

CISCO VALIDATED DESIGN

Adopting Fast Lane in Clinical Communications— Mobile Heartbeat

June 2017

Table of Contents

| | |
|--|-----------|
| Introduction | 1 |
| Fast Lane Overview | 1 |
| Understanding the Fast Lane Components..... | 2 |
| Fast Lane Observations – Mobile Heartbeat | 5 |
| Mobile Heartbeat–Fast Lane | 10 |
| Fast Lane Deployment Details..... | 12 |
| Verifying That Components Are Fast Lane – Ready..... | 12 |
| Configuring Mobility Device Manager..... | 15 |
| Verifying End-to-End QoS | 17 |
| Verifying That Fast lane Is Operational | 19 |
| Appendix A: Product List..... | 24 |
| Appendix B: Changes | 25 |

Introduction

Optimizing the caregiver experience for healthcare organizations who are adopting clinical communication system is a complex task. Together, Apple, Cisco and Mobile Heartbeat™ have proven a number of benefits of a new technology called Fast lane. When a Cisco Fast lane enabled wireless network detects an Apple iOS 10+ device running a Fast lane enabled application such the MH-CURE™ application from Mobile Heartbeat, beautiful things can happen, and clinical teams notice.

For the first time, a truly end-to-end quality of service (QoS) policy can be implemented across a network, inclusive of the Apple iOS operating system, MH-CURE and across the wireless network. With this new capability, applications that your health care delivery organization identifies by as business critical can specify what level of service their application should receive.

Perhaps you are thinking that you have heard about QoS and are already receiving the benefits. With the onsite validation that Apple, Cisco, and Mobile Heartbeat recently conducted, there are considerable advantages for the clinical mobility user when Fast lane is enabled.

This guide serves a number of purposes related to Fast lane and Mobile Heartbeat. First, it describes the advantages seen during our joint testing and translates how those advantages result in a significantly improved end-user experience and clinical benefits. Second, it provides technical details around the results obtained during the joint Apple, Cisco, and Mobile Heartbeat testing. Lastly, it provides implementation details so that your healthcare delivery organization can improve their clinical communication end user experience.

FAST LANE OVERVIEW

Prioritizing mission-critical applications such as clinical communication based systems can be controlled through the use of a whitelist policy that is pushed down to the Apple iPhone or iPad through the use of a Mobility Device Manager (MDM). Applications that are Fast lane enabled and are explicitly named in the whitelist receive priority treatment in a truly end-to-end fashion. This prioritization is unique to Cisco and Apple and extends the priority and optimization within the Apple iOS and across the Cisco wireless and switched network.

When Apple introduced iOS 10, it enabled a series of QoS based queues that application developers can use to prioritize traffic as it passes down the stack and eventually reaches the wireless network adapter. These nine queues take into account the data types and priorities necessary to enable an optimized end-user experience. Voice traffic for example is typically composed of many relatively small packets that require extremely low latency. High-priority service of data that has been placed into the voice priority queue is critical to reducing latency and in passing them to the network PHY layer.

To achieve this granularity, iOS 10 introduced a highly optimized QoS architecture that can optimize the end-user experience for Fast lane enabled applications. Prior to this, tagged application traffic was mostly serviced with equal priority. This means large file transfers received the same priority as voice traffic. In a mobile device with constrained resources such as packet buffers or the congested wireless network to which it is attached, preservation of priority queuing is top-of-mind, and addressed by Fast lane.

UNDERSTANDING THE FAST LANE COMPONENTS

A few technology-based components need to be in place in order to implement Fast lane. This section examines each of these, starting at the Apple iOS mobile device and working towards the Healthcare Delivery Organization (HDO) datacenter.

Apple iOS Mobile Device

Fast lane is supported starting with release 10 of Apple iOS. Apple devices that support version 10 or higher support Fast lane. Advances in antenna design as well as Wi-Fi chip sets do favor the newer models of iPhones such as the iPhone 7 followed by the 6S and so on. The Apple SE (non-cellular) mobile device was included in the validation efforts that produced this design. Although not generally recommended for clinical environments, the device did provide support for Fast lane but did exhibit a relatively low end user experience, primarily due to the factors outlined above.

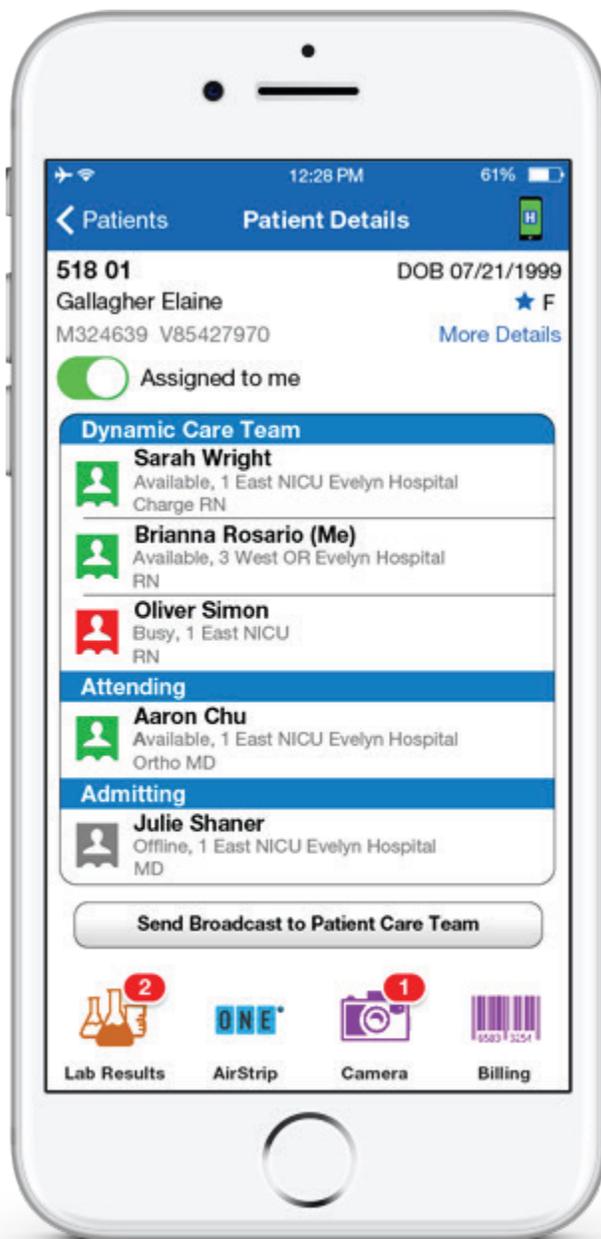
MH-CURE—Mobile Heartbeat

Often the most overlooked component is the mobile clinical communication application itself. Mobile Heartbeat worked with Apple and Cisco to implement Fast lane within their MH-CURE mobile application. This effort allowed the prioritization of voice traffic for their application to receive higher priority than any other application running at the same time.

In networks where contention for resources of any kind occur, a QoS policy allows the network infrastructure to provide priority treatment for such traffic. Other applications running at the same time on the same mobile device can be de-prioritized in the event that the healthcare delivery organization determines that they are not business critical. This decision overrides any marking that those applications may make by default.



