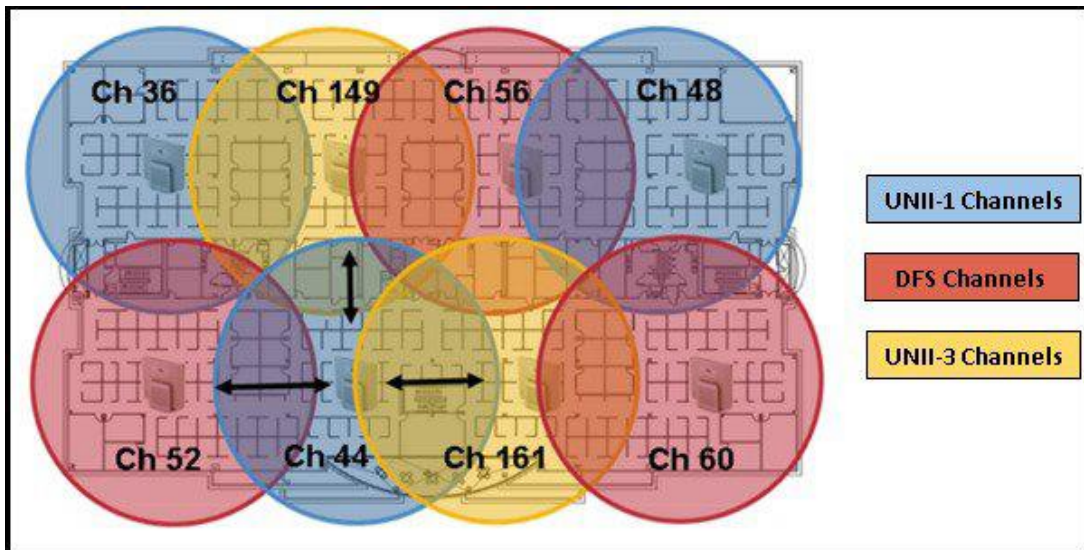
The 5 GHz channels are free of common devices operating on 2.4 GHz frequency such as Bluetooth, video cameras, and microwave ovens. With more channels being available on 5 GHz, there is a higher frequency re-use along with the channel utilization being generally lower due to the reduced co-channel interference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

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 recommend 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 app performance, a wireless network typically reaches capacity when the utilization reaches between 40 to 50% on 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 mitigated. 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 channel(s) to only the affected APs, and not globally across all APs.

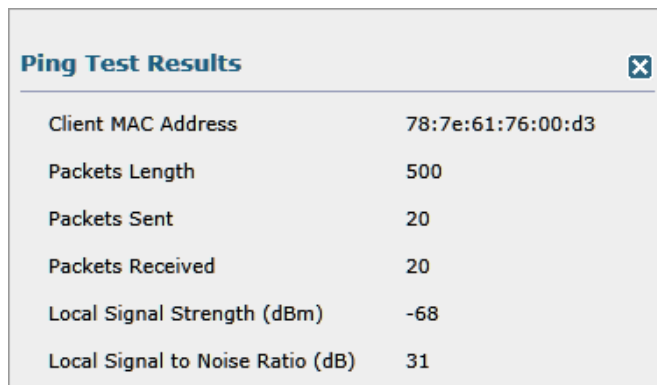
Note: Refer to RRM guidelines in Enterprise Mobility Design Guide for more details:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide.html.

To estimate if the current 5 GHz AP coverage is sufficient for apps 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) or 25 or higher should be maintained at all times. Such levels observed on an iOS device imply that Mac computers will benefit from at least the same signal levels. The same link test can be run for a Mac computer.

Performing a Link Test for an iOS device or Mac computer 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.



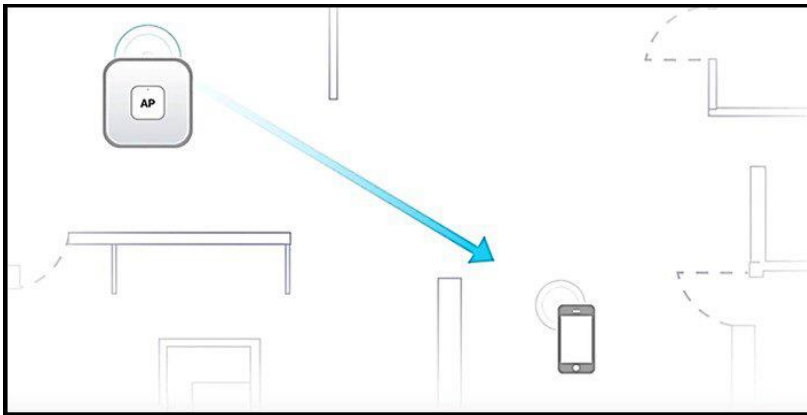
The screenshot shows a dialog box titled "Ping Test Results" with a close button (X) in the top right corner. The dialog contains a table with the following data:

Client MAC Address	78:7e:61:76:00:d3
Packets Length	500
Packets Sent	20
Packets Received	20
Local Signal Strength (dBm)	-68
Local Signal to Noise Ratio (dB)	31

ClientLink Beamforming

Cisco's patented beamforming technology – [ClientLink](#) functions to optimize the connection reliability for all devices. This is especially important for highly 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 iOS devices and Mac computers 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 iOS device

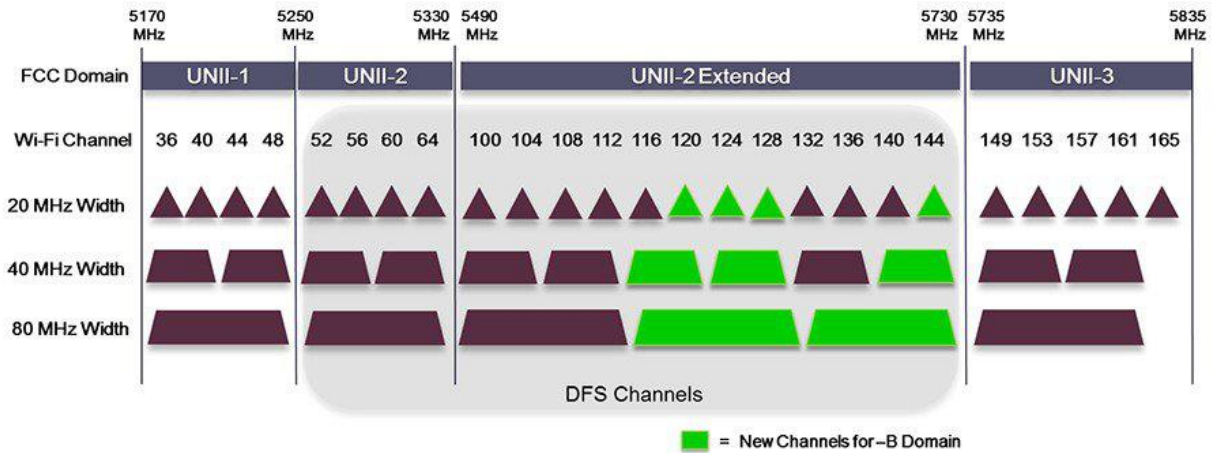


The core benefit of ClientLink technology is improved quality of Wi-Fi signal between the AP and the wireless client devices. The resulting high-quality link between the AP and the client device increases the chances of the client to remain connected at a higher data rate, and promotes the quality of 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.

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 approximately 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

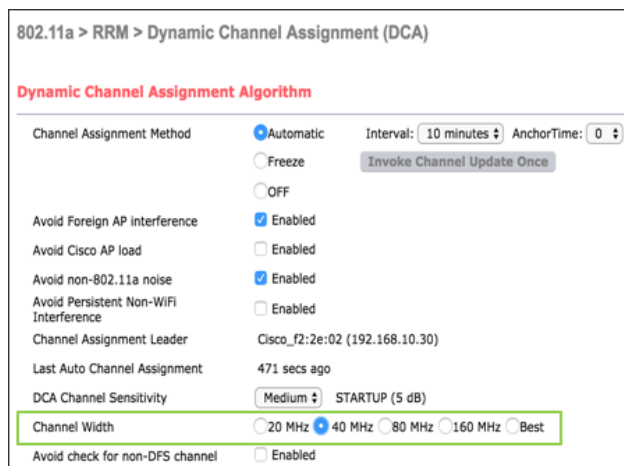


Cisco and Apple recommends the use of 40 MHz channel widths in environments where throughput performance is required, and 20 MHz for high AP/Client density deployment environments. To allow for an efficient 40-MHz wide deployment the use of DFS channels may become necessary in order to achieve optimal 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 12 (in the USA).

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.

Choose 20, 40 or 80 MHz. The best width based on your network environment can also be automatically determined by RRM. To enable this option, choose Best Channel Width, ensure that you limit the DBS algorithm

to a max bandwidth of 40 Mhz using the command line argument -(Cisco Controller) >config advanced 802.11a channel dca best-width-max 40. This will limit DBS assignments to a max of 40 MHz, by default the maximum is 80 Mhz.

DCA bandwidth can also be selected using an RF Profile and applied only to AP's contained in a specific AP group if global assignment is not desired.

Note: Refer to DCA guidelines in Enterprise Mobility Design Guide for more details:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide.html

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 iOS devices and Mac computers, 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 app 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 and disabling low 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 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

The screenshot shows the Cisco Wireless configuration interface for 802.11a Global Parameters. The left sidebar contains a navigation menu with categories like Access Points, Radios, Advanced, Mesh, ATF, RF Profiles, FlexConnect Groups, OEAP ACLs, Network Lists, and 802.11a/n/ac. The main content area is titled '802.11a Global Parameters' and is divided into 'General' and '802.11a Band Status' sections. The 'General' section includes settings for Network Status (Enabled), Beacon Period (100), Fragmentation Threshold (2346), DTPC Support (Disabled), Maximum Allowed Clients (200), RSSI Low Check (Disabled), and RSSI Threshold (-80). The '802.11a Band Status' section shows Low, Mid, and High bands all set to Enabled. A 'Data Rates**' section is highlighted with a green box, listing rates from 6 Mbps to 54 Mbps with modes: 6 Mbps (Disabled), 9 Mbps (Disabled), 12 Mbps (Mandatory), 18 Mbps (Supported), 24 Mbps (Mandatory), 36 Mbps (Supported), 48 Mbps (Supported), and 54 Mbps (Supported). Below this is the 'CCX Location Measurement' section with a Mode set to Disabled. A footnote explains that 'Mandatory' implies clients must support the rate, while 'Supported' implies they can.

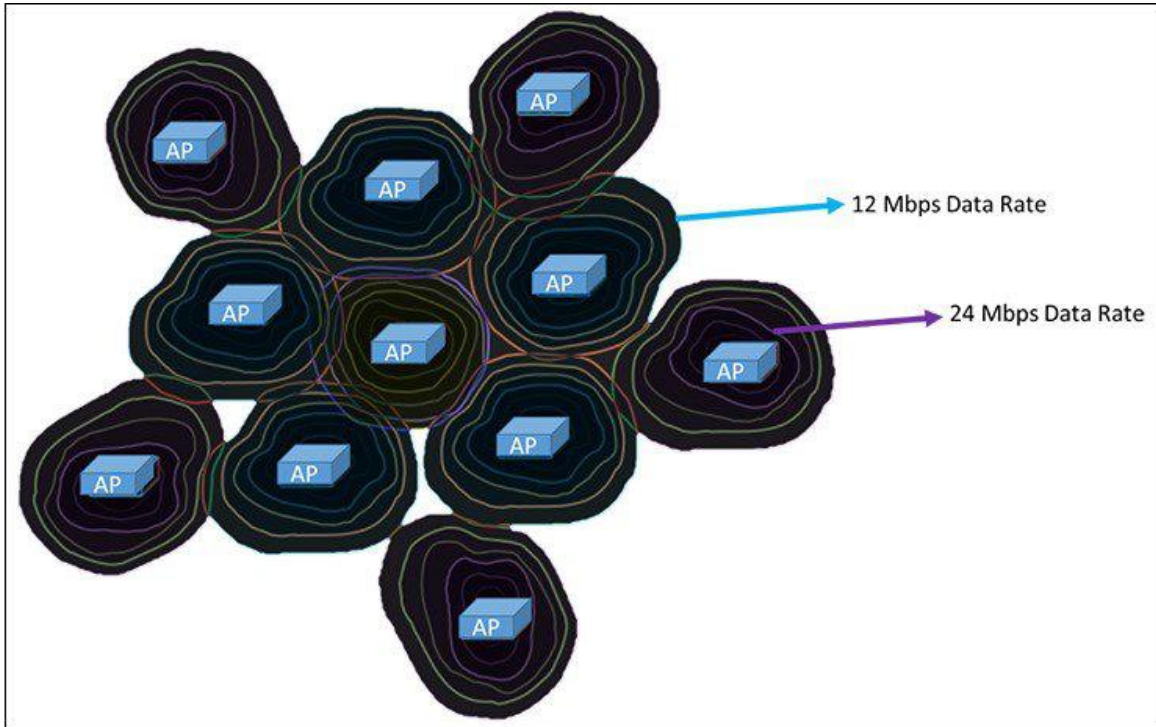
Navigate to **Wireless > 802.11a/n/ac > Network** to specify the rates at which data can be transmitted between the AP and the client.

