



Optimized WiFi Connectivity and Prioritized Business Apps

Table of Contents

| | |
|--------------------------------|----------|
| Introduction..... | 3 |
| Requirements | 3 |
| Components Used..... | 3 |
| Conventions..... | 3 |
| Adaptive 11r | 4 |
| Configurations Steps | 4 |
| Debug Commands..... | 8 |
| SNMP | 8 |
| Always on 11k and 11v..... | 9 |
| Prioritized Business Apps..... | 11 |
| Feature Overview | 11 |
| Configurations Steps | 12 |
| Debug Commands..... | 19 |
| SNMP | 19 |

Introduction

802.11r enabled WLAN provides faster roaming for wireless client devices. It is desired that iOS devices running iOS 10 will be able to join a WLAN with 11r enabled for better roaming experience. However, if 11r is enabled on a WLAN, the legacy devices that do not recognize the FT AKM's beacons and probe responses will not be able to join the WLAN. We need a way to identify the Client device capability and allow 11r capable device to join on the WLAN as an FT enabled device and at the same time to allow legacy device to join as an 11i/WPA2 device. Cisco WLC Software release 8.3 will enable 802.11r on an 802.11i-enabled WLAN selectively for iOS devices¹. The capable iOS devices will identify this functionality and perform an FT Association on the WLAN. The Cisco Wireless infrastructure will allow FT association on the WLAN from devices that can negotiate FT association on a non-FT WLAN.

In addition, with WLC running AireOS 8.3, 802.11k and 11v features are enabled by default on an SSID. These features help clients roam better by telling them when to roam and providing them with information about neighboring APs so that no time is wasted scanning when roaming is needed. Since iOS devices support dual-band, the 802.11k neighbor list is updated on dual-band, adaptively for iOS devices.

Apple iOS device mark QoS as per IETF recommendations. With WLC running AireOS 8.3, you can enable the Fastlane feature, which enables several beneficial functions:

- Your WLC QoS configuration is optimized globally to better support real-time applications
- iOS 10 devices can send upstream voice traffic without the requirement to perform WMM TSPEC/TCLAS negotiation. The infrastructure will honor the voice marking for these devices.
- You can apply a QoS profile to your iOS 10 devices, and decide which applications should receive QoS marking upstream, and which applications should be sent as best effort or background.

Requirements

WLC running AireOS 8.3 and higher, devices running iOS 10 and higher.

Components Used

The information in this document was created from tests in a specific lab environment. All the devices used to create this document started with a cleared (default) configuration. It is recommended to test these features in a test environment, if your network is live, make sure that you understand the potential impact of any command.

Conventions

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

¹iOS devices supporting the Optimized WiFi Connectivity solution are
iPhone 6s and later
iPhone 6s Plus and later
iPad Pro and later
iPhone SE

Adaptive 11r

On the Cisco Infrastructure side, Cisco AP will advertise the support for adaptive 802.11r in beacons and probes, and FT over the DS capability will be set.

On the client side, devices running iOS 10 or higher will look for the adaptive 11r feature support in the IE. If the capability bit is set, it will look for AKM (dot1x or PSK) and use FT dot1x or FT PSK respectively. The Apple device will send IE with FT support in its association request and also include the Vendor specific OUI.

Cisco WLAN will process the association request and respond with 802.11r support in association response, allowing FT association. The 4-Way handshake will involve FT Association.

This feature is supported on Local mode as well as FlexConnect mode APs, for all 802.11n and 802.11ac wave 1 APs controlled by a WLC running AireOS release 8.3².

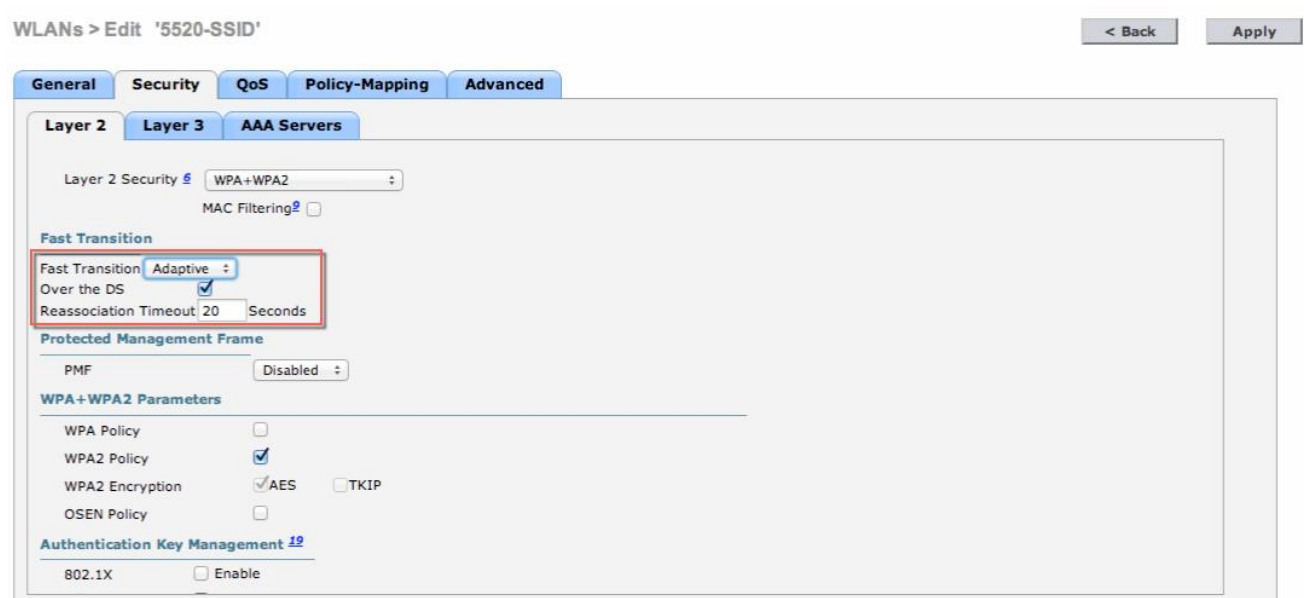
Legacy devices that do not recognize the FT AKM's beacons and probe responses will not be able to join the WLAN. We need a way to identify the Client device capability and allow 11r capable device to join on the WLAN as an FT enabled device and at the same time to allow legacy device to join as an 11i/WPA2 device. Cisco WLC Software release 8.3 will enable 802.11r on an 802.11i-enabled WLAN selectively for Apple devices¹. The capable Apple devices will identify this functionality and perform an FT Association on the WLAN.

Configurations Steps

1. Create a new WLAN (SSID) with PSK Layer 2 authentication (802.1x is also supported). The Adaptive 11r Feature is enabled by default. Over the DS is selected by default and re-association timeout is set to 20 seconds.