Figure 1 Mobile Heartbeat–MH-CURE application



Cisco Digital Healthcare Architecture

Cisco Digital Healthcare Architecture (DHA) is a set of healthcare-specific best practices that—when applied to campus, wireless, data center, Internet edge, collaboration, segmentation and security technologies—enable the HDOs ability to deploy solutions (for example, clinical communications) that advance the delivery of care with digital solutions.

By implementing a network infrastructure that complies with the best practices found in DHA, HDOs are assured of an optimized caregiver experience. This often results in quicker clinical adoption and adoption during the rollout phase of clinical communication systems. As those who have participated in rollout projects that involve implementing new technology to care teams, all aspects that eliminate poor acceptance must be implemented to ensure adoption.

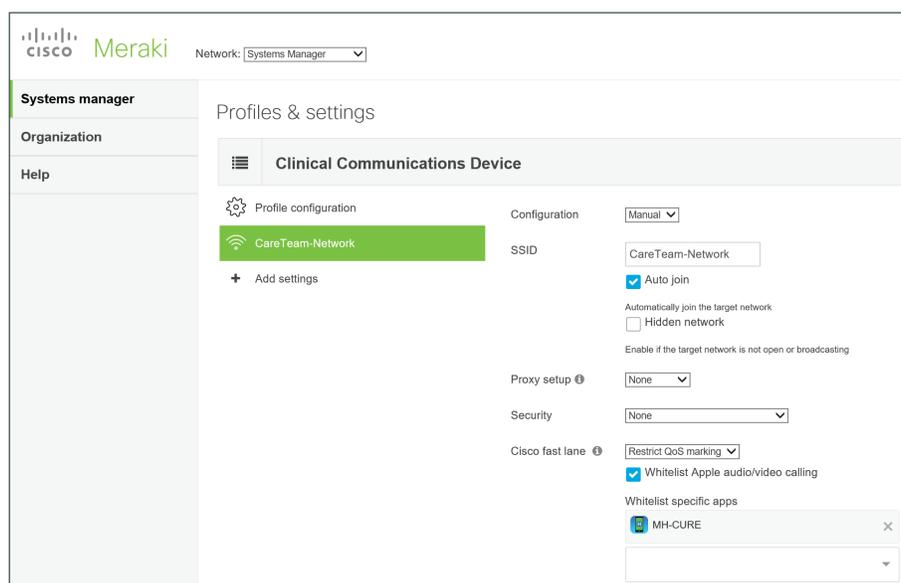
The benefits of using Fast lane and Cisco DHA not only provide optimized voice quality in the case of Mobile Heartbeat but also have other benefits. This includes improved battery performance due to the significant reduction in the retransmissions of traffic in a heavily congested cell (See Fast lane Observations – Mobile Heartbeat). In addition, significant improvements in audio quality are realized due to optimized roaming between access points (APs), a meaningful benefit for caregivers who rely on critical communication to deliver reliable quality care.

Mobility Device Manager

Rolling out hundreds if not thousands of mobile devices across your healthcare organization is no easy task. One such component that both streamlines and enhances the security and now performance of business-critical applications is the mobility device manager. This management software allows network administrators to deliver a consistent policy to the Apple iOS device that is being enrolled on your network.

During validation, the Meraki MDM was used to push a series of policies to the Apple iOS device. These policies included items such as which wireless network the device is allowed to connect to, as well as one other that is key: for the first time, the network administrator can identify which applications on the Apple iOS device should receive priority service. The whitelist contains a list of applications that if Fast lane enabled will receive end-to-end priority treatment on the network.

Figure 2 Meraki Mobility Device Manager—whitelist profile



By default, all Fast lane enabled applications in the absence of a whitelist receive priority treatment as identified within the Fast lane enabled mobile application. Once the HDO (Healthcare Delivery Organization) pushes a Wi-Fi profile that contains a Fast lane based whitelist, only those applications contained within the whitelist will receive priority service. All applications not in the whitelist will have their traffic reclassified as “Best Effort” or Background.

On the surface, this may not be inspiring, but for healthcare delivery organizations – this represents the first time that the network administrator can control which applications on the Apple mobile device are business critical to their organization.

FAST LANE OBSERVATIONS – MOBILE HEARTBEAT

This section discusses the tests that were performed in the Cisco RF Validation lab. Statistical analysis was performed on the RF packet captures on each of the access points within the lab. The findings about the improvements that Fast lane enables are based on this analysis.

Testing Strategy

The strategy was to baseline the wireless network with Fast lane enabled, during active calls when one of the iPhone users was mobile. This test consisted of walking a predefined loop while introducing audio on both mobile handsets. Roaming occurred between 3 APs along the path while a fourth AP was available in an 802.11k neighbor list. This AP (AP29) was strategically placed so that it would appear in the neighbor list, but was not an optimal roaming candidate.

Figure 3 Cisco RF validation lab—testing loop



Real-time interactive voice traffic has a unique characteristic: because it is real-time, the sampled audio stream is digitized and a data packet is transmitted every 20 ms (.02 seconds). This works out to a steady packet flow of 50 packets per second. This makes it easy to see the before and after effects of Fast lane. Any delays or retransmissions in transmitting these packets on timed bases are easy to spot by using statistical analysis and inspection.

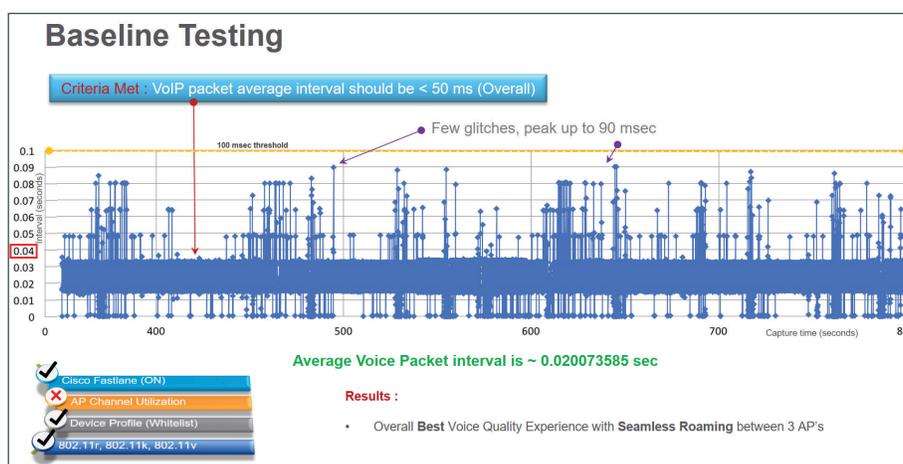
Baseline

The first step of the testing was to capture a baseline with Fast lane enabled, the MH-CURE application whitelisted, roaming optimizations of 802.11r/k/v enabled and near zero channel utilization.