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 should be able to receive packets currently set at the lowest mandatory rate and their radios must physically support the highest mandatory data rate. If they do not receive currently lowest mandatory rate frames the client may miss beacons, which may lead to disconnection. If more than one data rate is set to mandatory, multicast is sent at highest common mandatory rate of all associated clients. Broadcasts are always sent at lowest (not highest) mandatory rate.
- 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. Note that allowing a supported data rate below the minimum mandatory data rate may inhibit roaming as it increases the overlap area of the cells if not properly evaluated.
- Disabled:** The AP does not transmit data at this rate.

Configuring low data rates as mandatory increases the range at which packets sent by the AP can be received. The lower you set the lowest configured mandatory data rate, the greater the range of beacons and other packets from the AP. 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 app performance.

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



Cisco and Apple recommend 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 iOS devices and Mac computers on Cisco Wireless LAN. If the 5GHz coverage is marginal, setting 6 Mbps as the lowest mandatory rate could potentially resolve issues. 802.11n and 802.11ac rates all are of the Supported type (the 802.11 standard does not include them in the Mandatory category). Disabling 802.11n/ac rates was not found to improve the marginal performances of wireless clients. As such, Apple and Cisco do not recommend disabling low 802.11n/ac rates, even when low 802.11a rates are disabled.

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

802.1X/EAP Authentication

When iOS devices connect to a WLAN with enterprise security using 802.1X/EAP. It is recommended to take either of the following into consideration for the deployment:

1. Manage iOS client devices through an MDM solution, and push the certificate chain used for the WLAN in question in a corresponding profile. For more information on this, please refer to the following documentation from Apple:
<https://support.apple.com/en-us/HT207866>
<https://help.apple.com/deployment/ios/#/apd7b6d34790>
2. Alternatively, if option 1 above is not possible, use a wildcard certificate in the certificate chain used for the 802.1X/EAP authentications on the RADIUS / AAA server(s) which will service the WLAN in question. For more information on wildcard certificates with Cisco ISE, you can refer to the following document and corresponding excerpt accordingly:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/admin_guide/b_ise_admin_guide_23/b_ise_admin_guide_23_chapter_0111.html -
concept_8ECCCAF1252E40DDB9A786C0AC7BC3B2

Wildcard certificates address issues seen with IOS devices where the client stores trusted certificates within the profile, and does not follow the iOS keychain where the signing root is trusted. When an iOS client first communicates with a secure network, it does not explicitly trust the network certificate, even though a trusted Certificate Authority has signed the certificate. Using a wildcard certificate, the certificate will be the same across all secure networks under the same authority, so the user only has to accept the certificate once and successive authentications to different networks proceed without error or prompting.

If neither of the above methods are utilized, then it is expected behavior on the part of the iOS client device to prompt the user to trust the certificate every time a new RADIUS / AAA server is used to authenticate the iOS client device to the same WLAN. For instance, if the same WLAN is used in two different campuses that each have a dedicated RADIUS / AAA server. Then the end user should expect to have to trust the certificate once again that was used during the 802.1X/EAP authentication. Even if either the intermediate or root certificate is signed by the same certificate authority (CA), and previously trusted at the prior location using that same WLAN. The same may occur if the authentications to the same WLAN are load balanced among several RADIUS / AAA servers, a failover event occurs between RADIUS / AAA servers, and so forth.

Quality of Service

In order to achieve optimal results for apps running on iOS 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 Quality of Service

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](https://tools.ietf.org/html/rfc4594), which is the latest IETF guidelines on DSCP traffic marking) and the 802.11e mapping (for example <https://tools.ietf.org/html/draft-ietf-tsvwg-ieee-802-11-09>).

Table 2. Applied Default QoS marking for the main categories of traffic

Cisco 802.1p User Priority Traffic Type	IP DSCP (PHB Value)	IEEE 802.11e/WMM User Priority	Designative (Informative)	Cisco Designative
Reserved	56 - 63	7 (unused)	—	—
Reserved	48 - 55	6 (unused)	—	—
Voice	46 (EF)	6	Voice	Platinum
Signaling	40 (CS5)	5	Video	Gold
Interactive Video	34, 36, 38 (AF4x)	4	Video	Gold
Streaming Video	26, 28, 30 (AF3x)	4	Video	Gold
Voice Control (Signaling)	24 (CS3)	4	Video	Gold
Background (Transactional/Interactive)	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	Bronze

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 or above (Further updated in AireOS 8.3)

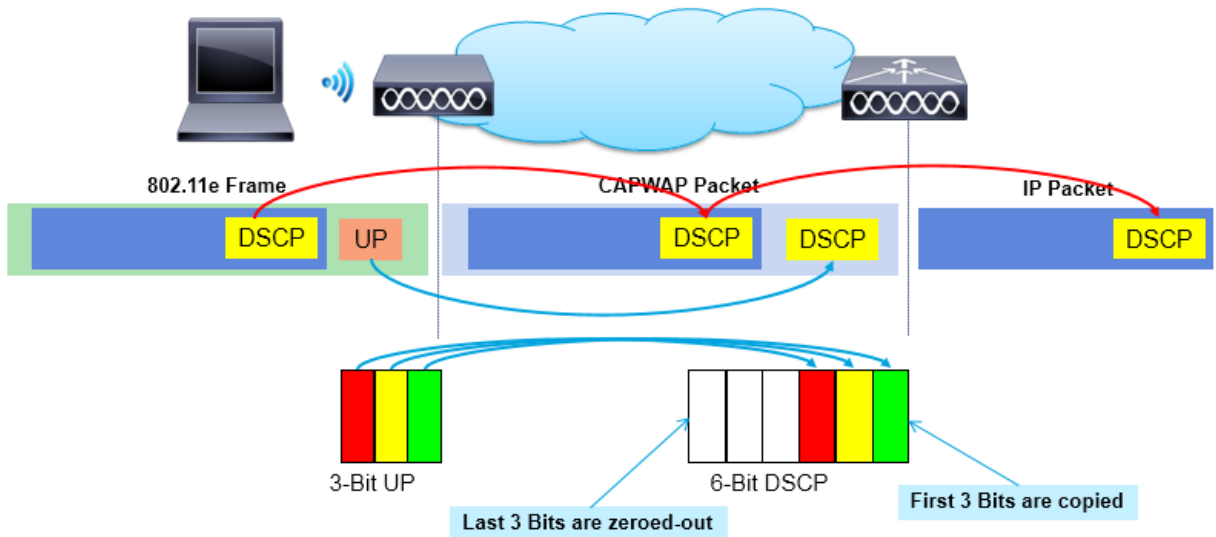
The screenshot displays the Cisco Wireless QoS Map Config page. The 'Qos Map' is set to 'Enable'. Under 'Up Stream', 'Trust DSCP UpStream' is selected. The 'DSCP to UP Map' section shows a table with columns 'UP', 'Start DSCP', and 'End DSCP'. The 'DSCP Exception List' section shows a table with columns 'DSCP' and 'UP'.

UP	Start DSCP	End DSCP
0	0	7
1	8	15
2	16	23
3	24	31
4	32	39
5	40	47
6	48	62
7	63	63

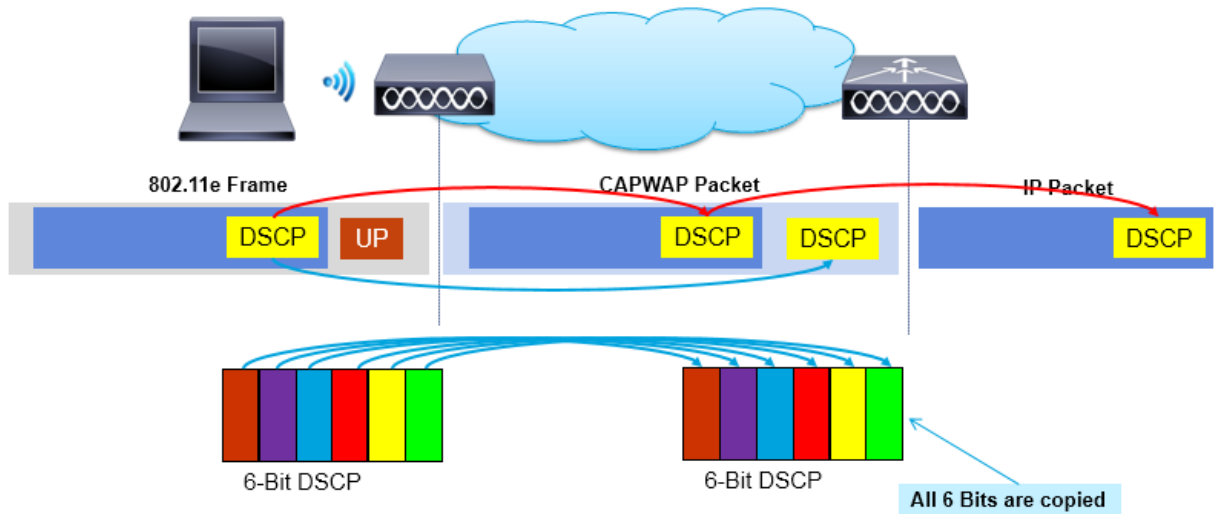
DSCP	UP
56	0
48	0
46	6
44	6
40	5
38	4
36	4
34	4
32	5
30	4
28	4
26	4
24	4
22	3
20	3
18	3
16	0
14	2
12	2
10	2
8	1

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

Trusting upstream UP is a common practice in the Wi-Fi industry. However, its result is to derive the CAPWAP outer header DSCP (Layer 3) QoS value from the UP (Layer 2) value. In general, Layer 2 values are valid on the local segment, and Layer 3 values are valid across segments. Deriving global values from locally-significant values is not considered best practice. Additionally, deriving DSCP values from UP values means that 3 QoS bits are used to translate into a 6-bit field, resulting in under-utilization of DSCP possibilities.



AireOS code 8.1 MR introduces the possibility to trust DSCP upstream, and derive the CAPWAP outer header DSCP (Layer 3) QoS value from the wireless client DSCP (Layer 3) value. The SSID QoS profile is used as a ceiling, to avoid QoS policy abuse. IOS clients mark DSCP and UP values. If your wireless clients mark DSCP values, Cisco recommends that you enable upstream DSCP trust, which allows the infrastructure to take full advantage of the DSCP 6 bit granular possibilities.



When enabling upstream DSCP trust, you can also decide on a custom DSCP to UP mapping. The default DSCP-to-UP mapping follows the rules mentioned in table 2 above. A custom mapping allows a more deterministic translation between incoming DSCP values and UP values. In particular:

Some DSCP values are not expected in a standard access network, for example, all odd DSCP values. A standard DSCP value is expected to be an even number. An odd DSCP number implies that the DSCP field least-significant bit, called MBZ (Must Be Zero), would be set to 1. Using a custom DSCP to

UP map allows you to make sure to all unexpected DSCP values are translated into best effort transmission in the cell, thus reducing the risk of QoS policy abuse.

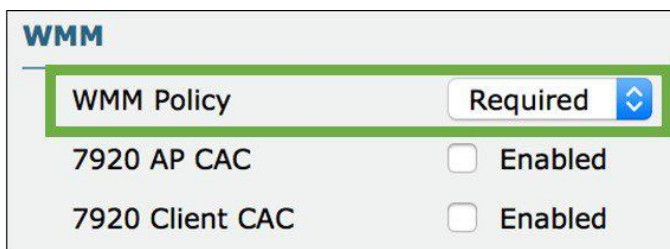
You can set a list of up to 21 exceptions. This configuration allows you to ensure that well-known DSCP values translate into recommended UP values, regardless of the value of the 3 MSBs.

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 app 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, 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 iOS devices and Mac computers only, then it is recommended to go with the 'required' setting.