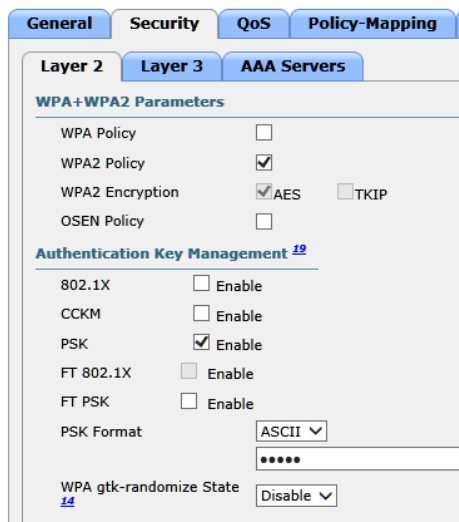
Note: When upgrading from a previous release, the Adaptive 11r feature will be disabled by default for an existing WLAN.

² AP1600/2600 Series Access Points, AP1700/2700 Series Access Points, AP3500 Series Access Points, AP3600 Series Access Points + 11ac Module, WSM, Hyperlocation module, 3602P, AP3700 Series Access Points + WSM, 3702P, OEAP600 Series OfficeExtend Access Points, AP700 Series Access Points, AP700W Series Access Points, AP1530 Series Access Points, AP1550 Series Access Points, AP1570 Series Access Points, and AP1040/1140/1260 Series Access Points.



This can be changed using the GUI or the CLI command:

- config wlan security ft adaptive enable/disable
2. Enable AKM as 802.1x or PSK instead of FT 802.1x or FT PSK.



3. Enable the WLAN and associate three different clients to the SSID
 - iPad and iPhone devices running iOS 10 or higher
 - iPad and iPhone devices running iOS 9 or lower
 - Non-iOS device
4. Verify that
 - iPad or iPhone running iOS 10 or higher associates as a 11r client

- iPad or iPhone running iOS 9 or lower associates as a regular 802.11i client
- Non-Apple device associates as a regular 802.11i client

5. Verify that

- iPad or iPhone running iOS 10 or higher fast roams to a new AP
- iPad or iPhone running iOS 9 or lower slow roams to a new AP

Max Number of Records: 10 | Clear AVC Stats

General | **AVC Statistics**

Client Properties

MAC Address: 40:33:1a:cc:17:c8
 IPv4 Address: 10.10.10.110
 IPv6 Address: fe80::75:47d1:b779:3815

Client Type: Simple IP
 User Name: [redacted]
 Port Number: 8
 Interface: management
 VLAN ID: 10
 Quarantine VLAN ID: 0
 CCX Version: Not Supported
 E2E Version: Not Supported
 Mobility Role: Local
 Mobility Peer IP Address: N/A
 Mobility Move Count: 0
 Policy Manager State: RUN
 Management Frame Protection: No
 UpTime (Sec): 179
 Current TxRateSet: m15
 Data RateSet: 1,0,2,0,5,5,11,0,6,0,9,0,12,0,18,0,24,0,36,0,48,0,54,0
 KTS CAC Capability: No
 802.11u: Not Supported
 802.11v BSS Transition: Supported

AP Properties

AP Address: 3c:08:f6:b2:e5:40
 AP Name: AP3702-SujRt
 AP Type: 802.11bn
 AP radio slot Id: 0
 WLAN Profile: ODDMZ-PSK
 WLAN SSID: ODDMZ-PSK
 Status: Associated
 Association ID: 1
 802.11 Authentication: Open System
 Reason Code: 1
 Status Code: 0
 CF Pollable: Not Implemented
 CF Poll Request: Not Implemented
 Short Preamble: Implemented
 PBCC: Not Implemented
 Channel Agility: Not Implemented
 Timeout: 0
 WEP State: WEP Enable

Lync Properties

Lync State: Disabled
 Audio Qos Policy: Silver
 Video Qos Policy: Silver
 App-Share Qos Policy: Silver
 File Transfer Qos Policy: Silver

Running Lync Calls

Call Type: [redacted] | Call Id: [redacted]

PMIP Properties

Mobility type: Simple

Allowed (URL)IP address

Security Information

Security Policy Completed: Yes
 Policy Type: RSN (WPA2)
 Auth Key Mgmt: FT-PSK
 Encryption Cipher: CCMP (AES)

Max Number of Records: 10 | Clear AVC Stats

General | **AVC Statistics**

Client Properties

MAC Address: 74:e1:b6:b7:6d:22
 IPv4 Address: 10.10.10.107
 IPv6 Address: fe80::1c95:e73f:519:2ab2

Client Type: Simple IP
 User Name: [redacted]
 Port Number: 8
 Interface: management
 VLAN ID: 10
 Quarantine VLAN ID: 0
 CCX Version: Not Supported
 E2E Version: Not Supported
 Mobility Role: Local
 Mobility Peer IP Address: N/A
 Mobility Move Count: 0
 Policy Manager State: RUN
 Management Frame Protection: No
 UpTime (Sec): 56392
 Current TxRateSet: m7
 Data RateSet: 18,0,24,0,36,0,48,0,54,0
 KTS CAC Capability: No
 802.11u: Not Supported
 802.11v BSS Transition: Not Supported

AP Properties

AP Address: fd:7f:06:4d:c5:70
 AP Name: AP2700
 AP Type: 802.11an
 AP radio slot Id: 1
 WLAN Profile: ODDMZ-PSK
 WLAN SSID: ODDMZ-PSK
 Status: Associated
 Association ID: 2
 802.11 Authentication: Open System
 Reason Code: 1
 Status Code: 0
 CF Pollable: Not Implemented
 CF Poll Request: Not Implemented
 Short Preamble: Not Implemented
 PBCC: Not Implemented
 Channel Agility: Not Implemented
 Timeout: 0
 WEP State: WEP Enable

Lync Properties

Lync State: Disabled
 Audio Qos Policy: Silver
 Video Qos Policy: Silver
 App-Share Qos Policy: Silver
 File Transfer Qos Policy: Silver

Running Lync Calls

Call Type: [redacted] | Call Id: [redacted]