In Figure 4, it is clear that almost all traffic is transmitted well under the 20 ms objective. There are a few spikes, but generally speaking, the voice stream was not delayed while being transmitted from the iPhone in the “Up” direction towards the access point. This is an ideal situation because reliance on the jitter buffer or codec concealment mechanisms do not really come into play.

Also, note that there are no indications of long roam times, dead air, or such when roaming between the access points (AP1, AP21, AP10) while traversing the test loop, as shown in Figure 3.

Figure 4 Mobile Heartbeat baseline testing

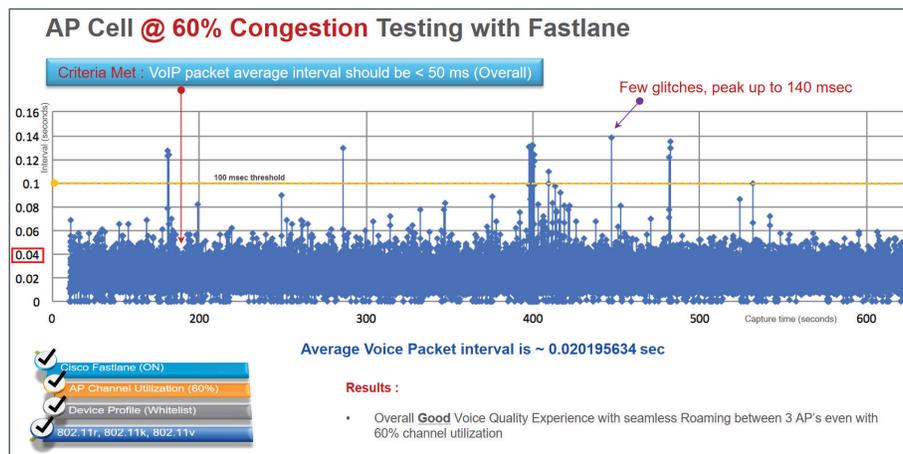


Fast Lane with 60% channel utilization

The next test was to create a condition with wireless traffic simulators where the area being serviced by AP1 shown in Figure 3 is congested to 60% channel utilization. This value is well beyond that which one would typically find in any well design Wi-Fi network, especially one designed using the best practices found in the Cisco Digital Healthcare Architecture.

Even in this test—with Fast lane enabled, the MH-CURE application whitelisted, and roaming optimizations of 802.11r/k/v enabled—although there are some delays in transmitting the voice stream, they are well below our 50 ms objective. These higher delays (max of 35 ms) are caused by channel contention and the iPhone under test trying to get access to the channel.

Figure 5 Fast lane Testing with 60% channel utilization



Disabling Fast Lane for the MH-CURE application

Up to this point, things have gone pretty well, even on a wireless network with a channel utilization of 60%, as well as DFS based channels. Audio quality did not exhibit any significant issues during each of the tests performed with Fast lane enabled.

The next portion of the testing is to start to disable the optimizations that, thus far have yielded some impressive results.

The first is to disable Fast lane through any of the following means:

- Disable Fast lane on the Cisco Wireless LAN controller.
- Use an MDM to push down a whitelist that does not contain the MH-CURE application.
- Switch to an SSID/WLAN that is not listed in the whitelist profile, etc.

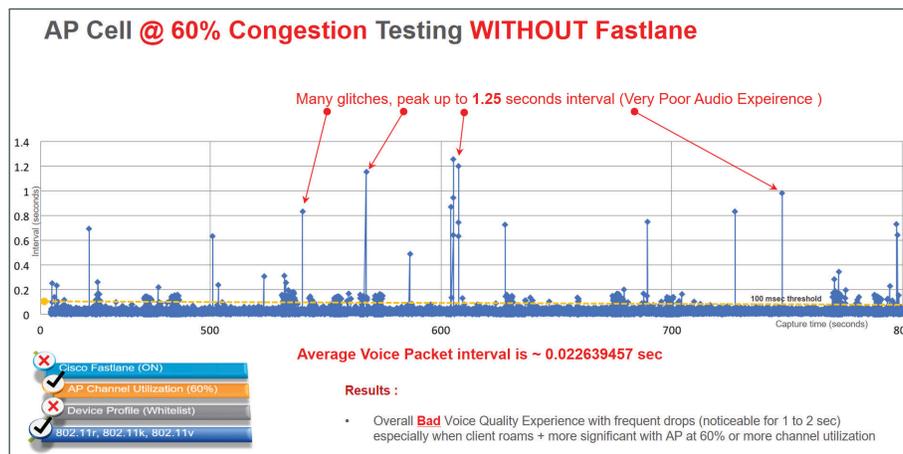
In all cases, similar results were obtained during each of the tests performed.

In Figure 7, the vertical scale has been reduced by a factor of 10, now starting at .1 second or 100 ms. The transmission interval of the voice traffic has significant spikes, some peaking at .7 seconds. During these times, the jitter buffer on the receiver has been exhausted, because they typically range from 30-50 ms, or for some advanced codecs, 100-200ms. In all cases, the result to the user is a perceptible audio artifact or a noticeable distortion of the audio stream.

Depending on the audio codec used, these distortions can manifest themselves as metallic voice followed by chops in the audio and finally dead air. This is when the clinical users begin to lose confidence in the network. This is especially true when care providers are exchanging phone numbers, dosing information, or anything else where a dropped digit in the speech, if noticed by the listener, requires that the speaker repeat himself or herself.

During this test, with the same Wi-Fi network in place and the AP placement unchanged, the end-user experience during the call was significantly worse than when Fast lane was enabled for the MH-CURE application on the Wi-Fi network.

Figure 6 Fast lane disabled, 60% utilization

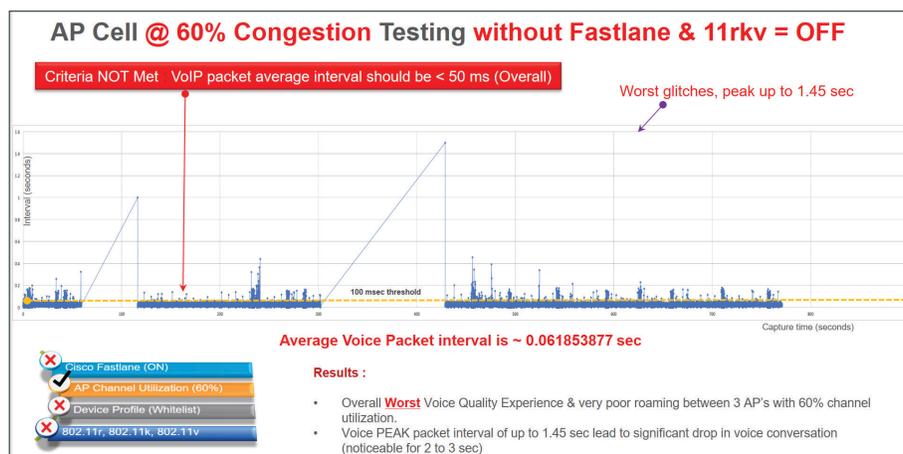


Disabling Both Fast Lane and 802.11k/r/v

In the next test, we congested the AP1 cell to 60% and disabled both Fast lane and 802.11k/r/v. The same test procedure was performed (as shown in Figure 3) with significant issues encountered when entering the congested AP1 cell. As shown on the figure below, times of no connectivity for the mobile client occurred with spikes well over 100 ms and some as high as 1.45 seconds.