Figure 10. Configuring WMM on the WLAN



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. However, WMM support is mandated for 802.11n and 802.11ac certification. Any 802.11n or 802.11ac client is required to support WMM. Networks that include a large proportion of non-WMM clients may set the WMM Policy to Allowed. iOS and Mac clients will enable WMM while non-WMM clients will also be allowed to join the WLAN. However, the presence of non-WMM clients may negatively affect the overall performance of the WLAN.

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 app has to appropriately support WMM for the upstream traffic. iOS devices can support the network-level WMM settings (e.g. platinum or voice) in addition to app-layer support. Apple provides app developers the ability to mark their packets at the app layer that ensures specific packets queued to appropriate WMM level. App developers should ensure that the iOS app tags the appropriate WMM marking so client's upstream traffic is properly tagged

WLAN Quality of Service Profiles

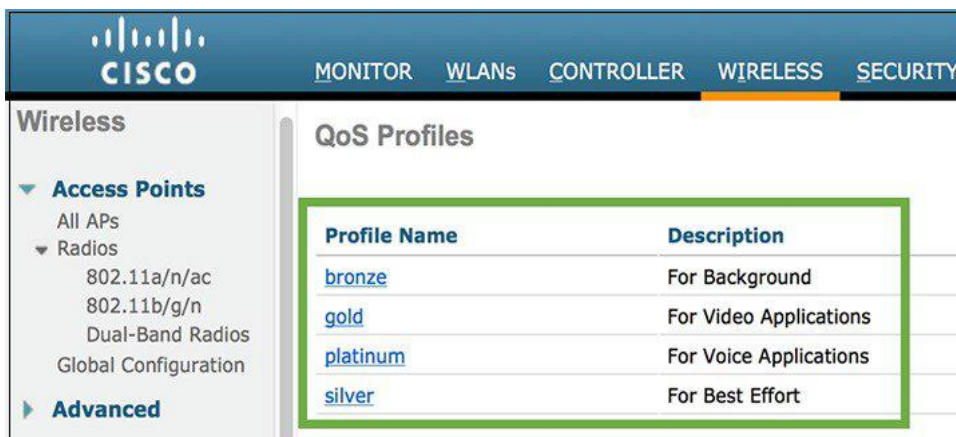
From the Cisco WLAN Controller user interface, you can assign a QoS profile (Platinum, Gold, Silver, and Bronze) to each SSID. This profile determines the highest QoS level expected and allowed to be used on this SSID. The role of a QoS profile is to set the ceiling (the maximum level of QoS that clients 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. The target QoS value for multicast and non-WMM traffic is configurable.

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 apps 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 iOS devices communicate.

Figure 11. Verifying QoS Profile configurations



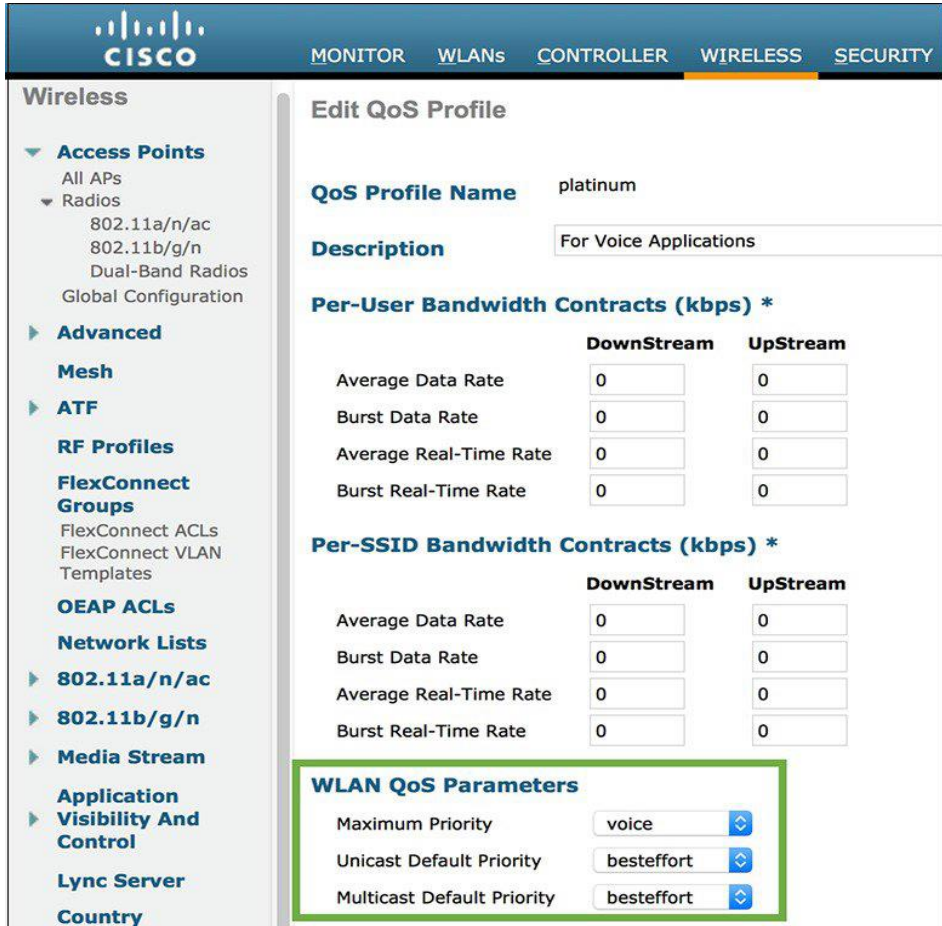
The screenshot shows the Cisco WLAN Controller interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The 'WIRELESS' tab is selected. On the left, the 'Wireless' menu is expanded to show 'Access Points' (All APs, Radios) and 'Advanced'. The main content area displays 'QoS Profiles' with a table listing four profiles: bronze, gold, platinum, and silver, each with a description of its intended use.

Profile Name	Description
bronze	For Background
gold	For Video Applications
platinum	For Voice Applications
silver	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



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 iOS devices, you will need to make the parameter changes accordingly.

To honor the traffic marked as voice for all iOS 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.

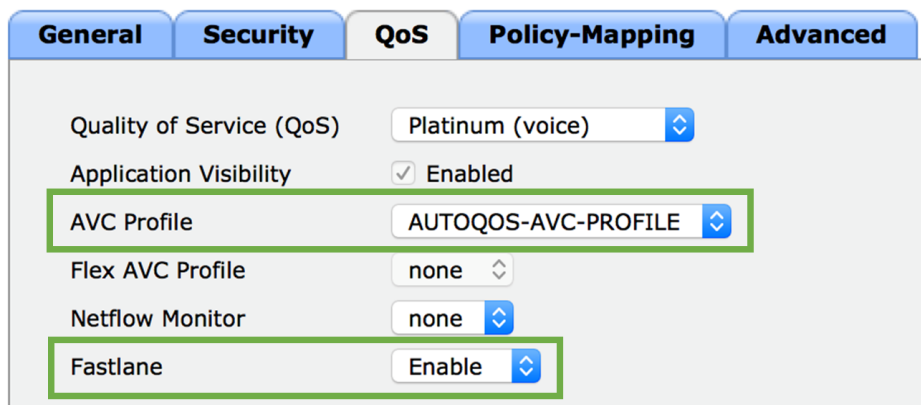
Cisco Fast lane Configurations

This configuration is only applicable to Cisco controllers running AireOS 8.3 or later, devices running iOS 10 or later and MacBook computers running macOS High Sierra 10.13 or later.

The Cisco Fast lane configuration is an easy way to ensure that QoS is optimally configured in your WLAN controller, especially if iOS or Mac clients are expected to be a sizeable portion of the wireless clients. Configuring a WLAN controller for QoS can be time consuming. This configuration also implies the configuration of multiple combined elements, which may be a challenging task for administrators.

To facilitate optimal configuration of QoS on a WLAN controller, especially when devices running iOS 10 or later or computers running macOS High Sierra 10.13 or later are expected to be a sizeable part of the wireless client base, Cisco has created a Fast lane option in the QoS tab of the WLAN configuration pages.

Figure 14. Configuring Fastlane on the WLAN



Note: Enabling Fast lane (on a WLAN for the first time) will automatically disable all WLANs and Network. It will be reverted to the previous state once configuration is complete. It will also create an AUTOQOS-AVC-PROFILE, if it does not exist already.

When enabling the Fast lane QoS option for a WLAN, the following automatically happens:

- The 5 GHz and 2.4 GHz networks are temporarily disabled (to allow for the configuration below to be activated)
- Non-WMM and multicast traffic is set to Best Effort in the Platinum QoS profile
- UDP traffic bandwidth limitation is set to 0 (no restriction) in the Platinum QoS profile
- The Platinum QoS profile is applied to the configured WLAN
- The Fastlane EDCA profile, matching the recommendations of the new revision of the 802.11 standard (802.11-2016), is activated for both bands

- Wireless CAC (ACM) is enabled for Voice traffic (for both bands), based on load calculation (in AireOS code release 8.5 and before). 50% of the bandwidth is allocated for voice traffic, and 6% for roaming voice traffic (in AireOS code release 8.5 and before). Wireless CAC is not enabled in AireOS code release 8.6 or later.
- DSCP is trusted upstream, and a custom DSCP-to-UP map is configured, as displayed in figure 9 above.
- The fastlane feature is enabled on the WLAN. This feature is used in the context of Fast lane profiles explained in the next section.
- An AUTOQOS-AVC-PROFILE AVC profile is created, if it does not exist already. This profile ensures that well-known applications (including voice and video traffic from applications such as jabber, Cisco phones, Webex, Lync) are marked for QoS appropriately. This profile can later be edited. This profile is not mandatory for Fastlane, it provides a convenient pre-installed AVC profile to facilitate deployments.
- The 5 GHz and 2.4 GHz networks are re-enabled.

An important aspect of Cisco Fast lane is Wireless CAC. The UP 6 queue has very high priority and is intended for Voice traffic. To ensure that no QoS policy abuse would take place in the WLAN, the 802.11 standard and the WMM certification allow the infrastructure to verify what traffic stations intend to send to this queue. This verification relies on the Access Control Mandatory (ACM) bit being enabled for the UP 6 queue. When this bit is enabled, stations that intend to send UP 6 traffic must first send an Add Traffic Stream (ADDTS) request to the AP. This request contains a field called Traffic Specification (TSPEC) that describes the intended traffic. The AP responds with an ADDTS response, that authorizes or declines the intended traffic. When ACM is enabled, a station should not use the UP 6 queue without ADDTS exchange.

When ACM is enabled and stations send upstream traffic with UP 6 without going through the ADDTS exchange, the return traffic is best effort. In other words, the wireless infrastructure does not honor UP 6 on the return path.

Cisco and Apple worked extensively together to ensure that traffic would receive the QoS marking matching IETF recommendations. As a result, traffic coming from devices running iOS 10 or later, and from computers running macOS High Sierra 10.13 and later is treated differently in a Cisco wireless infrastructure running AireOS code 8.3 or later. Even though the ADDTS exchange may not occur, UP 6 traffic coming from devices running iOS 10 or later, and from computers running macOS High Sierra 10.13 and later is honored, and the return traffic also goes through the privileged UP 6 queue. To allow for this mutual trust, special bits are present in beacons, probe requests, probe responses and association frames, to allow the client and infrastructure sides to acknowledge each other and establish this trust.

A practical result of enabling ACM with Cisco Fast lane is that stations performing ADDTS exchange, and devices running iOS 10 or later, and computers running macOS High Sierra 10.13 and later sending voice traffic (even if they do not perform ADDTS exchange), can benefit from the UP 6 queue for voice traffic. However, other stations that do not perform ADDTS will have to use another queue (typically Video or Best Effort). In a congested environment, this configuration may result in lower performances for these stations. For this reason, Wireless CAC is not enabled automatically when Fastlane is configured in AireOS 8.6 or later. Wireless CAC can be enabled manually on the WLAN controller with all AireOS code releases. Wireless CAC is enabled automatically when Fastlane is configured in AireOS code releases 8.3, 8.4 and 8.5.

Cisco Fast lane Profiles

Cisco wireless infrastructure running AireOS 8.3 or later and devices running iOS 10 or later, and computers running macOS High Sierra 10.13 and later perform a mutual client-infrastructure recognition exchange. When Fastlane is enabled on a WLAN (please see Cisco Fast lane configuration section above), the wireless infrastructure informs devices running iOS 10 or later and computers running macOS High Sierra 10.13 and later that a special treatment can be used for apps that use QoS marking. Some apps can be allowed to use QoS marking while others will be sent in the best effort or background queues.