PMIP Properties

Mobility type: Simple

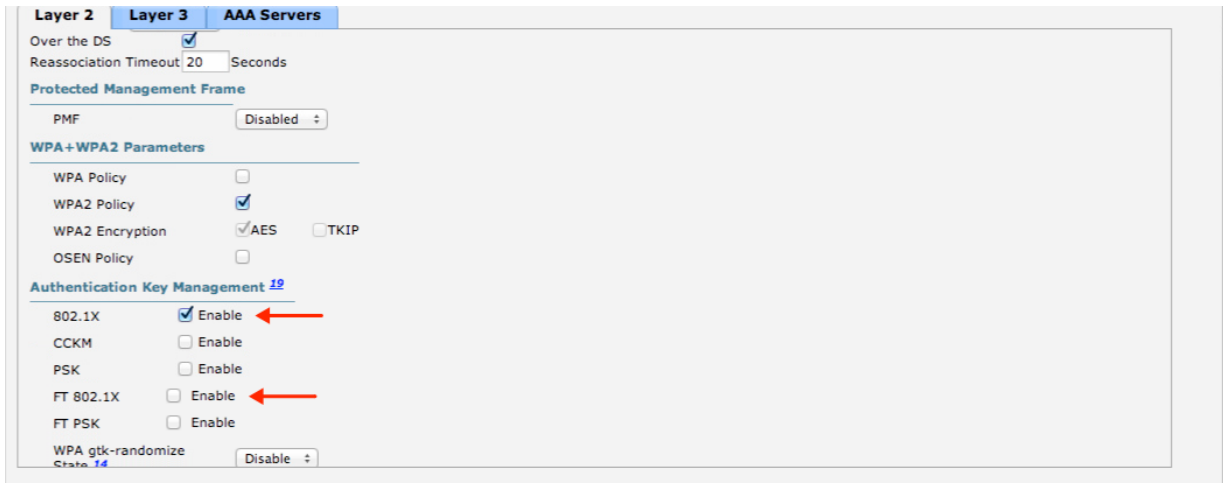
Allowed (URL)IP address

Security Information

Security Policy Completed: Yes
 Policy Type: RSN (WPA2)
 Auth Key Mgmt: PSK
 Encryption Cipher: CCMP (AES)
 EAP Type: N/A

Additional Guidelines for Configuration

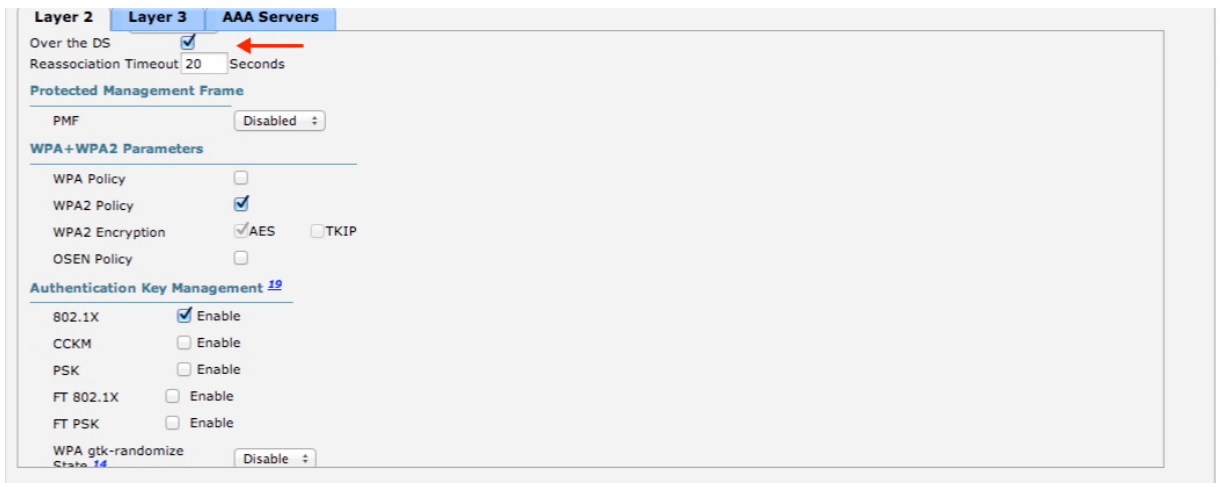
1. Configure 802.1x or PSK as AKM instead of the FT variants



CLI Commands:

- config wlan security wpa akm 802.1x enable
- Or
- config wlan security wpa akm psk enable

2. Enable/Disable FT over the ds and set re-assoc timeout, if required



CLI Commands:

- config wlan security ft over-the-ds enable/disable
- config wlan security ft reassociation-timeout

Debug Commands

The following commands can be used to debug this feature:

- debug client <client-mac>
- debug snmp mib enable

SNMP

cLWSecDot11EssFtMode entry in the parent MIB CLWSecDot11EssCckmEntry returns the state of 11r on the WLAN as shown below:

| k_cLWSecDot11EssCckmEntry_get | Returns | Reason |
|-------------------------------|----------|----------------------------------|
| | 0 | 11r disabled/WLAN does not exist |
| | 1 | 11r mode enabled |
| | 2 | 11r mode adaptive |

Always on 11k and 11v

With release 8.3, 802.11k and 11v features are enabled by default on an SSID. These features help clients roam better by telling them when to roam and providing them with information about neighboring APs so that no time is wasted scanning when roaming is needed.

802.11k Assisted Roaming

802.11k allows 11k capable clients to request a neighbor report containing information about known neighbor APs that are candidates for roaming.

To facilitate roaming, an 11k capable client associated with an AP sends a request for a list of neighbor APs. The request is in the form of an 802.11 management frame known as an action 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. From the response frame the client knows which APs are candidates for the next roam. The use of 802.11k radio resource management (RRM) processes allows the client to roam efficiently and quickly.

With the neighbor list information, the 11k capable client does not need to probe all of the 2.4 GHz and 5 GHz channels to find an AP it can roam to. Not having to probe all of the channels reduces channel utilization on all channels, thereby increasing bandwidth on all channels. It also reduces roam times and improves the decisions made by the client. Additionally, it increases battery life of the device because it is neither changing the radio configuration for each channel nor sending probe requests on each channel.

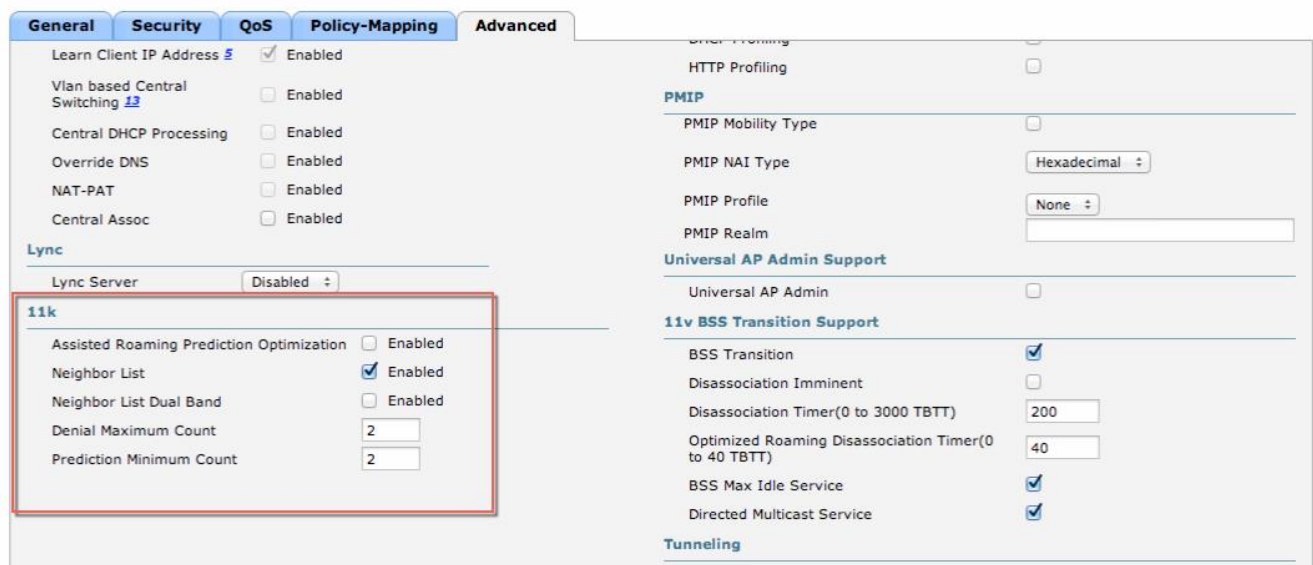
It avoids the device having to process all of the probe response frames.