Audio quality during this set of tests was well below acceptable levels and unacceptable in any clinical setting.

Figure 7 Fast lane and 802.11k/r/v disabled, 60% channel utilization



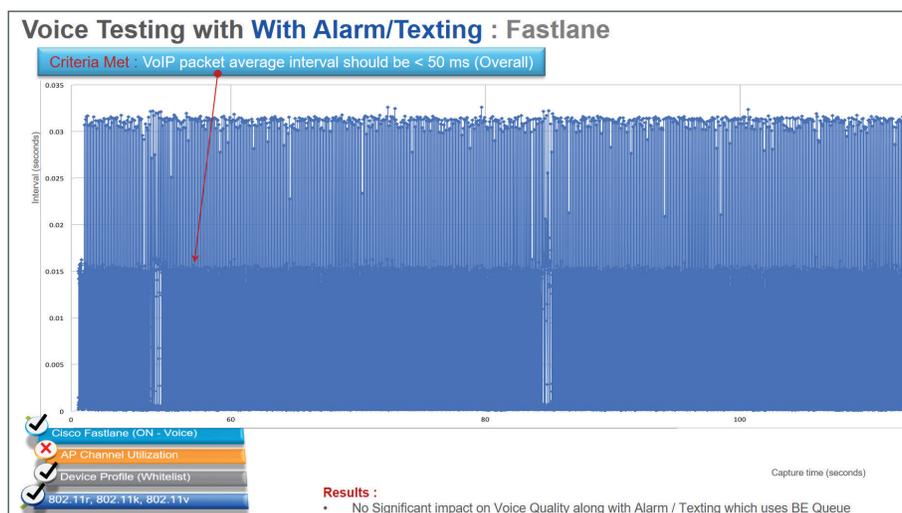
Secure Text Messaging Impacts to Voice Quality

The final test analyzed whether voice quality would be negatively impacted by secure text messaging. In the version of MH-CURE tested, the secure text messages were not prioritized using Fast lane and were instead sent as best effort traffic with each one being received without any noticeable delay.

The parameter for this test was to send a secure text message every 5 seconds to the mobile device. As shown in the figure below, voice traffic averaged approximately 15 ms with peaks of approximately 33 ms. Notice that during the testing, there are no perceivable delays in the transmitted traffic. With peaks of 33 ms, the exhaustion of the jitter buffer did not occur, as there were no noticeable voice imperfections detected during the testing.

In summary, the use of secure text messaging did not have a negative impact to voice quality.

Figure 8 Impacts to voice from secure text messaging

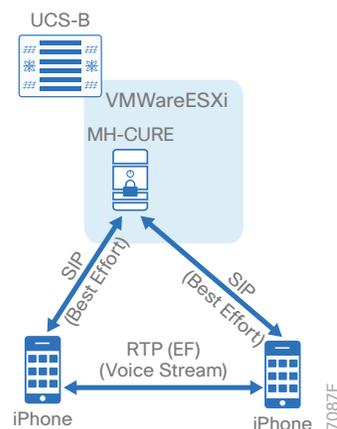


MOBILE HEARTBEAT—FAST LANE

MH-CURE Call Flow

It is important to understand the data communication flows that comprise the complete Clinical Communication solution. Not all of the flows may be Fast lane enabled, but those that ISV deemed critical may be enabled with the Fast lane capable markings. Figure 9, for example, shows the interaction between the Mobile Heartbeat server and iPhone handsets when placing or receiving a voice call with the MH-CURE application.

Figure 9 MH-CURE Call Flow Diagram



In most deployment scenarios, call control requests are forwarded to the MH-CURE server using standard SIP signaling. In a normal SIP call setup, the calling party sends a SIP Invite to the call control stating the directory number to which it wishes to connect. The call control then issues an invite to the handset with the registered destination directory number.

Table 1 Mobile Heartbeat—MH-CURE voice QoS recommendations

| | IP protocol | Apple NSURLSession classification | Recommended DSCP QoS marking | Resulting 802.11e Layer 2 marking |
|------------|-------------|-----------------------------------|------------------------------|-----------------------------------|
| RTP stream | UDP | NET_SERVICE_TYPE_VO | EF | UP 6 |

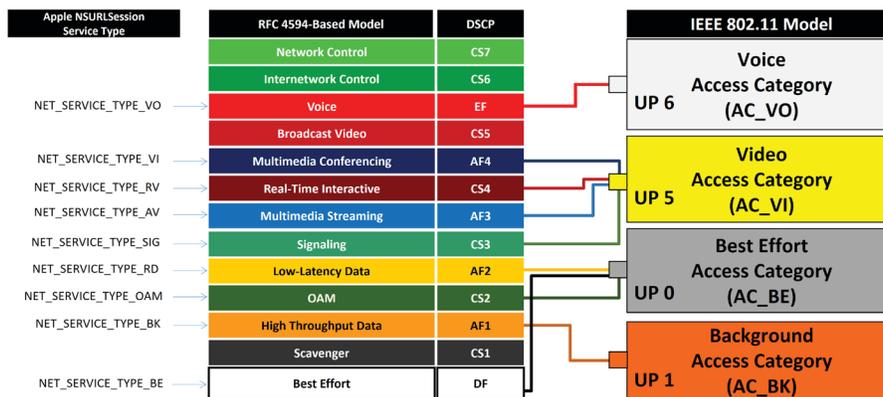
Mobile Heartbeat also supports integration directly with Cisco Unified Communications Manager (CUCM). When integrating with CUCM directly, each MH-CURE device appears to CUCM as a 3rd party SIP line side device. For the Fast lane testing, other than codec selection, the use of one call control over another has no bearing. There are operating modes that would allow the RTP voice stream to hairpin through the call control, but none of the testing performed used this method. Instead, iPhone-to-iPhone calling only used the call control for call setup and the RTP voice stream is direct between the iPhones.

The figure below is not specific to Mobile Heartbeat; rather, it shows the QoS mapping from within the Fast lane enabled application to Layer 3 and Layer 2/802.11 QoS mode. It is provided here so that the mappings from the application layer to the resulting DSCP marking from within the iOS as well as the IEEE 802.11 markings. Essen-

tially, the figure below shows this marking from beginning to end, provided there is no further remarking of traffic elsewhere in the network.

Figure 10 End-to-end QoS mapping

Apple NSURLSession / DSCP / UP Mapping (iOS):



Fast Lane Deployment Details

This section provides the steps necessary to implement Fast lane with the Mobile Heartbeat MH-CURE application. There is no prescribed sequence necessary, but this design is organized from the perspective of the Fast lane-enabled application, infrastructure, and iPhone to the MDM used to roll out the application and whitelist policy, through the network and finally to the Wireless LAN.