System administrators can deploy configuration profiles to iOS devices and Mac computers using any EMM or MDM solution or the Apple Configurator. With iOS 10 and macOS High Sierra 10.13 or later, these profiles can be simple QoS profiles. Such profiles list applications that are allowed to use QoS in a Cisco fast lane network. These profiles are deployed following the standard profile provisioning procedure for devices running iOS 10 or later and macOS High Sierra 10.13 or later. Listing which apps should be in the whitelist allows the system administrator to privilege apps that are business-relevant, and push to the best effort or background queues applications that are not relevant to the business.

With Fast lane profiles, the following behavior occurs:

- Fastlane is activated on a per WLAN basis on a Cisco WLAN controller running 8.3 or later, by enabling the Fastlane function in the WLAN QoS configuration tab.
- By default, all apps are whitelisted. When no profile is pushed to devices running iOS 10 or later, or macOS High Sierra 10.13 or later, in a Cisco Fast lane network, all apps can mark upstream QoS.
- When a QoS profile is applied to a supporting iOS device or Mac computer in a Fastlane network, only those applications that are in the whitelist are allowed to mark upstream QoS. Applications that are not in the whitelist are sent as best effort (or background, if their QoS marking is less than best effort).
- Apple Facetime and Wi-Fi Calling are a specific traffic category, and are whitelisted by default. They can be sent to the best effort queue by deactivating a specific bit (QoSMarkingAppleAudioVideoCalls) in the QoS profile. Cisco does not recommend deactivating this bit for most networks.
- In a non-Fast lane network, upstream DSCP is generally unmarked, and the concept of whitelist does not apply.

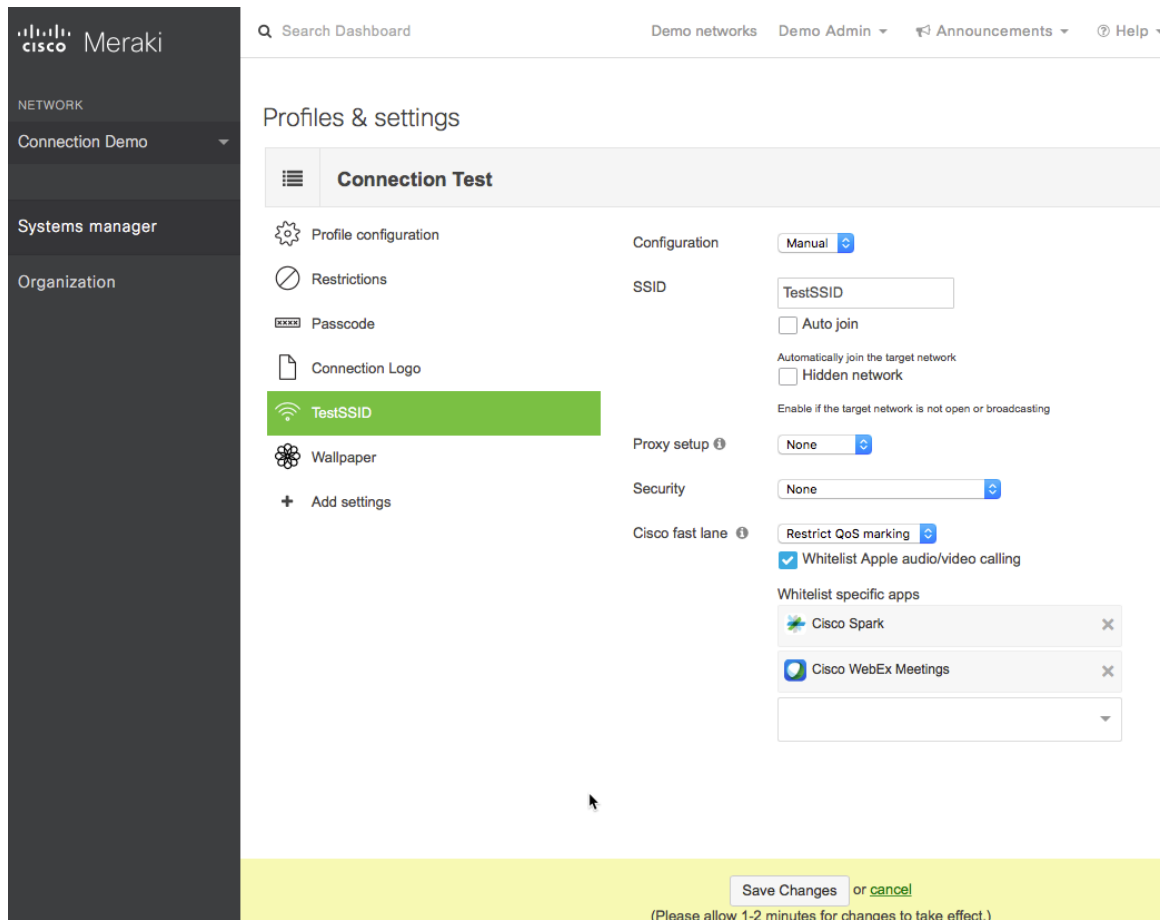
Deploying Cisco Fast lane Profiles with Systems Manager

Cisco's Enterprise Mobility Management (EMM) solution, Meraki Systems Manager, can be used to manage mobile devices. Devices running iOS 10 or later and macOS High Sierra 10.13 and later can be provisioned with a Fast lane profile (please see Cisco Fast lane profiles section above) in order to whitelist specific apps, which are allowed to mark upstream QoS.

Fast lane profiles can be configured in the Meraki dashboard by navigating to Systems Manager > MDM > Settings > Wi-Fi and selecting the option to 'Restrict QoS marking'. Profiles will be pushed over the air and can be scoped using tags (see the note below for more about tagging). Fast lane profiles are added into a wireless profile.

Systems Manager integrates directly with the iOS App Store, and administrators can search for and add apps directly to the fast lane profile as shown in the figure below.

Figure 15. Configuring Cisco Fast lane settings and adding apps



Refer to the following for general information or more information about tagging:

<https://meraki.cisco.com/products/systems-manager/>

<https://documentation.meraki.com/SM/Tagging>

Note: Cisco Fast lane profiles are not available in the legacy version of Systems Manager. Refer to the following page for more information about upgrading to the new version of Systems Manager:

https://documentation.meraki.com/zGeneral_Administration/Licensing/Systems_Manager_Licensing#Upgrading_from_Legacy_SM

Optimized Enhanced Distribution Channel Access

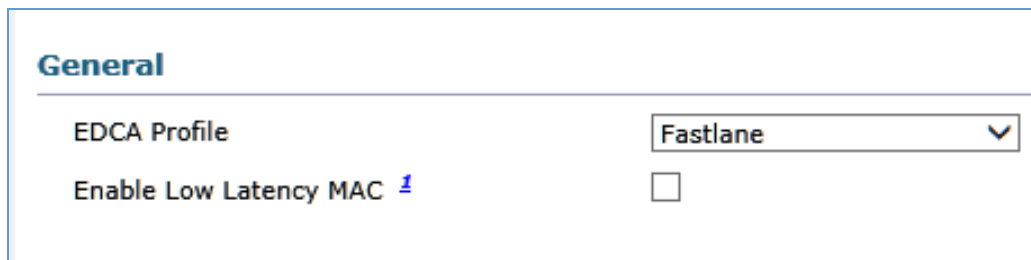
This configuration is only applicable to Cisco controllers running AireOS 8.3 or later. AireOS controllers also implement a new EDCA profile called Fastlane. This optimized EDCA feature is derived from the latest version of EDCA in the IEEE 802.11 standard, and directly benefits iOS devices connecting to Cisco infrastructure.

Previous generation of EDCA configurations based on IEEE 802.11e-2005 allowed voice and video queues in limited time consumption. Other queues were not limited in time-consumption. The updated version improves the mechanism to control the traffic queues to allow faster speeds, and allocate limited time consumption values for all queues, based on the protocols enabled in the cell. With optimized EDCA enabled on the Cisco WLAN controller, iOS devices, Mac computers and other clients connected to a Cisco infrastructure will automatically implement new 802.11 EDCA recommendations, benefiting all cell devices. This provides a better environment for Real voice / video traffic to be accurately prioritized, while other & unmarked traffic to be controlled.

Configuring Optimized EDCA

The new IEEE-802.11 EDCA Parameters can be enabled by choosing Fastlane profile for the EDCA parameter on the controller running AireOS 8.3 or above:

Figure 16. Configuring EDCA for Cisco Fast lane parameters



The screenshot shows a configuration page titled "General" for EDCA Parameters. It contains two settings: "EDCA Profile" is set to "Fastlane" via a dropdown menu, and "Enable Low Latency MAC" is an unchecked checkbox.

Navigate to Wireless > 802.11a/n/ac > EDCA Parameters to assign the Fastlane configuration to the EDCA settings.

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

App 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 1300 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 or later, operating with next-generation Network-Based Application Recognition (NBAR2) engine 13 and above. With this capability, you can

correctly identify all apps running on iOS devices or Mac computers 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.

After 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 iOS devices or Mac computers 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 iOS devices or Mac computers with Cisco Jabber

Cisco Jabber is available on all iOS devices and Mac computers as a collaboration app. It offers several types of services: File transfer, app 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 voice 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 iOS devices or Mac computers. Jabber traffic should already be marked properly, both coming from iOS and Mac clients and the infrastructure. However, this section can be used as a general guiding principle for other business-relevant applications.

This policy ensures that marking will be re-established correctly, if it has been modified on the packet path. 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.

Note: If Cisco Fast lane is enabled on Cisco controller running AireOS 8.3 or later, the AUTOQOS-AVC_PROFILE, which is automatically applied already contains Jabber app. It is recommended to use the auto profile over manual configuration shown in this section.

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

Figure 15. Creating an AVC profile for Jabber



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

Figure 16. Adding rules to mark the application traffic types to the AVC Profile



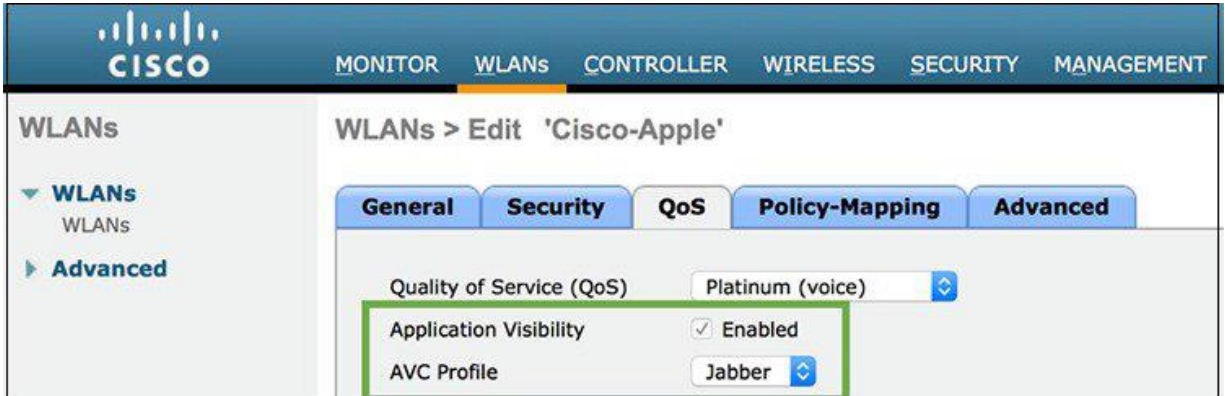
Navigate to **Wireless > Application Visibility And Control > AVC Profiles** and click on the profile to add a rule for the app to be marked.

Figure 17. Verifying all the rules for the application traffic type associated to the AVC Profile



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.