Step 1 : Click WLANs.

Step 2 : Choose WLAN ID > Edit page.

Step 3 : Click Advanced tab.

Step 4 : In the 11k area, the feature is enabled by default on a newly created SSID



The screenshot shows the 'Advanced' configuration tab for a WLAN. The '11k' section is highlighted with a red box and contains the following settings:

| Setting | Value |
|--|---|
| Assisted Roaming Prediction Optimization | <input type="checkbox"/> Enabled |
| Neighbor List | <input checked="" type="checkbox"/> Enabled |
| Neighbor List Dual Band | <input type="checkbox"/> Enabled |
| Denial Maximum Count | 2 |
| Prediction Minimum Count | 2 |

The '11v BSS Transition Support' section contains the following settings:

| Setting | Value |
|--|-------------------------------------|
| BSS Transition | <input checked="" type="checkbox"/> |
| Disassociation Imminent | <input type="checkbox"/> |
| Disassociation Timer(0 to 3000 TBTT) | 200 |
| Optimized Roaming Disassociation Timer(0 to 40 TBTT) | 40 |
| BSS Max Idle Service | <input checked="" type="checkbox"/> |
| Directed Multicast Service | <input checked="" type="checkbox"/> |

The Neighbor List Dual Band configuration is not enabled in the configuration as shown above but for Apple devices that negotiate adaptive capability with Cisco WLAN Infrastructure, the Dual band neighbor list is selectively enabled to allow the clients to leverage the benefit of both bands.

Managing 802.11v BSS Transition

802.11v BSS Transition is applied to the following three scenarios:

Solicited request—Client can send an 802.11v BSS Transition Management Query before roaming for a better option of AP to re-associate with a client.

Unsolicited Load Balancing request—If an AP is heavily loaded, it sends out an 802.11v BSS Transition Management Request to an associated client.

Unsolicited Optimized Roaming request—If a client's RSSI and rate do not meet the requirement, AP sends out an 802.11v BSS Transition Management Request to this client.

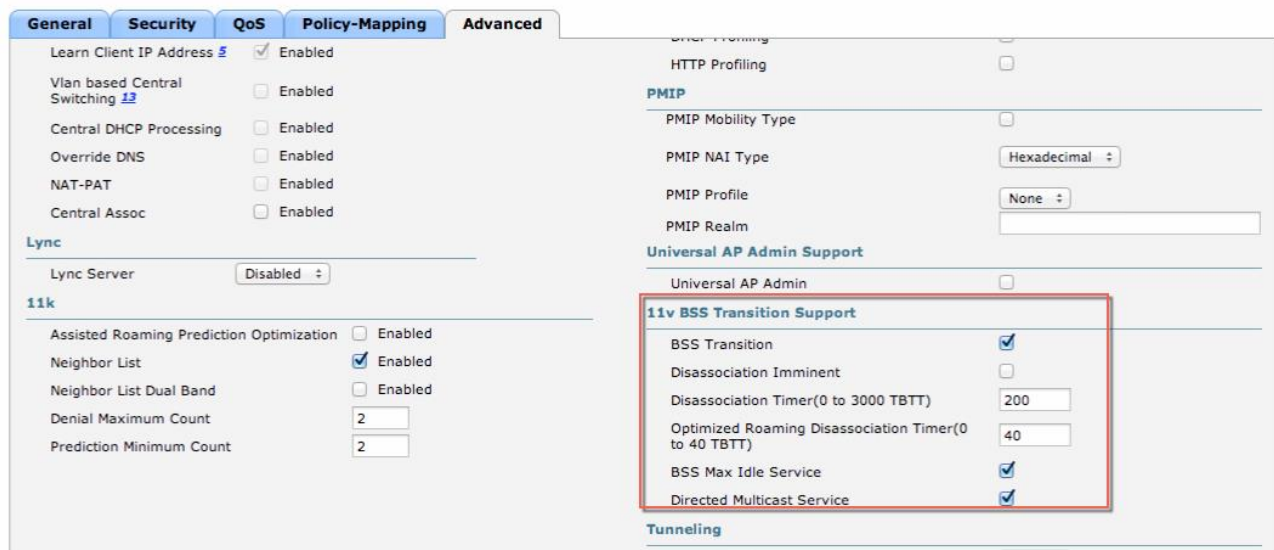
802.11v BSS Transition Management Request is a suggestion given to client. Client can make its own decision whether to follow the suggestion or not. To force disassociating a client, you can turn on the disassociation-imminent function. This function is to disassociate the client after a period of time if the client does not re-associate to another AP.

Step 1 : Click WLANs.

Step 2 : Choose WLAN ID > Edit page.

Step 3 : Click Advanced tab.

Step 4 : In the 11v BSS Transition Support section, the feature is enabled by default on a newly created SSID as shown below:



The screenshot shows the 'Advanced' configuration tab for a WLAN. The '11v BSS Transition Support' section is highlighted with a red box. The configuration for this section is as follows:

| Feature | Configuration |
|--|---|
| BSS Transition | <input checked="" type="checkbox"/> Enabled |
| Disassociation Imminent | <input type="checkbox"/> Disabled |
| Disassociation Timer(0 to 3000 TBTT) | 200 |
| Optimized Roaming Disassociation Timer(0 to 40 TBTT) | 40 |
| BSS Max Idle Service | <input checked="" type="checkbox"/> Enabled |
| Directed Multicast Service | <input checked="" type="checkbox"/> Enabled |

Prioritized Business Apps

QoS is a key component of traffic transmission efficiency in congested environments. QoS allows applications to be marked to reflect their importance for the business operations. In a wired infrastructure, this marking can be used to set different priority levels based on the marking value, and also perform operations of bandwidth allocation and control, based on the application category or marking. In a wireless environment, marking is also used to associate applications to one of the 8 User Priority queues. Association to a queue is also used to differentiate the statistical frequency at which an application accesses the wireless medium. Proper marking at the infrastructure level results in optimized downstream traffic, where applications of higher business relevance can receive a statistical transmission advantage, and real-time applications can be prioritized over non-interactive applications. The same effect is applicable upstream when the client station marks QoS properly.

iOS devices mark QoS as per IETF recommendations. With WLC running AireOS 8.3, you can enable the Fastlane feature, which enables several beneficial functions:

- Your WLC QoS configuration is optimized globally to better support real-time applications
- Your devices running iOS 10 can send upstream voice traffic without the requirement to perform WMM TSPEC/TCLAS negotiation. The infrastructure will honor the voice marking for these devices.
- You can apply a QoS profile to your iOS 10 devices, and decide which applications should receive QoS marking upstream, and which applications should be sent as best effort or background.