PROCESS

Verifying That Components Are Fast Lane-Ready

1. Verify MH-CURE mobile application for the iPhone
2. Ensure Apple iOS Version
3. Verify Cisco WLC

This table lists Fast lane-supported versions of software. Over time, these versions will change, but at the time of this writing (March 2017), these are the currently available versions and the ones that were used during the joint validation process.

Table 2 Software versions for Fast lane support

| | Version |
|-------------------------------|-------------------------|
| MH-CURE for iPhone | 11.1.0 RC1 |
| Apple iOS | 10.0 or higher (10.2.1) |
| Cisco Wireless LAN controller | 8.3.112.0 or higher |

Procedure 1 Verify MH-CURE mobile application for the iPhone

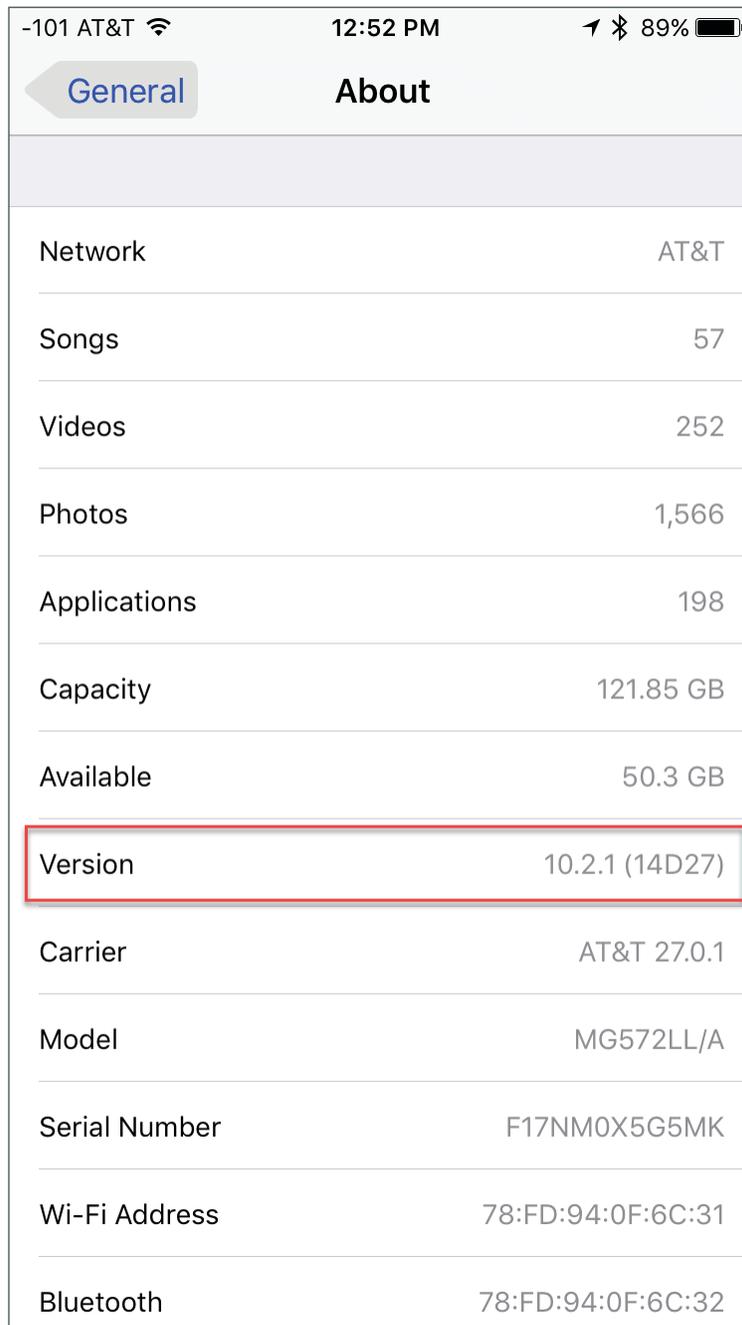
Step 1: Verify that the Mobile Heartbeat–MH-CURE application is version 11.1.0 RC1 or higher.

Step 2: Ensure that all previously deployed versions of MH-CURE have been updated to the proper Fast lane-capable version.

Procedure 2 Ensure Apple iOS Version

Ensure that all deployed versions of Apple iPhones or iPads are running iOS release 10.2.1 or higher.

Step 1: On the iPhone, select **Settings > General > About** and note the version, as shown below.



| General | | About | |
|---------------|--|-------|-------------------|
| Network | | | AT&T |
| Songs | | | 57 |
| Videos | | | 252 |
| Photos | | | 1,566 |
| Applications | | | 198 |
| Capacity | | | 121.85 GB |
| Available | | | 50.3 GB |
| Version | | | 10.2.1 (14D27) |
| Carrier | | | AT&T 27.0.1 |
| Model | | | MG572LL/A |
| Serial Number | | | F17NM0X5G5MK |
| Wi-Fi Address | | | 78:FD:94:0F:6C:31 |
| Bluetooth | | | 78:FD:94:0F:6C:32 |

Procedure 3 Verify Cisco WLC

The Cisco WLC must be running release 8.3 or higher. As of the time of this writing (March 2017), the recommended release is 8.3.112.0.

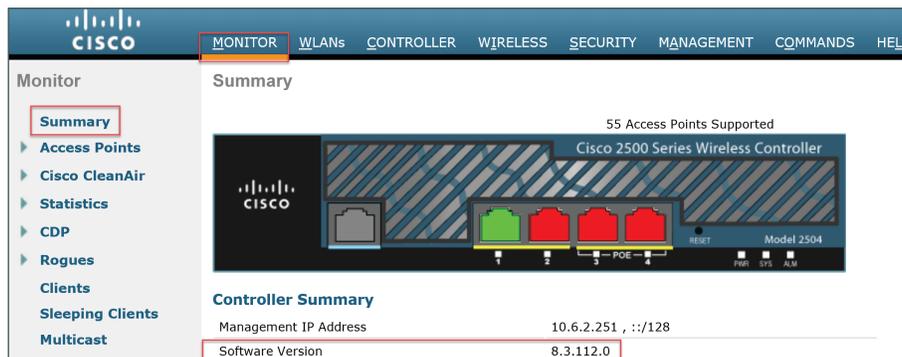
Step 1: Log on to the Cisco Wireless LAN controller.

Step 2: On some releases of the WLC, you will have to select **Advanced** in the upper right corner.



Step 3: On the **Monitor > Summary** tab, verify that the software version of the WLC is 8.3.112.0 or higher.