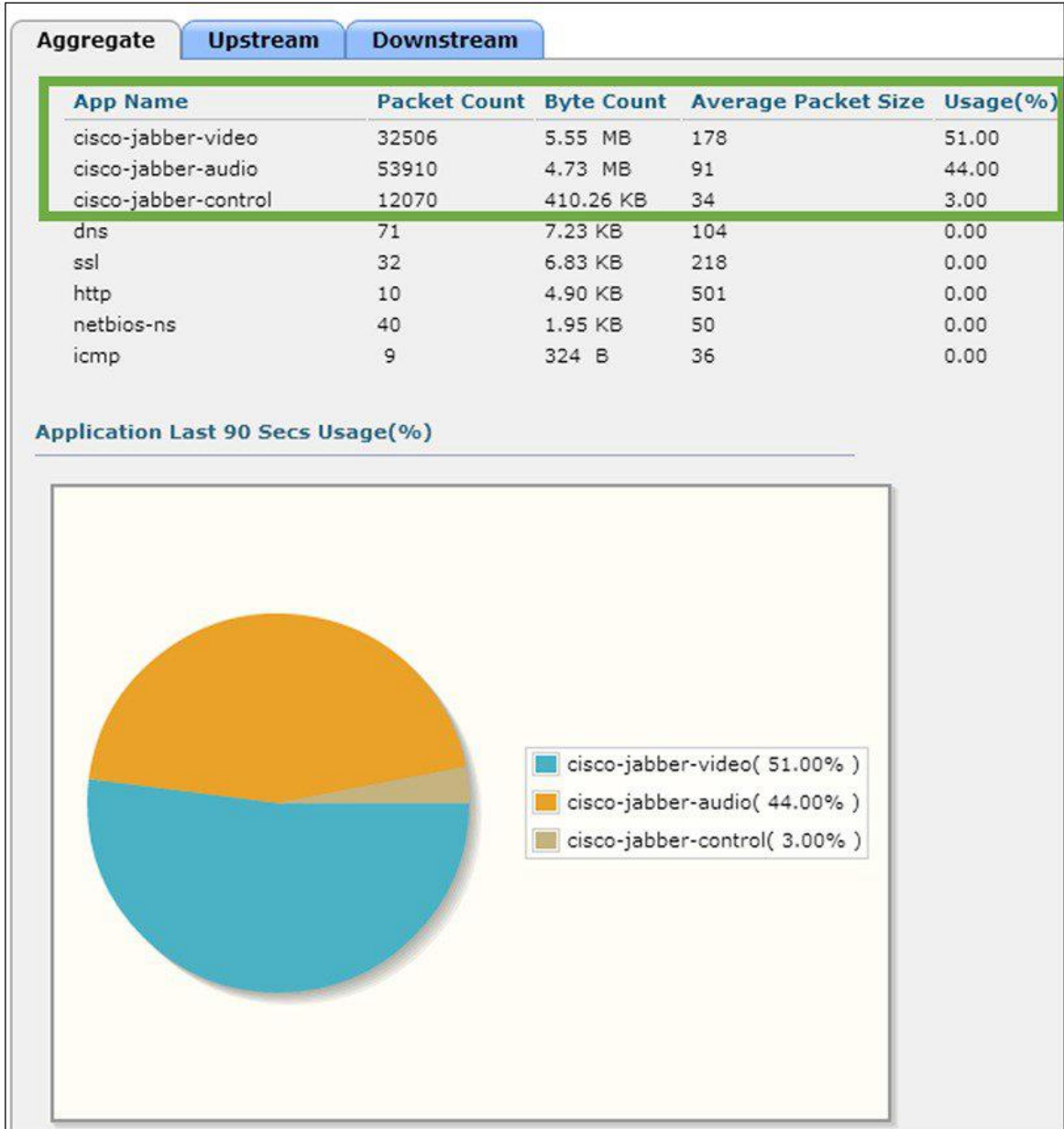
Figure 18. Enabling AVC on the WLAN, and applying the AVC Profile



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 iOS devices and Mac computers to the WLAN, and initiate Jabber voice and video calls on the network.

Figure 19. Verifying app 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.

Cisco Wi-Fi Optimization for iOS 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. Users moving while actively using a real-time app on a smartphone or tablet is common. As smartphones can be held close to the body (the human body limits RF signals), sudden changes to the RF signal are common for small form factor devices (smartphones, small tablets). By contrast, computers are larger, commonly include more than one antenna, are held farther away from the body, and consequently suffer less from sudden RF changes than smartphones or tablets. Providing smartphones with tablets with the ability of roaming extremely fast is therefore very important, especially for real-time apps. Cisco Wi-Fi optimizations for iOS mainly implies 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	Cisco Implementation	Apple Implementation
802.11r – Fast Transition (FT)	AireOS v7.2	iOS 6
Adaptive 802.11r	AireOS v8.3	iOS 10
802.11k – Neighbor Reporting	AireOS v7.4 (Recommended v8.0 MR3+)	iOS 6 (Recommended iOS 8 or above)
802.11v – BSS Transition Management	AireOS v8.0	iOS 7

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 app disruption.

Cisco and Apple recommend enabling 802.11k and 802.11v on the Cisco Wireless LAN infrastructure for supporting iOS devices in order to implement an enterprise environment configured for efficient roaming. Mac computers do not require 802.11v and 802.11k, but associate transparently to WLANs where these protocols are enabled. Cisco and Apple also recommend enabling 802.11r on the Cisco Wireless LAN infrastructure to increase the efficiency of key exchanges during roaming. However, this recommendation should only be considered for a WLAN where all expected devices have support for 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. Enabling 802.11v and 802.11k should not have any impact on non-supporting devices. These devices will just not benefit from the roaming enhancements brought by these two standards. See [Apple's device list](#) to check whether your iOS 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.

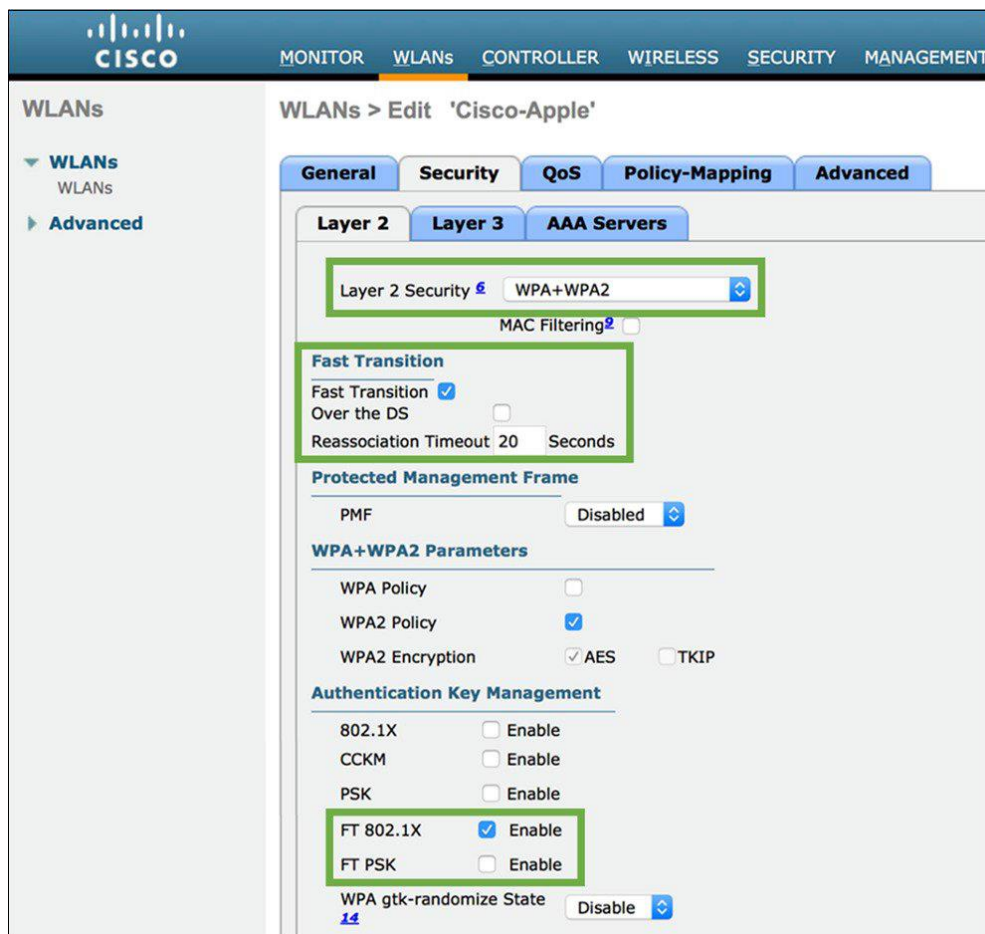
iOS devices and Mac computers make use of RSSI thresholds to trigger the roam scanning mechanism. This trigger threshold is the minimum signal level a client requires to maintain the current connection. IOS clients monitor and maintain the current Wi-Fi connection until the RSSI crosses the -70 dBm threshold. Mac clients monitor and maintain the current Wi-Fi connection until the RSSI crosses the -75 dBm threshold. Once crossed, the client initiates a scan to find a suitable AP that can roamed to.

802.11r - Fast Transition

802.11r is an enhancement which allows for the Client-AP handshake and key material exchange 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 apps such as voice and video over Wi-Fi.

Configuring 802.11r on Cisco Controller

Figure 20. 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

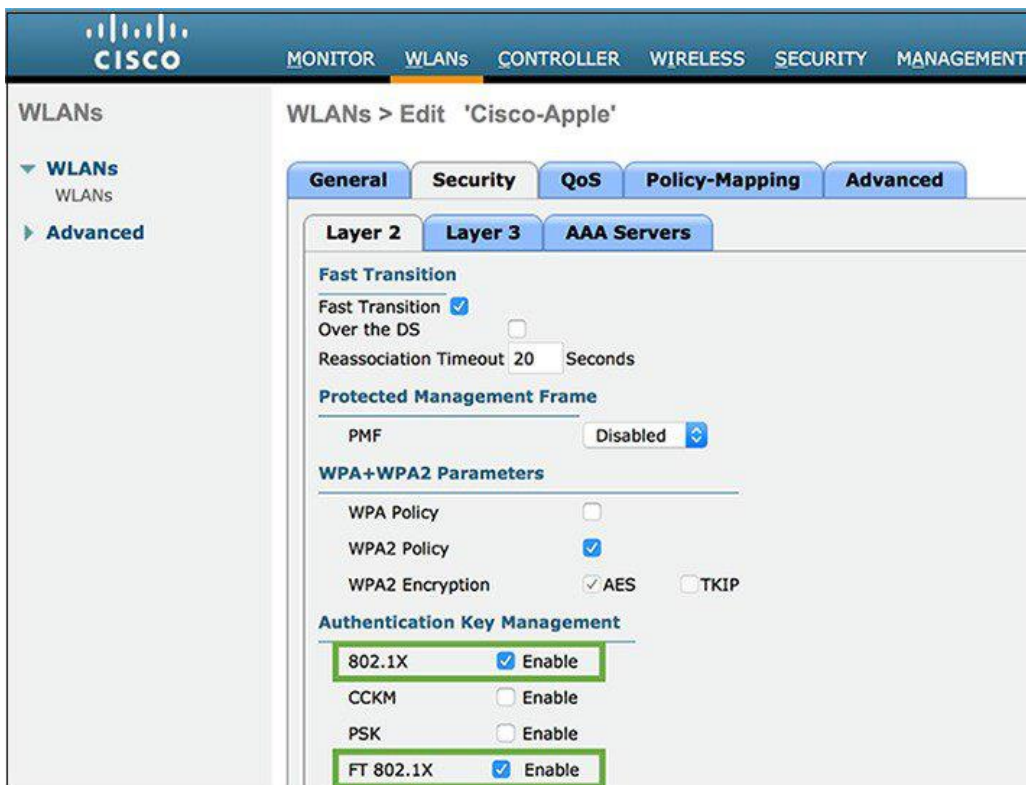
Unchecking Over-the-DS implies FT uses over-the-air mode. For a high density enterprise environment, Cisco and Apple recommend to use 802.11r with Over the air transition for optimal 11r-FT performance.

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 clients that don't support 802.11r as they are unaware of how to process the Fast Transitions Information Elements (IEs) during authentication. 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 21. 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 join this 802.11r-mixed-mode WLAN. Clients with newer wireless LAN chipsets and clients with updated chipset drivers with **11r-compatibility** may all be able to use the 11r mixed-mode SSID configuration. For example, Apple introduced the 11r-compatibility drivers for the MacBook notebook computers running OS X Mavericks v10.9, which allowed the MacBook to correctly identify and associate to a mixed mode SSID (e.g. FT-PSK + PSK). Any MacBook running an older version of macOS (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.

Adaptive 802.11r

The configuration is to all devices, but the adaptive 11r feature will only be applied to supporting iOS devices running iOS 10 or later. All other devices will be able to associate using standard WPA2 (including Mac clients).

Adaptive 802.11r is an enhancement feature specifically designed for iOS devices associating to a Cisco WLAN infrastructure in order to optimize the speed of key negotiation during roaming events in encrypted (WPA2) WLANs. With Cisco AireOS 8.3 and later configured for Adaptive 11r, all iOS devices running iOS 10 or later, upon associating to the Cisco AP, will automatically implement 802.11r even when 11r is not openly enabled on the wireless network configuration.

