CISCO VALIDATED DESIGN

Adopting Fast Lane in Clinical Communications—PatientSafe Solutions

June 2017

Table of Contents

Introduction

Optimizing the caregiver experience for healthcare organizations who are adopting clinical communication system is a complex task. Together, Apple, Cisco, and PatientSafe Solutions have proven the benefits of a new technology called Fastlane. When a Cisco Fast lane enabled wireless network detects an Apple iOS 10+ device running a Fast lane enabled application like the PatientTouch application from PatientSafe, wonderful things happen, and clinical teams notice.

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

Apple, Cisco, and PatientSafe recently conducted onsite Fast lane QoS validation, demonstrating the considerable advantages for the clinical mobility user:

- Improved audio and video quality.
- Optimized clinical application performance.
- Reduced battery consumption.

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

FAST LANE OVERVIEW

Prioritizing business-critical applications such as clinical communications 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 Fastlane.

UNDERSTANDING FAST LANE COMPONENTS

A few technology-based components need to be in place in order to implement Fastlane. 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

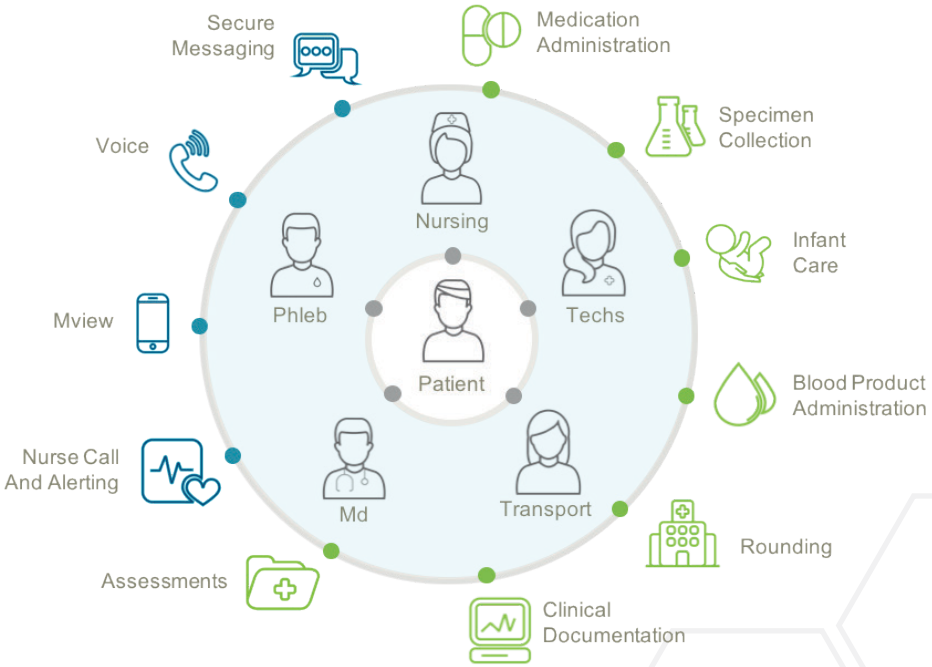
Fast lane is supported starting with release 10 of Apple iOS. Apple devices that support version 10 or higher support Fastlane. Advances in antenna design as well as Wi-Fi chip sets do favor the newer models of iPhones such as the iPhone 7, followed by the 6S and so on. In addition, the Apple SE (non-cellular) 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 exhibited a relatively low end user experience, primarily due to the factors outlined above.

PatientTouch from PatientSafe Solutions

A Unified Communications and Workflow Solution

PatientTouch is the only clinical communications platform that unifies secure communication with workflow, consolidating multiple devices and siloed applications into one integrated solution. Unlike rip-and-replace, single-purpose solutions, PatientTouch integrates seamlessly with your current IT infrastructure, maximizing return on investment and decreasing cost by reducing device, application, and vendor management.