Figure 11 Wireless LAN Controller Code Version



PROCESS

Configuring Mobility Device Manager

1. Access Mobility Device Manager

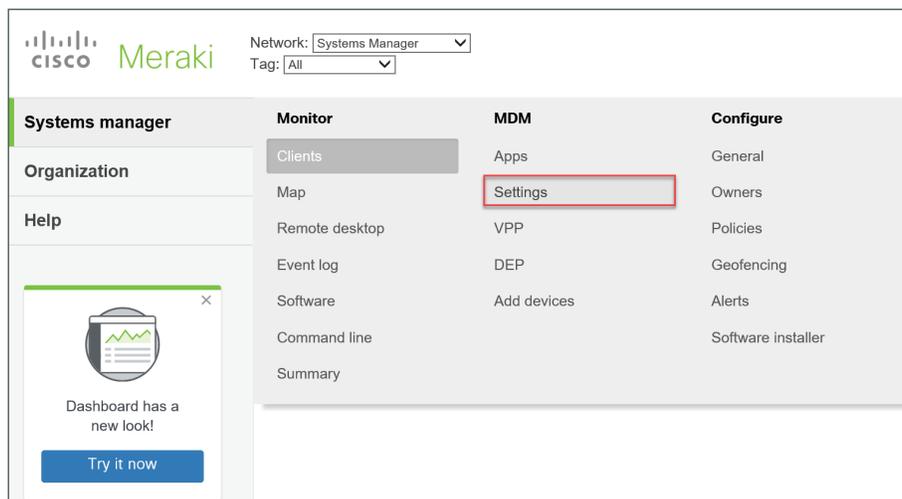
There are a number of different MDMs available on the market. It is beyond the scope of this guide to describe the use of each MDM product and version. Instead, it shows the major steps required. Accomplishing these steps on your specific MDM product is required.

For the Fast lane validation that was completed with Mobile Heartbeat, the Cisco Meraki Mobility Device Manager was used.

Procedure 1 Access Mobility Device Manager

Step 1: Login to the Meraki System Manager at https://account.meraki.com/secure/login/dashboard_login

Step 2: Select **Systems Manager > Settings**.



Step 3: If no profile exists within the Meraki System Manager, create a profile by clicking **Create a profile**.

Step 4: Depending on your installation type (Meraki Managed Profile with or without Apple User Scoping), click **Create new profile**.

Step 5: Provide a meaningful name for the Profile, along with a description. You may also specify the Removal Policy requiring the user to enter a password before the policy can be removed from the iOS device. If you have placed all of the clinical mobile devices into a common scope or group, select that group from the **Scope > Apply to devices** list; otherwise, select **All devices**.

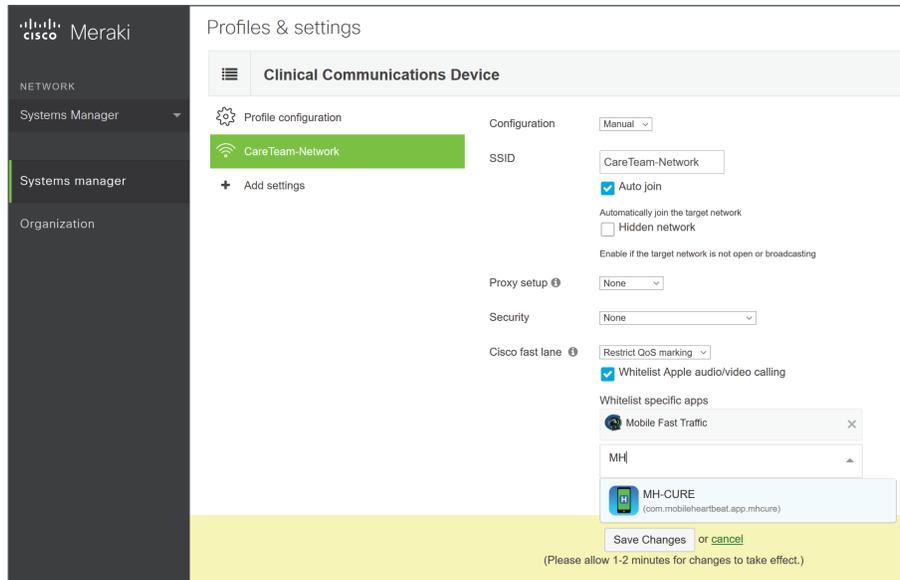
The screenshot shows the Meraki Systems Manager interface for configuring a profile. The profile is named "Clinical Communications Device" and is a Meraki managed profile. The description is "This profile will be used by all care team devices". The removal policy is set to "Allow users to remove this profile". The scope is set to "All devices". The installation info shows "All devices". A table below shows the devices in scope:

| Name | System type | OS | Installation | Tags | Status |
|-------------|-------------|------------|---------------|----------------|-----------------------|
| 1 St4Phone2 | iPhone 6 | iOS 10.2.1 | Not installed | recently-added | Will be added on save |

Step 6: Select the **Add settings** option to create a specific Wi-Fi policy, and then select the WiFi icon.

The screenshot shows the Meraki Systems Manager interface for configuring a profile. The profile is named "Clinical Communications Device". The "Add settings" button is highlighted with a red box. Below it, a grid of settings icons is displayed, with the "WiFi" icon also highlighted with a red box.

Step 7: Specify the SSID that the Clinical Communication end users will use to connect to the Wi-Fi network (example: CareTeam-Network). Optionally select **Auto Join** if you want the mobile device to automatically join the network. If the network is hidden from SSID advertisement, select **Hidden Network**. Select the appropriate security level for this SSID. Under Cisco Fast lane, select **Restrict QoS marking**. Optionally select **Whitelist Apple audio/video calling** to be included in the QoS marking.



Step 8: Select any other applications that are Fast lane enabled and deemed mission critical.

Step 9: Click **Save Changes**.

PROCESS

Verifying End-to-End QoS

1. Configure WLC QoS

For QoS to be effective, it must be enabled on all network infrastructure devices that comprise the path of the Clinical Communication traffic. This includes the following places in the network:

- WLC
- Access layer switches and distribution and core switches
- Data center switching that provides connectivity to the Mobile Heartbeat application suite
- Any WAN link hub or spoke routers
- Hypervisor-based QoS

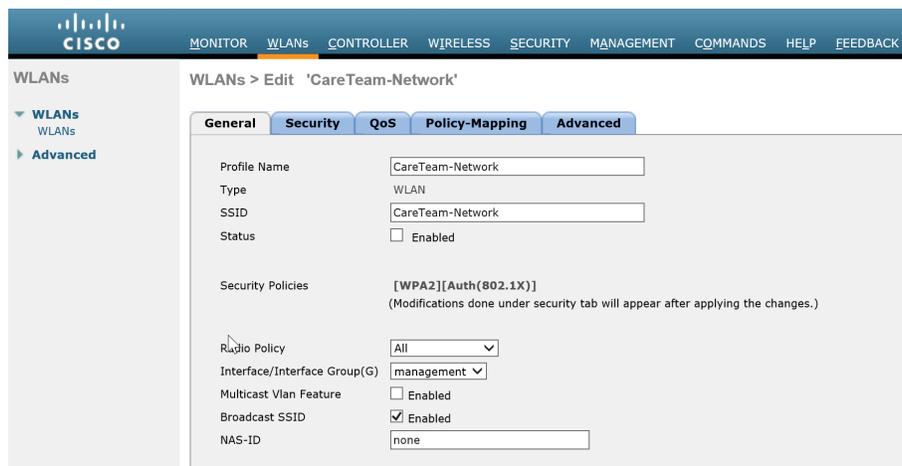
It is beyond the scope of this document to investigate and provide guidance on each infrastructure component in the list above. Because the WLC is a key component to Fast lane, the following section provides guidance on the WLC QoS configuration. For all other infrastructure components listed above, it is recommended that guidance be sought directly from the manufacturer of those components.