Note: iOS devices supporting Adaptive 802.11r are iPhone 6S, 6S Plus, iPhone 7, iPhone SE, iPhone 8, iPhone 8 Plus and later, iPhone X, and iPad pros.

Figure 22. Enabling Adaptive 802.11r on the WLAN

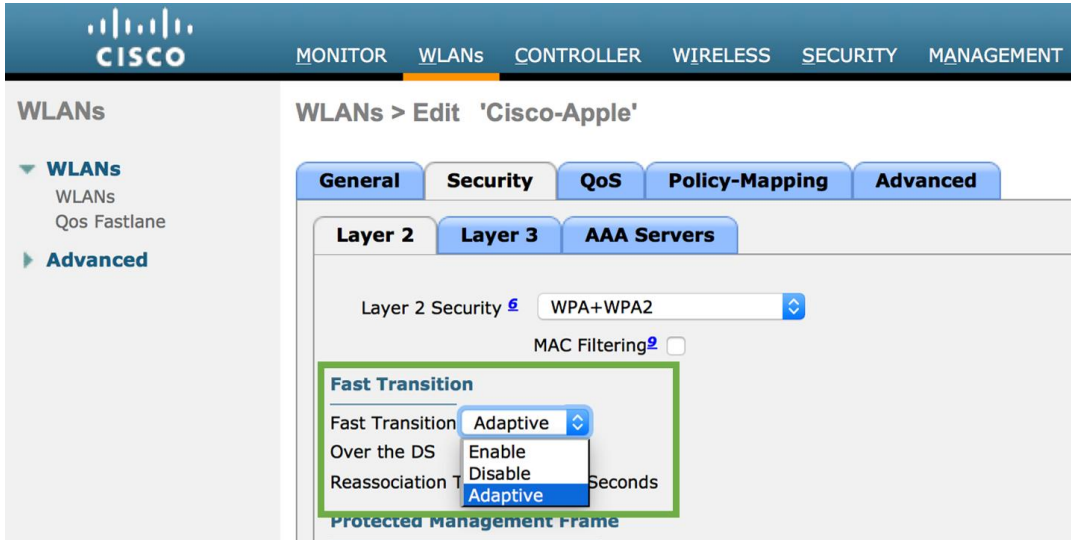
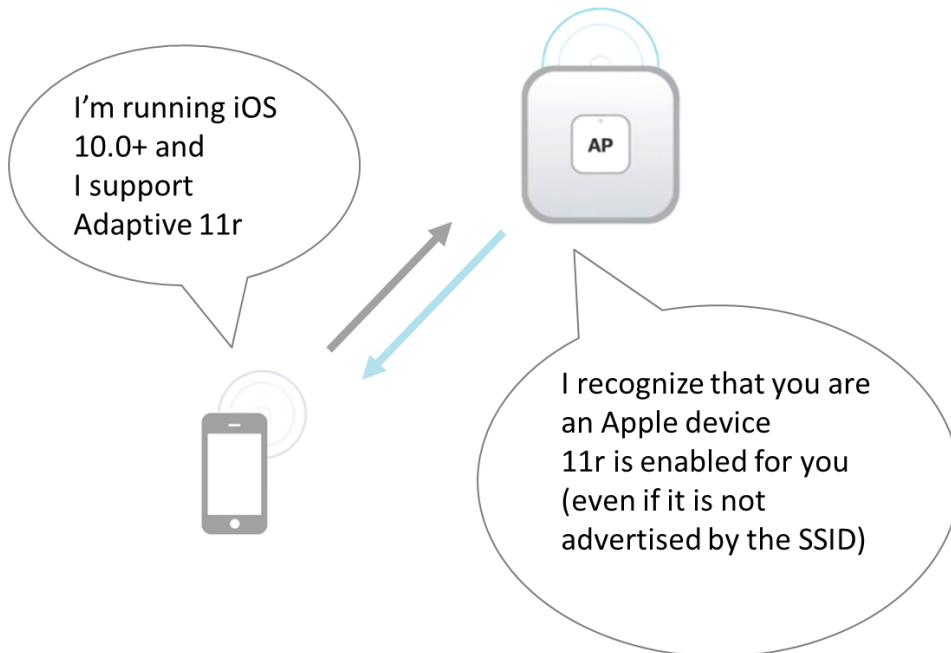


Figure 23. An iOS device running iOS 10 or above automatically gets the Adaptive 802.11r configuration from a controller running 8.3 or above configured with adaptive 11r



Once adaptive 802.11r is enabled on the WLAN, the AP provides the information in the beacons. In Association Request from devices running iOS 10 or later, 802.11r is automatically requested, as the device is aware of the adaptive 802.11r configuration before it even initiates the association request. The AP then provides the Association Response confirming 802.11r by mentioning domain and Fast BSS Transition (802.11r) parameters.

802.11k - Radio Measurement & Neighbor Reporting

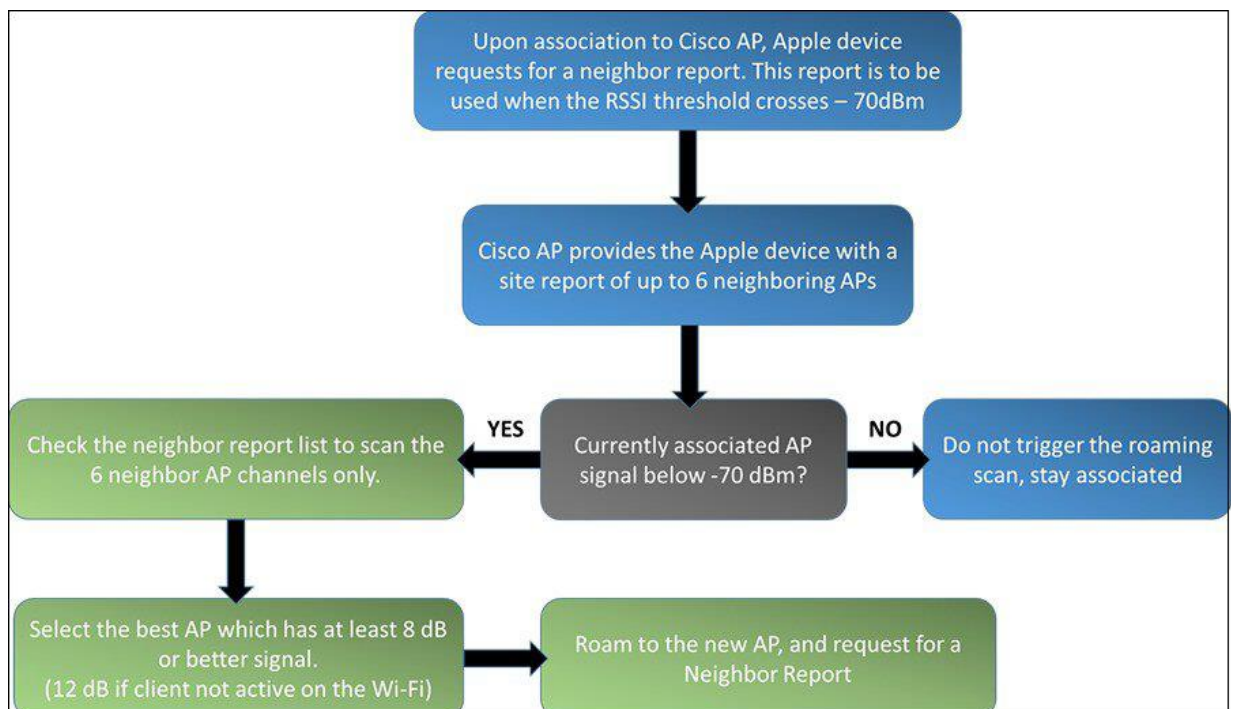
The 802.11k standard allows clients to request reports containing information about known neighbor APs that are candidates for roaming. The request is in the form of an 802.11 management frame known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with their Wi-Fi channel 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 it should roam to. This feature is especially useful from clients with high mobility and constrained battery resources, such as smartphones and tablets.

Although 802.11k support was officially introduced by Cisco in AireOS 7.4 and Apple in iOS 6, there were design changes that were implemented by Apple in iOS 8 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 or above updates for iOS devices. Mac computers do not support 802.11k, but associate transparently to networks where 802.11k is enabled. With AireOS 8.3 and up, enabling Cisco Fast lane on the WLAN network automatically enables 802.11k on the network SSID.

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 iOS 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 24. Neighbor Report processing flow for iOS devices supporting 802.11k (iOS 8 or later)



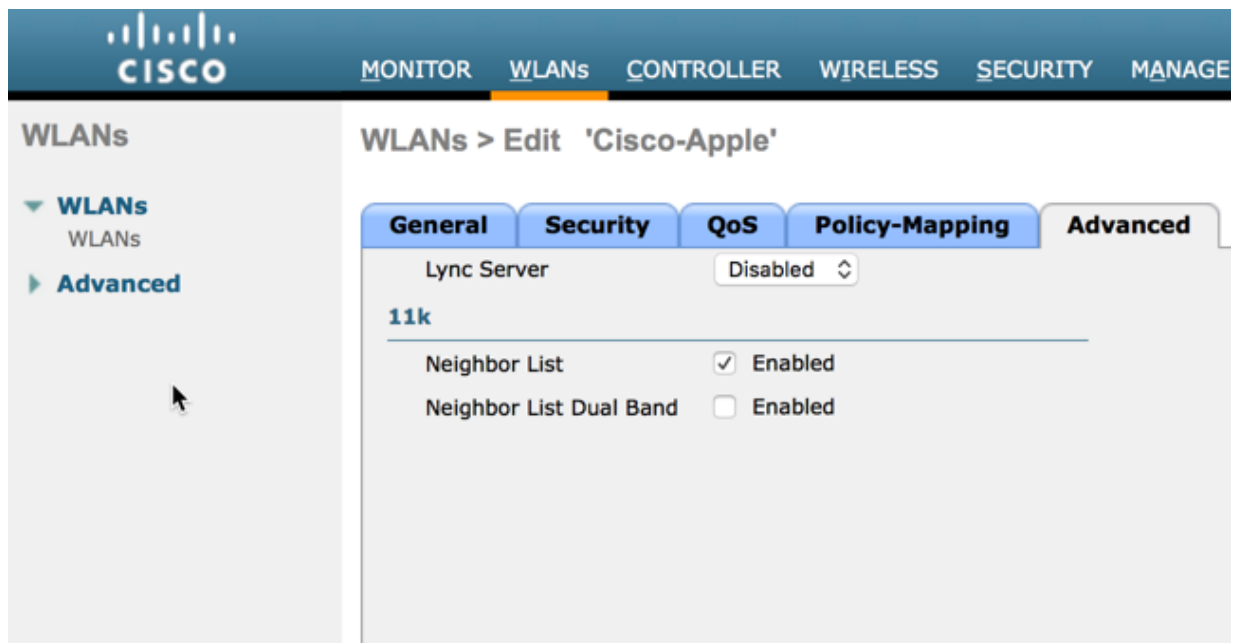
Note: Refer to Apple iPhone roaming behavior and optimization guide for more details:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/iPhone_roam/b_iPhone-roaming.html.

Using 802.11k to discovering and figuring out which AP should the device potentially roam (associate) to, is only part of the process - post this, iOS devices also needs to swiftly complete the authentication process, so the users experience minimal disruption in service. In this process, iOS devices authenticate 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 iOS 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 25. Enabling Neighbor Report on the WLAN



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. 802.11k is enabled by default in AireOS code release 8.3 and later.

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. This feature is especially useful from clients with high mobility, such as smartphones and tablets.

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

iOS 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 iOS 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. Mac computers do not support 802.11v, but associate transparently to networks where 802.11v is enabled.

Configuring 802.11v on Cisco Controller

Figure 26. 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.

Cisco Wi-Fi Analytics for iOS

802.11k and 802.11v aim at helping clients to determine the next best set of access points to roam to. The list of APs is determined by the WLAN controller for each AP, based AP-to-AP signals and clients roaming behaviors. However, inequalities in the transmit and receive chains in clients may make that the actual ordered list of best APs, from each client perspective and location, may be different from the calculated ordered list by the AP for that client. As a result, the AP may return to the client a list of APs that may not always fully align with the list of APs the client would compute by itself.