Feature Overview

On the Cisco Infrastructure side, Cisco AP will advertise the support for Fastlane as soon as the feature is enabled on the target WLAN.

On the client side, iOS devices running iOS 10 or higher will look for Fastlane support in AP management frames. The iOS 10 device will also mark its support for Fastlane in upstream frames.

When Fastlane is enabled on a first WLAN, the controller is automatically configured for optimal QoS support for Wi-Fi devices. In particular, the global Platinum profile is configured to allow traffic up to Voice, and sets the Unicast Default Priority and the Multicast Default Priority parameters to Best Effort. Per user UDP bandwidth contracts are disabled on that profile, along with 802.1p. The Platinum profile is then attached to the target WLAN. Wireless CAC (ACM) and Expedited Bandwidth are enabled for the Voice queue for both bands, and the maximum voice bandwidth is set to 50%. A DSCP-to-UP and UP-to-DSCP customized map is configured to map the values recommended by the IETF RFC 4594³ and draft-szigetti-ieee-802-11-01⁴. DSCP is trusted for upstream traffic. An AutoQoS profile is created, that applies the recommended marking to the most common 32 well-known applications that typically require differentiated QoS treatment. When Application Visibility is enabled on the target WLAN, this Auto-QoS profile is automatically applied. iOS 10 devices can receive a QoS profile (provisioned using standard Apple profile provisioning techniques). This QoS profile lists the applications that can be put in a whitelist. Applications in a whitelist are authorized to apply upstream QoS marking using Apple Service Type method. Applications that are not in the Whitelist do not mark upstream QoS in a Fastlane enabled network. By default, all applications are whitelisted (i.e.

³ <https://tools.ietf.org/html/rfc4594>

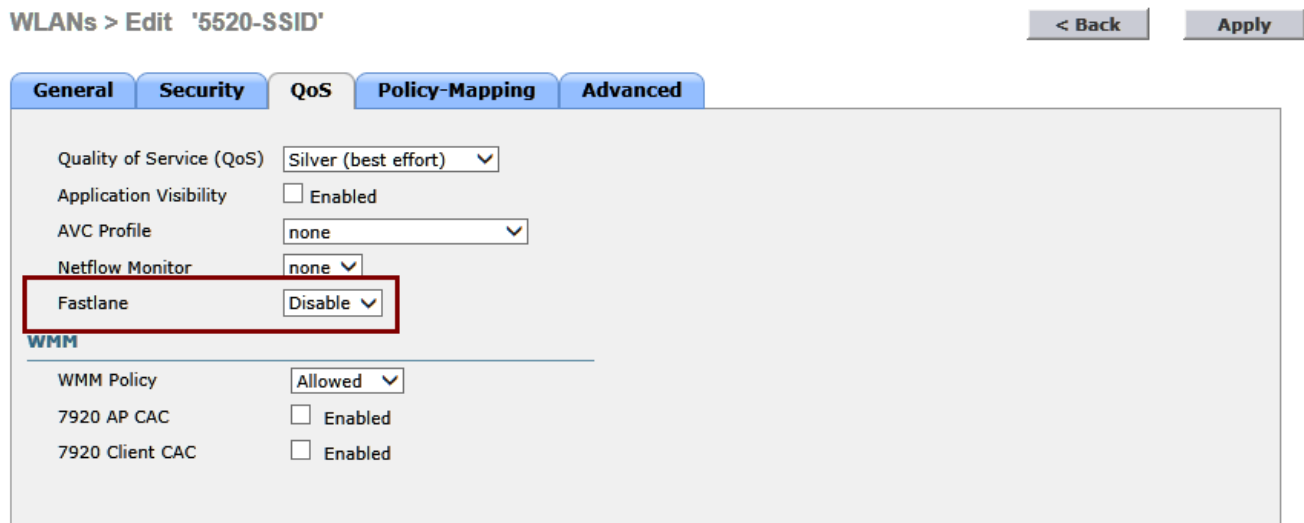
⁴ <https://tools.ietf.org/html/draft-szigeti-tsvwg-ieee-802-11-02>

without a QoS whitelist, all applications can mark QoS; when a whitelist is deployed, only applications in the whitelist will mark QoS using the Service_Type method, other applications will receive best effort or background QoS treatment). When supporting iOS 10 devices, associate to a WLAN that is configured for Fastlane, they apply the QoS profile they previously received. The AP also trusts the iOS QoS marking. In particular, traffic marked as Voice is trusted even if the client does not perform admission control (ADDTs).

This feature is supported on Local mode as well as FlexConnect mode APs, for all 802.11n and 802.11ac wave 1 APs controlled by a WLC running AireOS release 8.3⁵.

Configurations Steps

1. Create a new WLAN. Fastlane is not enabled by default.



This can be changed using the GUI or the CLI command:

- `config qos Fastlane enable/disable wlan <wlan id>`

A warning message will show, expressing that enabling Fastlane on a WLAN will make global changes, and therefore will temporarily disable both bands (both bands are re-enabled automatically as the command completes).

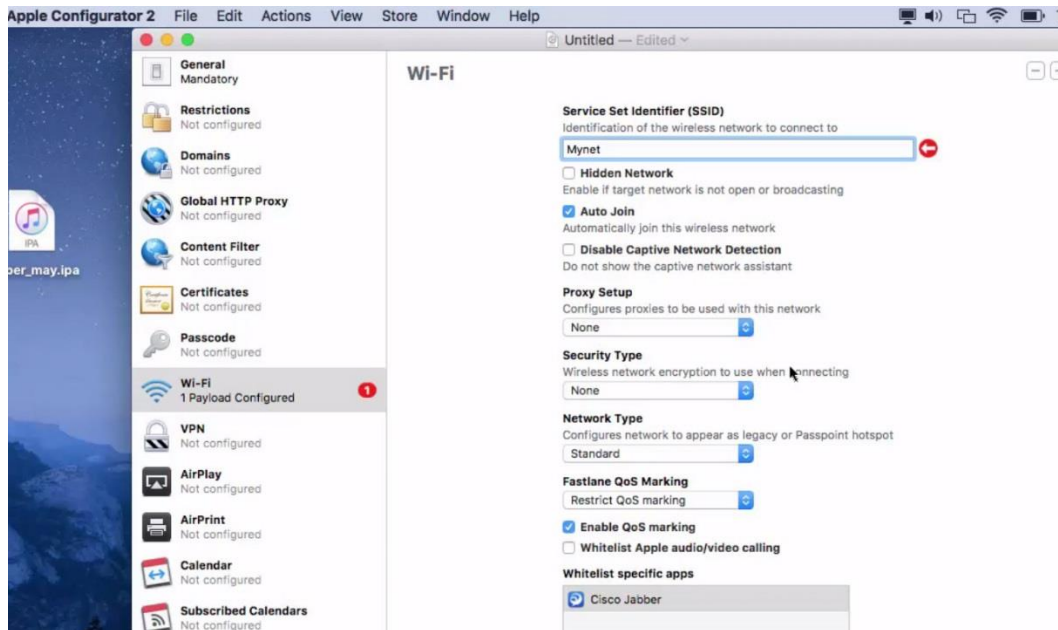
2. Verify that:
 - Fastlane is enabled in the WLAN QoS tab.
 - The WLAN QoS profile is now set to Platinum.