Procedure 1 Configure WLC QoS

Step 1: In your browser, log on to Cisco WLC.

Step 2: Select **MONITOR** then click **Advanced**.

Step 3: On the WLANs tab, enter the WLAN SSID that corresponds to the WLAN that will be used for the Clinical Communications network. (example: CareTeam-Network).

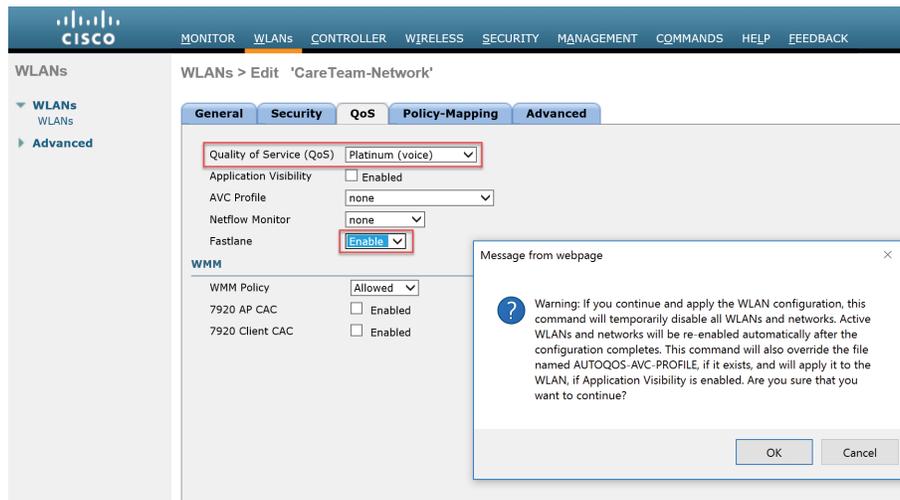


The screenshot shows the Cisco WLC configuration interface for the 'CareTeam-Network' WLAN. The 'Advanced' tab is selected, and the following configuration is visible:

| Field | Value |
|------------------------------|---|
| Profile Name | CareTeam-Network |
| Type | WLAN |
| SSID | CareTeam-Network |
| Status | <input type="checkbox"/> Enabled |
| Security Policies | [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) |
| Radio Policy | All |
| Interface/Interface Group(G) | management |
| Multicast Vlan Feature | <input type="checkbox"/> Enabled |
| Broadcast SSID | <input checked="" type="checkbox"/> Enabled |
| NAS-ID | none |

Step 4: On the QoS tab, in the **Quality of Service** list, select **Platinum (voice)**.

Step 5: In the **Fast lane** list, select **Enable**. A warning appears, informing you of a temporary disruption in connectivity. If this is acceptable, click **OK** and click **Apply**.



Caution

Enabling Fast lane will temporarily disable and re-enable the Wireless LAN Configuration. In all clinical settings, this change should be scheduled to prevent a disruption to the delivery of care.

Step 6: Save the configuration.

PROCESS

Verifying That Fast lane Is Operational

1. Verify Fast Lane is operational

There are two levels of verifying that Fast lane is operational. The first is to check that Fast lane has been enabled on the WLAN being used by the Clinical Communication team using the Cisco Fast Traffic application available in the Apple AppStore.

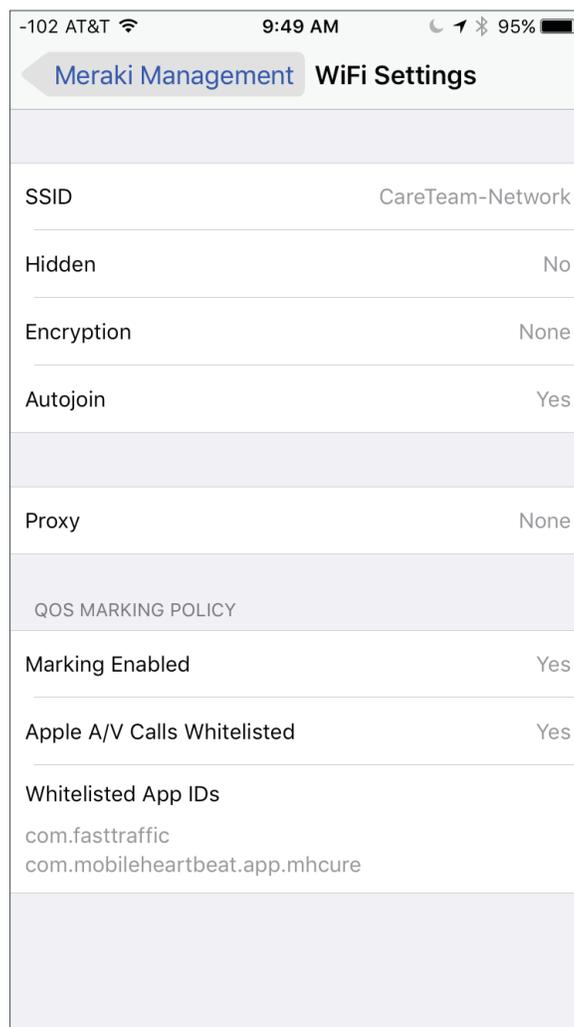
The second and more precise option is to perform an RF packet capture of an iOS device that has the MH-CURE application installed. This will require a device capable of capturing packets on the Wi-Fi RF network, such as Wireshark on a MacBook Pro or sniffer mode on a Cisco access point.

Procedure 1 Verify Fast Lane is operational**Option 1: Use the Fast Traffic app**

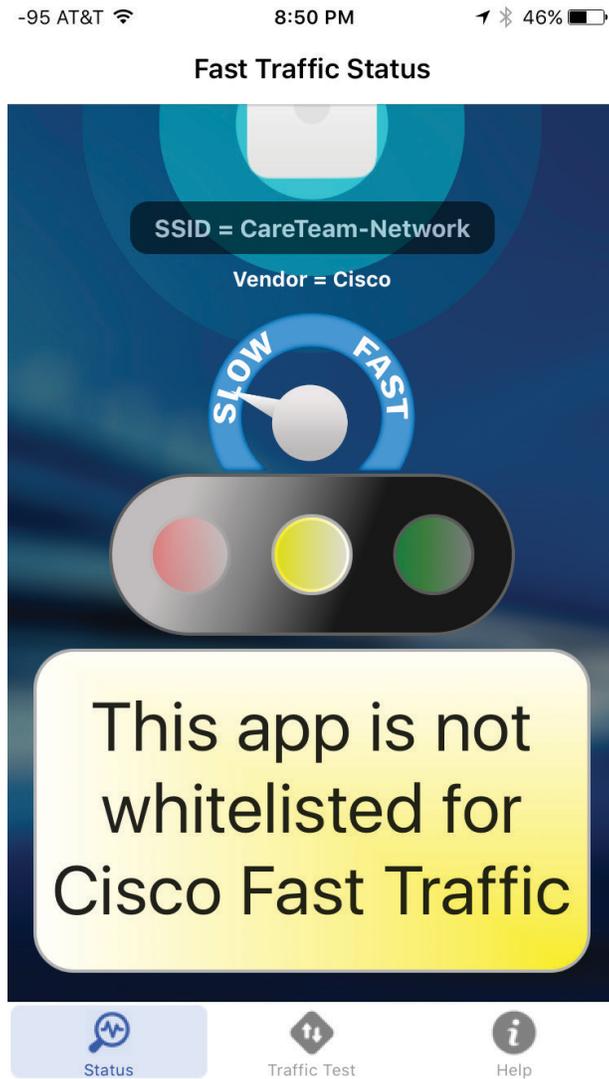
Step 1: From the Apple AppStore, download and install the Cisco Fast Traffic application onto an iOS device.