In order to avoid such misalignment, iOS devices running iOS 11 or later, connected to WLANs on WLAN controllers running AireOS 8.5 or later implement Cisco Wi-Fi Analytics for iOS. With this feature, iOS clients connecting to a new AP, or roaming to a new AP, send the list of APs that were detected just prior to association for the target WLAN. This communication takes the form of an unsolicited 802.11k beacon report action frame sent by the client just after association is completed. This feature is automatic and does not require any specific configuration. This list is visible in the WLAN controller interface for each client under Monitoring > Network Summary > Clients > Individual client.

The screenshot shows the Cisco 5500 Series Wireless Controller interface. The left sidebar contains navigation options: Monitoring, Network Summary, Access Points, Clients, Rogues, Access Points, Clients, Interferers, Wireless Dashboard, AP Performance, Client Performance, and Best Practices. The main content area is titled 'CLIENT VIEW' and shows details for a client named 'wifi-user' (Host Name: iPhoneSeven). The 'GENERAL' section includes fields for MAC Address (d4:51:9d:9a:af:e0), Uptime (Associated since 13 Minutes 12 Seconds), SSID (11radap1x), AP Name (bar_1 (Ch 36)), Nearest APs (calsica_1(-55 dBm), 3700(-65 dBm)), Device Type (iPhone 7), OS Version (11.0), Previous AP (58:ac:78:d4:29), Last disassociation reason (Proprietary failure), Performance (Signal Strength: -57 dBm, Signal Quality: 31 dB, Connection Speed: 360 Mbps, Channel Width: 40 MHz), Capabilities (802.11ac (5GHz) Spatial Stream: 2), Cisco Compatible (Not Supported), and Connection Score (85%). The 'CONNECTIVITY' section shows a flow diagram with steps: Start, Association, Authentication, DHCP, and Online. The 'TOP APPLICATIONS' section lists applications and their usage: ping (56.4 MB, 99.74%), apple-services (76.0 KB, 0.13%), icmp (27.8 KB, 0.05%), dns (27.5 KB, 0.05%), ntp (7.3 KB, 0.01%), all-web-services (5.7 KB, 0.01%), itunes (4.5 KB, 0.01%), and icloud (1.1 KB, 0%). The 'CLIENT SCAN REPORT' section shows a table of nearby APs:

Mac Address	RSSI	Channel
08:01:30:4a:51:e2	-63	38
58:ac:78:d4:29	-75	38
a0:ec:f9:5d:17:82	-80	38

The Cisco WLAN infrastructure uses this information to further optimize the list of AP returned to roaming clients at each location.

Additionally, connecting iOS 11 and later clients also specify their hardware model and software code release in an unsolicited action frame. This information is useful to contrast characteristics, and build a different list of APs based on the client type. This information is also useful for troubleshooting.

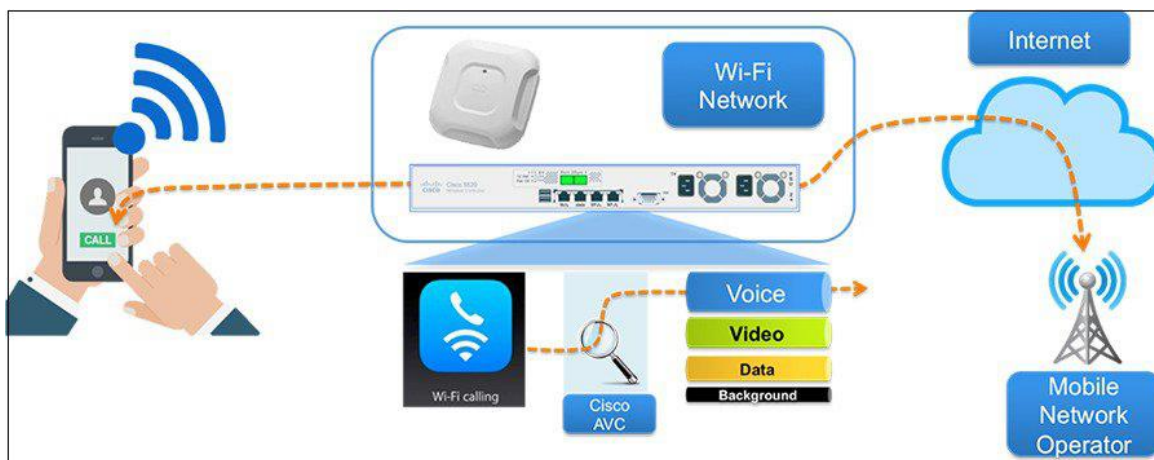
Also, supporting iOS 11 and later clients send a reason code upon deassociation. This reason code allows the infrastructure to understand the disconnections that are caused by RF issues, from deassociations caused by service issues (e.g. AAA session timeout or validation failure) or user actions (e.g. pressing Off button or disabling Wi-Fi). This information can be used to further optimize the list of access points returned to each client, and can also help network administrators troubleshoot disconnection issues. iPhones 7 and later, and iPad pro and later support iOS Analytics, when connecting to Cisco WLANs on AireOS 8.5 and later.

Wi-Fi Calling with iOS devices on Cisco WLAN

Apple introduced Wi-Fi Calling across multiple iPhone models (iPhone 5c or later) in September 2014 with its iOS 8 update, and has since been adding major network carriers who offer Wi-Fi calling service. With [iOS 9 update](#), more network carriers have been added to the list of carriers that support Wi-Fi calling. With extended Wi-Fi calling services, users can make Wi-Fi calls directly from another iOS device. An optimized wireless network has become important for Wi-Fi calling in an enterprise environment.

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 iPhone is sent within an Encapsulated Security Payload (ESP) in Voice priority (UP6). For iOS devices running iOS 10 or above, upstream Wi-Fi calling packets are also marked DSCP 46 (EF).

Figure 27. Optimizing Wi-Fi Calling over Cisco WLAN with Cisco AVC



In most service provider networks, 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.

In iOS 10 or later, when using QoS profiles, Wi-Fi calling is always whitelisted by default. You cannot send Wi-Fi calling to the best effort queue by merely omitting the app name from the whitelist. If your network configuration mandates that Wi-Fi calling should not be sent as voice traffic, you can push a QoS profile to iOS devices running iOS 10 with the `QoSMarkingAppleAudioVideoCalls` set to 0, so as to disable QoS for Wi-Fi calling. Doing so will also push Facetime to be sent as best effort. In most networks, Wi-Fi calling is considered as a valid voice application, and its marking is maintained.

There are several key design considerations to keep in mind when designing for Wi-Fi Calling including AP Cell Size, Data Rates, Deployment density, and Roaming enhancements (802.11r/k/v).

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>

Bonjour on Cisco WLAN

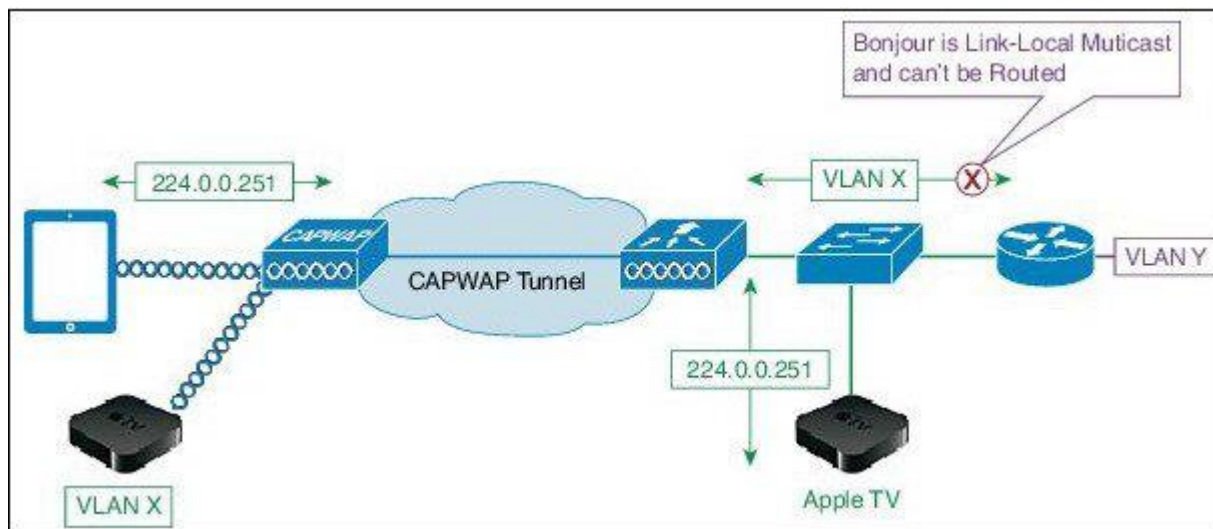
Bonjour is known as zero configuration networking, that locates devices such as printers, other computers, and the services that those devices offer on a local network using multicast Domain Name System (mDNS) service records.

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

- Printing services
- File sharing services
- Remote desktop services
- iTunes file sharing
- iTunes wireless iOS device syncing (in iOS v5 or later)
- AirPlay, which offers these streaming services:
 - Music broadcasting in iOS v4.2 or later
 - Video broadcasting in iOS v4.3 or later
 - Full screen mirroring in iOS v5 or later (iPad 2, 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 28. Bonjour services for Apple TV on Cisco WLAN



Note: Refer to Cisco v8.1 Bonjour Deployment Guide document for more details:

<https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/WLAN-Bonjour-DG/WLAN-Bonjour-DG.pdf>

Knowing your Wireless Environment

In addition to designing your Cisco WLAN around the best practices for iOS devices and Mac computers, network maintenance and monitoring helps to keep track of the overall network health. The application and roaming performance for iOS devices and Mac computers is 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.

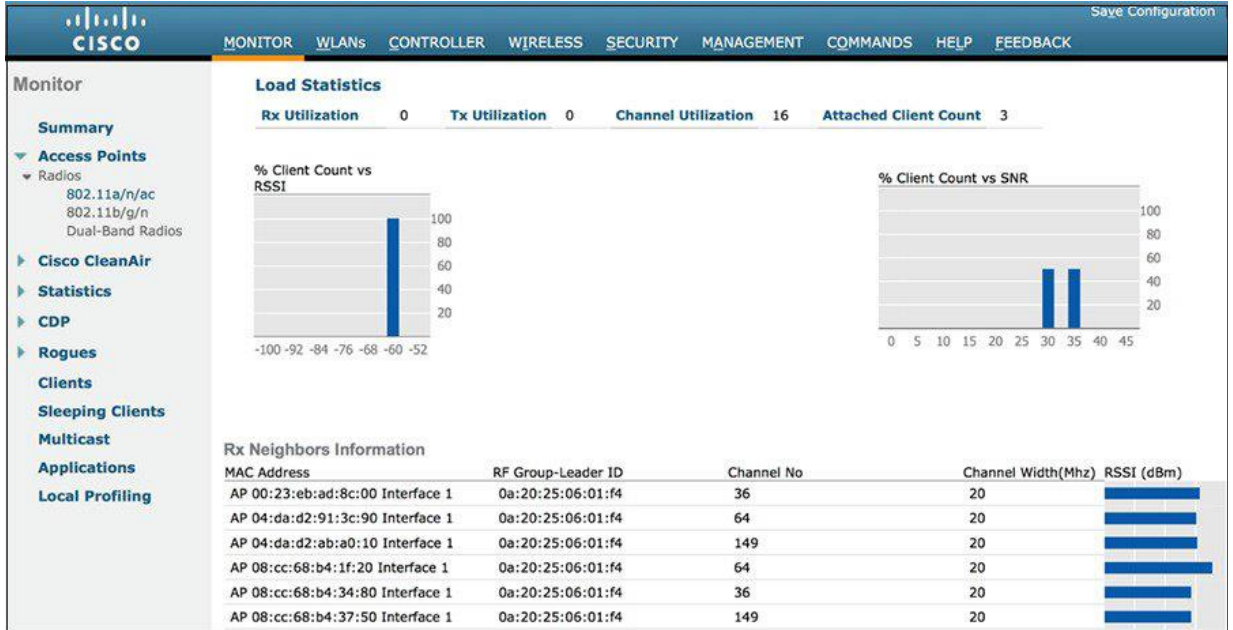
Figure 29. Checking AP Statistics to monitor the RF environment



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 iOS devices and Mac computers, and what data rates might be in actual use because of RSSI and SNR for the associated clients.