⁵ AP1600/2600 Series Access Points, AP1700/2700 Series Access Points, AP3500 Series Access Points, AP3600 Series Access Points + 11ac Module, WSM, Hyperlocation module, 3602P, AP3700 Series Access Points + WSM, 3702P, OEAP600 Series OfficeExtend Access Points, AP700 Series Access Points, AP700W Series Access Points, AP1530 Series Access Points, AP1550 Series Access Points, AP1570 Series Access Points, and AP1040/1140/1260 Series Access Points.

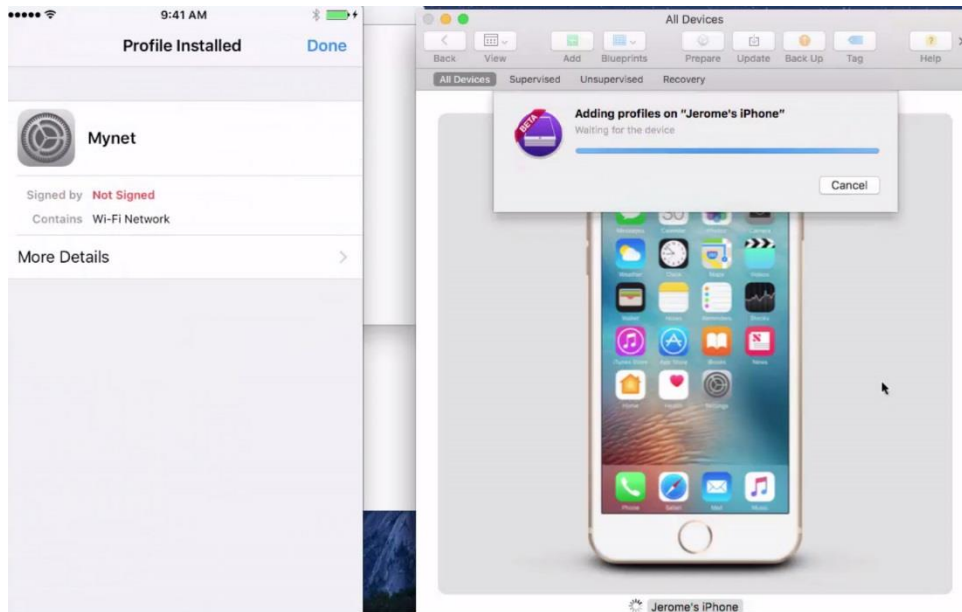
- In Wireless > QoS > Profiles > Platinum, Unicast Default Priority and Multicast Default Priority are set to Best Effort. Wired QoS protocol is set to None.
 - In Wireless > QoS > QoS Map, QoS map is enabled, along with Trust DSCP Upstream. The QoS map creates 19 exceptions to map well-known DSCP values to the value recommended by the IETF. All other DSCP values are mapped to the general UP matching their 3 MSB.
 - In Wireless > 802.11a/n/ac > Media, Call Admission Control is now enabled, with 50% max RF bandwidth allocated to Voice traffic. The same setting is visible in the Wireless > 802.11b/g/n > Media page.
 - In Wireless > 802.11a/n/ac > EDCA Parameters, the EDCA Profile is now Fastlane. The same setting is visible in the Wireless > 802.11b/g/n > EDCA Parameters page.
3. Enable the WLAN and associate three different clients to the SSID
 - iPad and iPhone devices running iOS 10 or higher, with or without a profile listing whitelisted apps.
 - iPad and iPhone devices running iOS 9 or lower
 - non-iOS devices
 4. Verify that
 - iPad and iPhone devices running iOS 10 or higher associate as Fastlane clients
 - iPad and iPhone devices running iOS 9 or lower associate as regular clients
 - Non-iOS devices associate as regular clients

CLI Command:

- Show client details <mac address>
.../..
Fastlane Client: Yes
5. Optionally, create a QoS profile using Apple configurator or your MDM software and deploy it to the iOS 10 client. The QoS profile needs to match the target SSID name. For example, you can use Apple Configurator 2.3 or later to create a profile on MacOS. In the Wi-Fi section of the profile, you can configure the target SSID and choose which apps should be whitelisted. The example below creates a profile for the Mynet SSID, whitelists Cisco Jabber (Jabber will mark QoS). As Apple Audio and Video Calling is disabled, Wi-Fi calling and Facetime will not mark QoS (disabling Apple Audio and Video Calling is not recommended practice, but an example for the purpose of this guide):



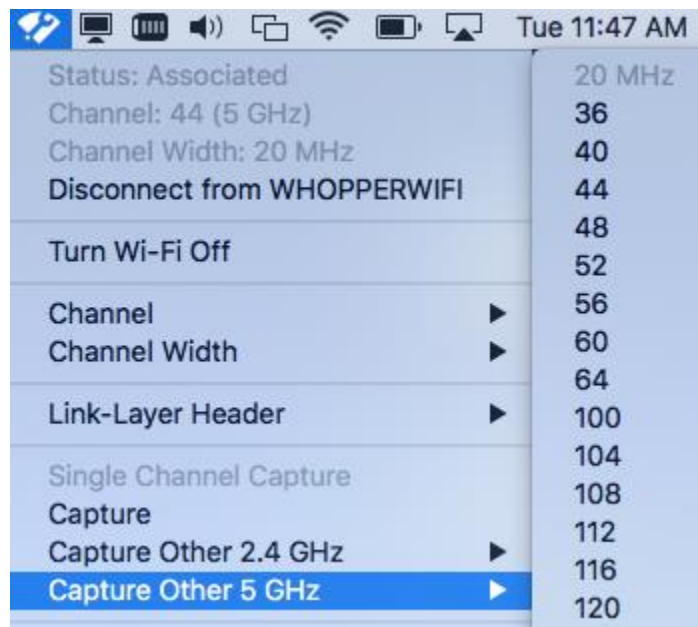
Once created, the profile can be pushed to the iOS 10 device through Apple Configurator.