Step 2: In Meraki MDM, add the Fast Traffic application to the whitelist and download the profile to the iOS device.

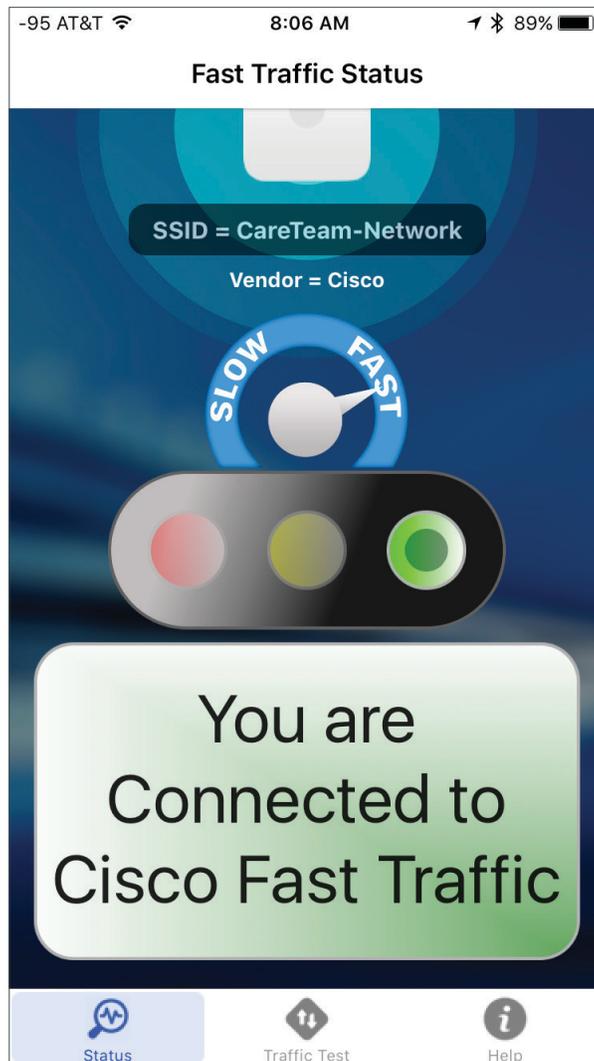
Step 3: On the iOS device, verify that the Wi-Fi policy is correct by navigating to **Settings > General > Device Management > Meraki Management > More Details > WiFi Settings**.



If Fast lane is enabled but the whitelist does not contain the Fast Traffic application, a message informs you that you're on a Fast lane network but that the application is not whitelisted, as shown.



If Fast lane is enabled and the application is whitelisted, the following should appear.



Tech Tip

After an MDM profile change is made to the Wi-Fi settings, such as removing an application from the whitelist, it is sometimes necessary to disconnect from the Wi-Fi network and reconnect in order for the changes to take effect.

Option 2: Use RF packet capture

Step 1: Ensure that the SSID/WLAN that is being used for this test does not have encryption enabled. Failure to turn off security and match the MDM Wi-Fi profile to the same settings will not allow you to see the DSCP QoS settings because they will be encrypted.

Step 2: Determine with which access point the iPhone being tested is associated.

Step 3: From the WLC, determine which channel is in use by the access point.

Step 4: Ensure that the device performing the RF-based packet capture is set to the same channel as the access point and begin the capture.

Step 5: On the iOS device, launch the MH-CURE application and place a call to any other handset.

Step 6: Stop the capture, and using Wireshark or another packet capture tool, decode the captured packet.

Step 7: On the Real Time Protocol (RTP) frames, expand the IP header as shown and verify that the DSCP marking is set to Expedited Forwarding 46 (EF).

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-----------|-------------|----------|--------|--|
| 4785 | 18.979900 | 10.9.5.17 | 10.9.5.35 | RTP | 184 | PT=opus, SSRC=0x6288C7C7, Seq=16001, Time=2880 |
| 4792 | 19.003102 | 10.9.5.17 | 10.9.5.35 | RTP | 185 | PT=opus, SSRC=0x6288C7C7, Seq=16002, Time=3840 |
| 4794 | 19.003516 | 10.9.5.17 | 10.9.5.35 | RTP | 185 | PT=opus, SSRC=0x6288C7C7, Seq=16002, Time=3840 |


```

> Frame 4792: 185 bytes on wire (1480 bits), 185 bytes captured (1480 bits) on interface 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .....TC
> Logical-Link Control
> Internet Protocol Version 4, Src: 10.9.5.17, Dst: 10.9.5.35
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  <v> Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10... = Differentiated Services Codepoint: Expedited Forwarding (46)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 91
  Identification: 0x116e (4462)
  > Flags: 0x00
  Fragment offset: 0
  Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0x4a27 [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.9.5.17
  Destination: 10.9.5.35
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
> User Datagram Protocol, Src Port: 4000, Dst Port: 20000
> Real-Time Transport Protocol
  
```

Tech Tip

Creating a blacklist that does not contain the Mobile Heartbeat applications and pushing this Wi-Fi profile to the phone with the MDM is one way to verify that the Fast lane marking of applications in the whitelist is functional.

Appendix A: Product List

The following products and software versions have been validated for CVD.

| Functional Area | Product | Part Numbers | Software Version |
|---------------------------------|-------------------------------|---|-----------------------------|
| Wireless network | Cisco Wireless LAN controller | AIR-CT5508-12-K9 | 8.3.112.0 release candidate |
| | Cisco Wireless Access Point | AIR-AP3802I-x-K9 | |
| Mobile device | iPhone 6S, 7 | iPhone 6S (MKRF2LL/A) iPhone 7 (MN8J2LL/A) | 8.2.1 (14D27) |
| Clinical Communication software | Mobile Heartbeat MH-CURE | N/A | 4.1.0 RC1 |
| Mobility Device Manager | Meraki System Manager | – | – |
| | Apple Configurator 2 | – | Version 2.3 (Sep 13, 2016) |

Appendix B: Changes

This is the initial version of this document.





Please use the [feedback form](#) to send comments and suggestions about this guide.



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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2017 Cisco Systems, Inc. All rights reserved.

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)