Figure 30. Monitoring for Client count against RSSI/SNR, and AP neighbors RSSI



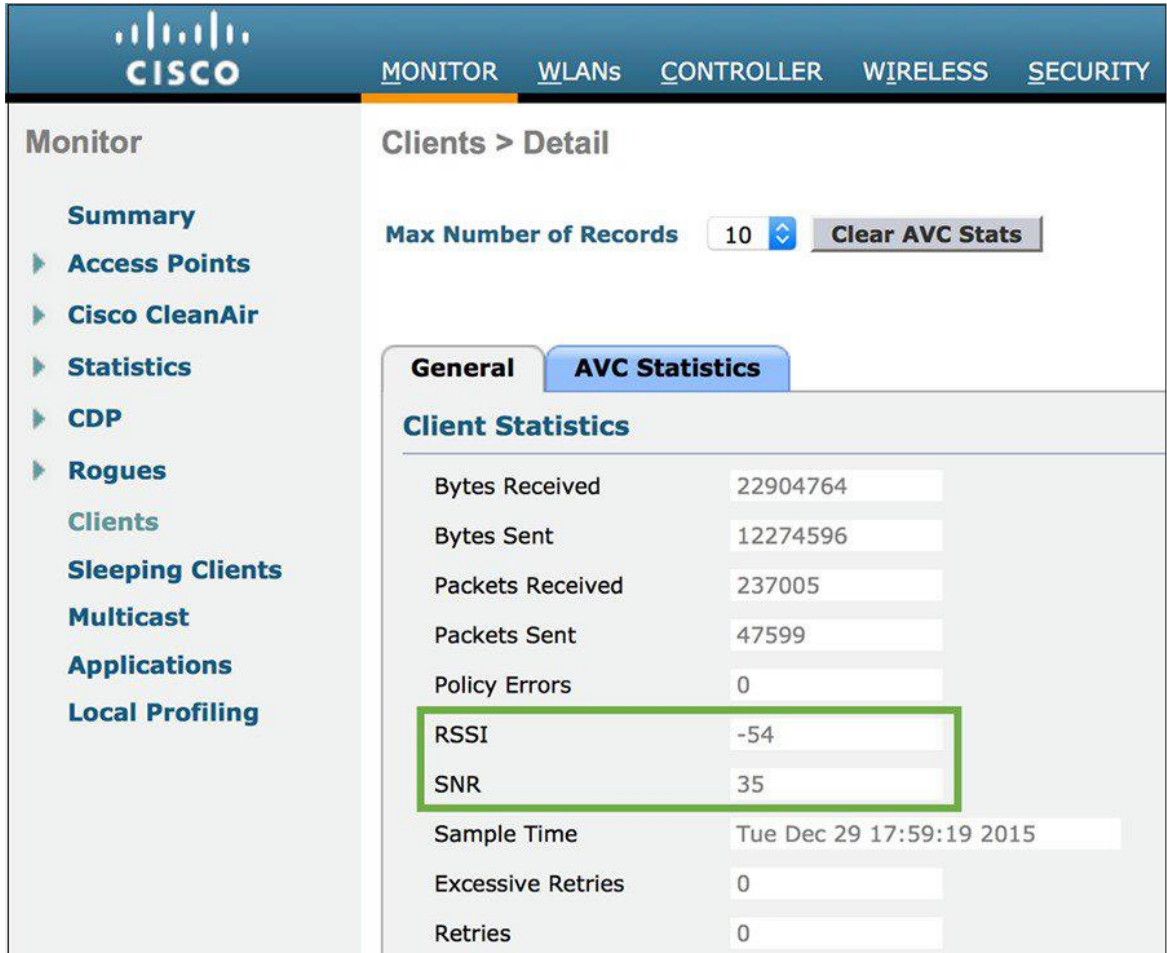
The information about the clients is the 'Rx Neighbors Information' can be used to get a quick understanding of how much coverage overlap there is between the APs that neighbor the AP with which iOS or Mac computers are associated.

Associated Device Monitoring

The next aspect of knowing the Wi-Fi environment is the connection status for iOS devices and Mac computers. 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 iOS device](#), tap on Settings 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 iOS 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. To determine the MAC address of a Mac computer, press the Option key while clicking the Wireless connection icon in the task bar. The MAC address is displayed just below the interface name, at the top of the popup window.

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 31. Monitoring Client RSSI and SNR statistics

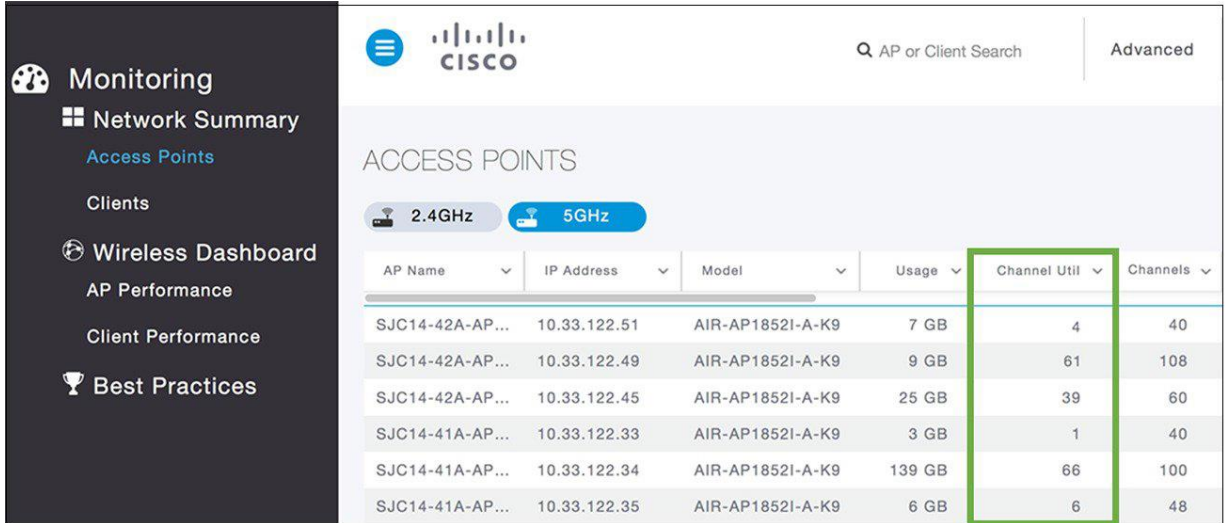


For example, an RSSI value of -45 dBm shows the AP can see the client at a stronger signal than a value of -67 dBm. The RSSI value is also important for knowing the coverage quality. If the value is too low, it could be an indication for poor connectivity. It is also an indicator of whether there is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

Channel Utilization

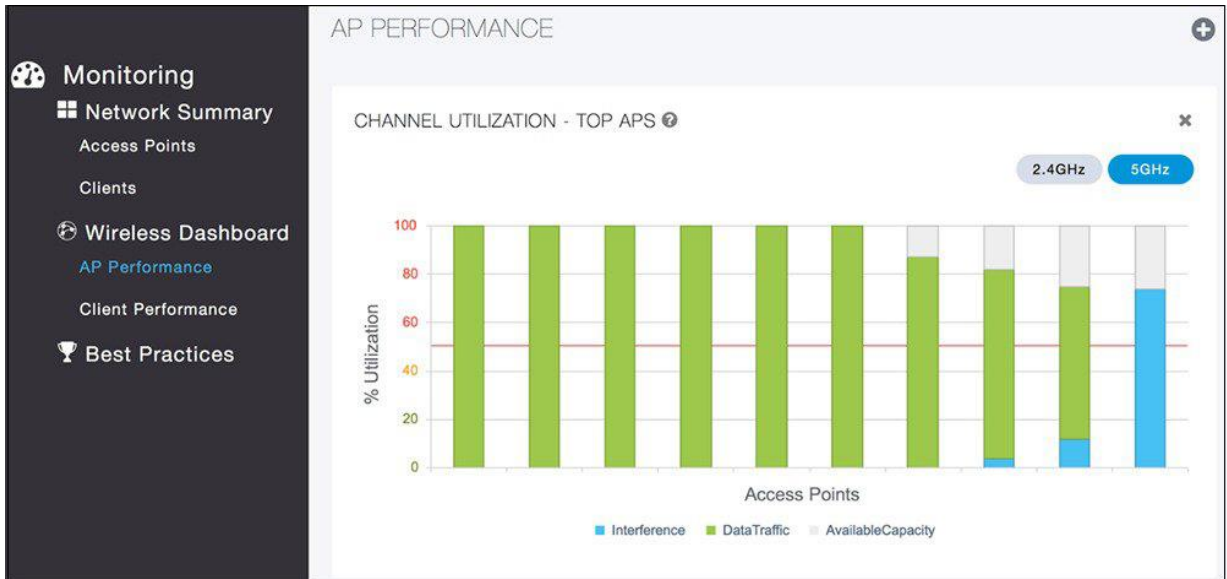
To compensate for the signal strength drop, as the phone moves away from an AP, the data rates shift down to a lower value. This helps to provide a more reliable packet delivery but reduces the throughput of the device and increases the air-time used by the device. More air-time consumed reduces the 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 iOS devices or Mac computers. The Wi-Fi channel is shared by the devices and the AP by way of their association.

Figure 32. 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 33. 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 iOS devices and Mac computers and their peer-to-peer behavior in your enterprise network. As of the third generation Rev.A of Apple TVs running Apple TV software version 7.0 or later, a new peer-to-peer methodology for AirPlay is introduced. Hereby [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 iOS 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 (BLE) 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 and AirPlay receiver). As such, this can also affect either channels 149+1, or 153-1 (Channels 36 and 44 in some countries) 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.

When a compatible iOS device or Mac computer has discovered a third generation Rev.A 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. Note that when using an Apple TV Rev.4 (2015), channels 149-161 can be used for the peer to peer communication. However, as with 802.11ac, channel width is dynamically determined per frame so channel width may be 40 MHz or even 20 MHz.

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 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 that is used to share content between iOS devices or Mac computers using peer to peer communication over Wi-Fi. 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 iOS devices or Mac computers are expected to use continuous peer-to-peer connections on a daily basis, a potential solution would 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.

Apple Watch is another portable device that 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 primary mode of connectivity is Bluetooth to transfer data back and forth between Apple

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 watchOS 2 update, Apple Watch can also use Tetherless Wi-Fi to connect to the Internet independently. It means that even without the iPhone, the Apple Watch will be able to connect to the Wi-Fi network. Since Apple Watch is 2.4 GHz only, there should not be any impact on the 5 GHz networks even if more than one Apple Watch is communicating with the Wi-Fi network.

iOS devices and Mac computers on Cisco WLAN Best Practices Summary

Recommendations for iOS devices and Mac computers on Cisco WLAN are summarized as follows:

- Cisco recommends a 5 GHz only network and coverage design for all iOS devices and Mac computers. 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 that all iOS devices and Mac computers 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. In networks with a large proportion of recent iOS clients and some non-802.11r clients, Adaptive 11r may provide similar performances while ensuring better compatibility between iOS and non-802.11r clients.
- For high density enterprise environments, Cisco and Apple recommend to use 802.11r with Over the air transition for optimal 11r-FT performance. For environments with large cells, 802.11r with Over the DS may reduce the number of packets dropped by clients at the edge of the cell.
- Cisco recommends configuring 802.11r adaptive mode for controllers running AireOS 8.3 or later.
- Cisco recommends configuring 802.11k on the WLAN to provide iOS devices with a neighbor list response. Cisco v8.0MR3 and v8.1.120.0 and iOS 8 is the minimum version recommended for 802.11k.
- Cisco and Apple recommend the use of 802.11v BSS Transition Management to help balance iOS 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 iOS devices and Mac computers on Cisco Wireless LAN. If the 5GHz coverage is marginal, set 6 Mbps as the lowest mandatory rate, and make sure that 12 and 24Mbps are enabled as well.
 - Cisco highly recommends leaving all MCS (802.11n and 802.11ac) rates enabled.
 - Cisco recommends that at all times an Apple device observes a minimum of 2 APs with an RSSI measurement of -67 dBm or better. Mac computers can also perform optimally when observing a minimum of 2 APs with an RSSI measurement of -72 dBm or better.
 - Cisco recommends monitoring for peer-to-peer communication activity on UNII-3 band channels in a high client density environment. If high number of iOS devices or Mac computers 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 Apple devices to most recent version of iOS and macOS.
 - 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

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

Cisco App Visibility and Control (AVC) Q & A

http://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/qa_c67-722538.html

Configuring App 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 Deployment Reference

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

Voice Over IP (VoIP) Best Practices Guide for iOS

<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

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

CXX-XXXXXX-XX 10/11