- Once the iOS device is provisioned with the QoS profile, associate the iOS 10 device to the target SSID. Launch the whitelisted application (Jabber in this example), then an application that is not in the whitelist (Facetime in this example) .

7. Verify that

- iPad and iPhone device running iOS 10 or higher mark QoS for applications in the whitelist, and send traffic for applications outside of the whitelist as best effort or background
- iPad and iPhone device running iOS 10 or higher, marking upstream traffic DSCP 46/UP6, receive downstream traffic also marked DSCP46/UP6, even if ACM is enabled and the iOS 10 client did not request a level of service through TSPEC/ADDTS.
- iPad and iPhone device running iOS 9 or lower may mark upstream traffic. However, returning traffic for the Voice queue will be sent as best effort, following the WMM specification.
- Non-iOS device may mark upstream traffic. However, returning traffic for the Voice queue will be sent as best effort, following the WMM specification, unless the non-iOS device performed an initial ADDTS request that was accepted.
- Regardless of their upstream marking, well-known applications such as Jabber receive the correct (as recommended by RFC 4594 and draft-szigetti-ieee-802-11-01) downstream marking, if Application and Visibility is enabled on the WLAN.
- These verifications are best conducted by capturing the WLAN channel traffic. On a MacOS laptop, you can use a combination of Wireshark to capture frames, and Airtool to configure the channel to capture:



In the capture, verify that the application in the whitelist gets the expected QoS marking. In this example, Jabber Audio receives DSCP EF and UP 6⁶:

⁶ Applications need to be updated for iOS 10 and natively mark QoS for marking to be visible. Please verify with your app provider which version should be used in order for the app to use iOS 10 Service_Type and display QoS marking in iOS 10.

| | | | | | | |
|------|-----------|-------------------|-----------------------|--------|-----|--------|
| 1639 | 13.198813 | 172.31.255.128 | 172.29.129.137 | RTP | 183 | 0x0006 |
| 1640 | 13.198886 | | Apple_1e:d4:b9 (5c... | 802.11 | 39 | |
| 1641 | 13.198965 | 172.31.255.128 | 172.29.129.137 | RTCP | 147 | 0x0000 |
| 1642 | 13.199036 | | Apple_1e:d4:b9 (5c... | 802.11 | 39 | |
| 1643 | 13.202159 | CiscoInc_db:df:7a | Broadcast | 802.11 | 246 | |
| 1644 | 13.212367 | 172.31.255.128 | 172.29.129.137 | RTP | 183 | 0x0006 |
| 1645 | 13.212442 | | Apple_1e:d4:b9 (5c... | 802.11 | 39 | |
| 1646 | 13.231941 | 172.31.255.128 | 172.29.129.137 | RTP | 183 | 0x0006 |
| 1647 | 13.232014 | | Apple_1e:d4:b9 (5c... | 802.11 | 39 | |
| 1648 | 13.241307 | 172.29.129.137 | 172.31.255.128 | RTP | 183 | 0x0006 |

```

Frame 1639: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 QoS Data, Flags: .....TC
Logical-Link Control
Internet Protocol Version 4, Src: 172.31.255.128, Dst: 172.29.129.137
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    
```

In this example, Facetime is not on the whitelist and sends traffic as best effort:

| | | | | | | |
|------|-----------|----------------|----------------|-----|-----|--------|
| 5712 | 32.356395 | 172.31.255.128 | 172.29.129.137 | UDP | 301 | 0x0000 |
|------|-----------|----------------|----------------|-----|-----|--------|

```

Receiver address: CiscoInc_db:ce:fc (a8:0c:0d:db:ce:fc)
Destination address: CiscoInc_b8:dd:c3 (24:b6:57:b8:dd:c3)
Transmitter address: Apple_1e:d4:b9 (5c:ad:cf:1e:d4:b9)
Source address: Apple_1e:d4:b9 (5c:ad:cf:1e:d4:b9)
BSS Id: CiscoInc_db:ce:fc (a8:0c:0d:db:ce:fc)
STA address: Apple_1e:d4:b9 (5c:ad:cf:1e:d4:b9)
.... .... 0000 = Fragment number: 0
1101 0001 1010 .... = Sequence number: 3354
▶ Frame check sequence: 0xe6ef930e [correct]
▶ Qos Control: 0x0000
▶ Logical-Link Control
▼ Internet Protocol Version 4, Src: 172.31.255.128, Dst: 172.29.129.137
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    
```

Additional Guidelines for Configuration

1. Application Visibility is an optional element of Fastlane configuration. You can enable Fastlane on a WLAN without enabling Application Visibility.

WLANs > Edit '5520-SSID'

< Back

Apply

General **Security** **QoS** **Policy-Mapping** **Advanced**

Quality of Service (QoS)

Application Visibility Enabled

AVC Profile

Netflow Monitor

Fastlane

WMM

WMM Policy

7920 AP CAC Enabled

7920 Client CAC Enabled

When Application Visibility is enabled on a Fastlane WLAN, the recommended Auto-QoS-AVC Profile is applied to the WLAN. You cannot apply another AVC profile, unless you choose to also disable Fastlane.

WLANs > Edit '5520-SSID'

< Back

Apply

General **Security** **QoS** **Policy-Mapping** **Advanced**

Quality of Service (QoS)

Application Visibility Enabled

AVC Profile

Netflow Monitor

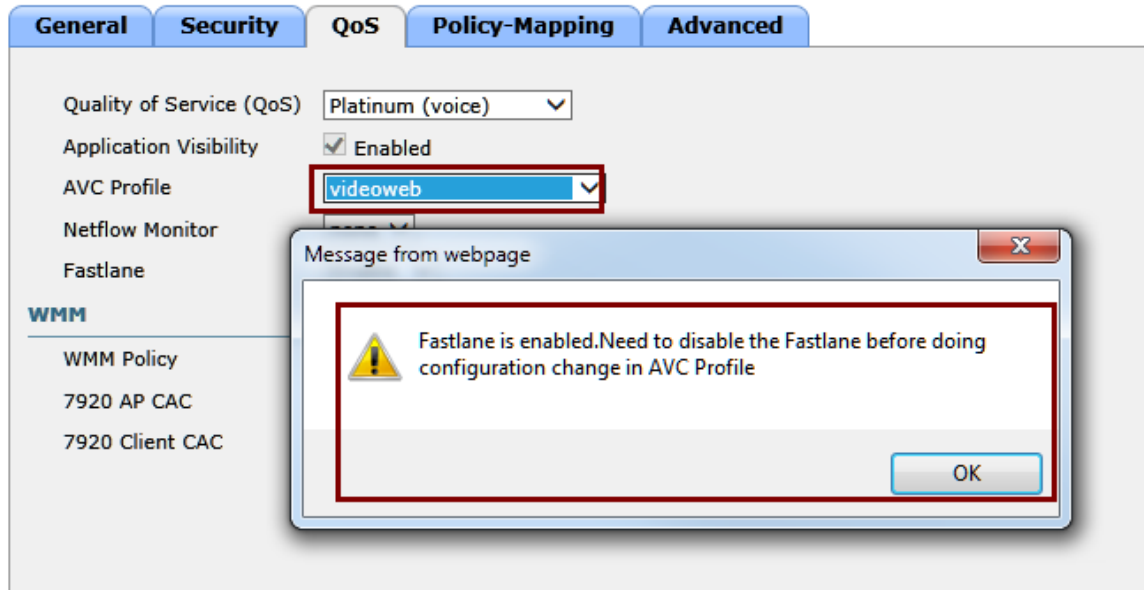
Fastlane

WMM

WMM Policy

7920 AP CAC Enabled

7920 Client CAC Enabled



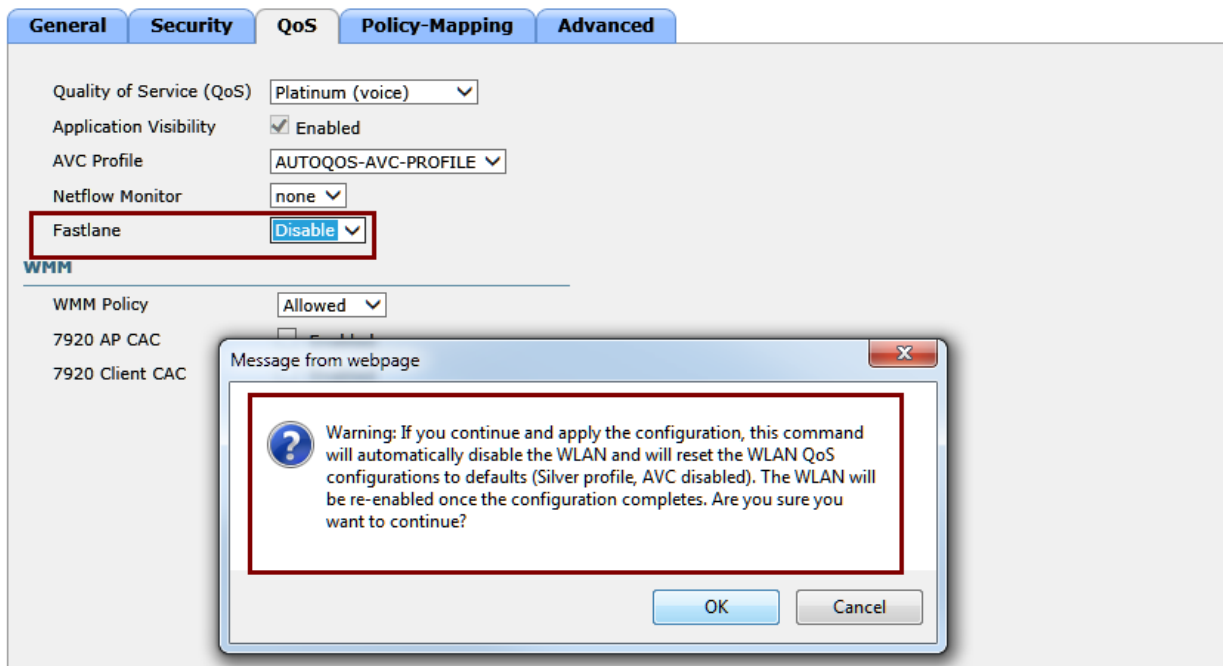
CLI Command:

- `config wlan avc <wlan id> visibility enable`

2. You can disable Fastlane for individual WLANs. The WLAN QoS policy will be returned to Silver (default), and Application Visibility will be reset to its defaults (disabled). Once the command completes, you can edit the WLAN and manually change the associated QoS profile and enabled Application Visibility if needed:

WLANs > Edit '5520-SSID'

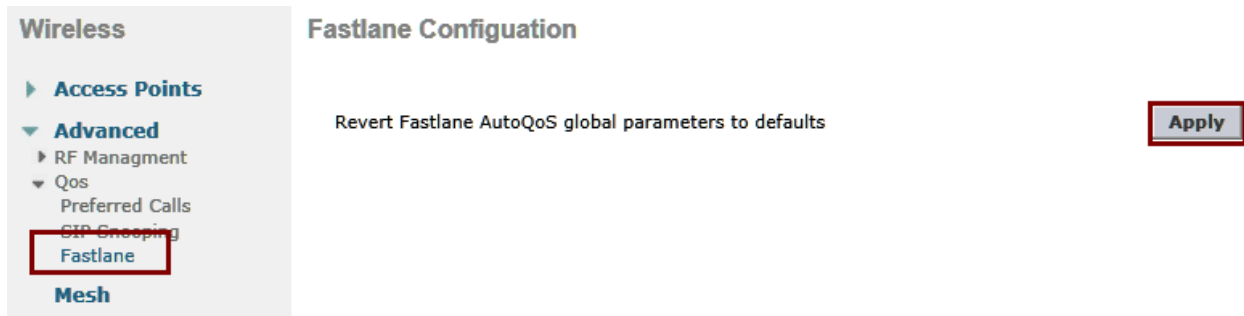
< Back Apply



CLI Command:

- Config qos Fastlane disable wlan <wlan id>

3. Once Fastlane has been disabled on all WLANs, you can also revert the WLC global QoS configuration to its defaults. To do so, use the Fastlane global configuration page. Fastlane cannot be disabled globally if a WLAN still has Fastlane enabled. When Fastlane is disabled globally, the Platinum QoS profile is reset to defaults (Maximum Priority stays to Voice, but Unicast Default Priority and Multicast Default Priority are reset to Voice). Wireless CAC (ACM) is disabled for Voice, and the associated maximum bandwidth is returned to its default, 75%. QoS maps are disabled and upstream QoS uses UP instead of DSCP.



CLI Command:

- Config qos Fastlane disable global

Note: Although you need to disable Fastlane globally to return the WLC global QoS configuration to its defaults, you do not need to enable Fastlane globally. Enabling Fastlane on a first WLAN also enables Fastlane global parameters.

Debug Commands

The following commands can be used to debug this feature.

- debug client <client-mac>
- debug snmp mib enable

SNMP

cLQoSFastlaneDisable entry returns the global state of Fastlane as shown below:

| cLQoSFastlaneDisable_get | Returns | Reason |
|--------------------------|----------|---------------------|
| | 0 | Reserved |
| | 1 | Disabled |
| | 2 | No operation |



cLWlanQosFastlane entry returns the state of Fastlane for an individual WLAN as shown below:

| cLWlanQosFastlane_get | Returns | Reason |
|-----------------------|--------------|--------------------------|
| | True | Fastlane enabled |
| | False | Fastlane disabled |