Figure 1 *PatientTouch unites communication and workflow in one app, on one device*

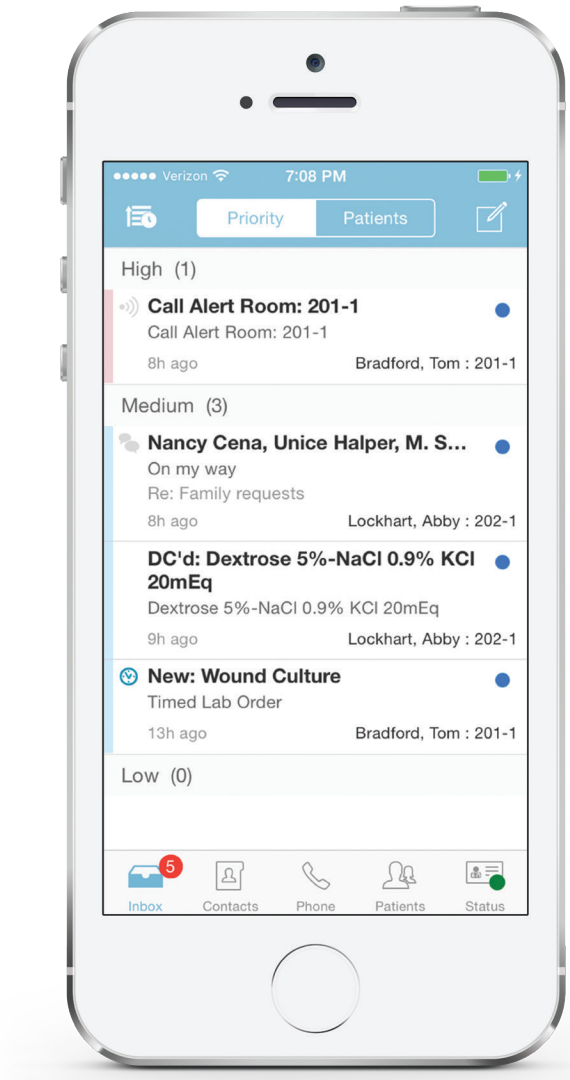


How It Works

PatientTouch delivers secure messaging, voice, critical alerts, nurse calls, and high-frequency clinical workflows like specimen collection, rounding, assessments, nursing documentation and more – in one mobile app, on one device.

The Unified Inbox prioritizes all incoming messages, alerts, notifications, tasks, vitals, reminders, and results for every member of the care team – physicians, nurses and ancillary staff – giving them a comprehensive view of their care delivery day wherever they are.

Figure 2 *PatientTouch Unified Inbox – all messages, alerts, results in one prioritized inbox*



Fully integrated with your EMR and other clinical systems, relevant patient and clinical information can be accessed from within the application to support efficient decision making. Real-time patient and clinical information is automatically embedded in text messages for faster, safer collaboration in fewer communication cycles. The system integrates with your scheduling systems and directories to ensure the assigned care team is always connected - across shifts, facilities, and the patient's care trajectory.

Security and HIPAA-compliance

PatientTouch provides fully HIPAA-compliant functionality including secured messaging, user profile-based patient information access restriction, and full audit reporting. This careful selection of technology enables your facility to derive further efficiencies and care coordination value from existing infrastructure investments without compromising security or patient privacy. Unlike other vendors, PatientTouch only stores data on your secured and encrypted databases. Data is never stored locally on the mobile device. With data secured at rest and in transport and no ePHI stored locally on the mobile device, the solution ensures even your BYOD users maintain the security and privacy you require.

Enterprise-grade

PatientTouch platform architecture is built for complex, multi-facility enterprises:

Manageability: Our Enterprise Manager functionality enables accurate modelling of your organization, dynamic assignment, and real-time routing of communications to the care team. You can manage assignments, alerting, telephony, and clinical systems from a centralized web console.

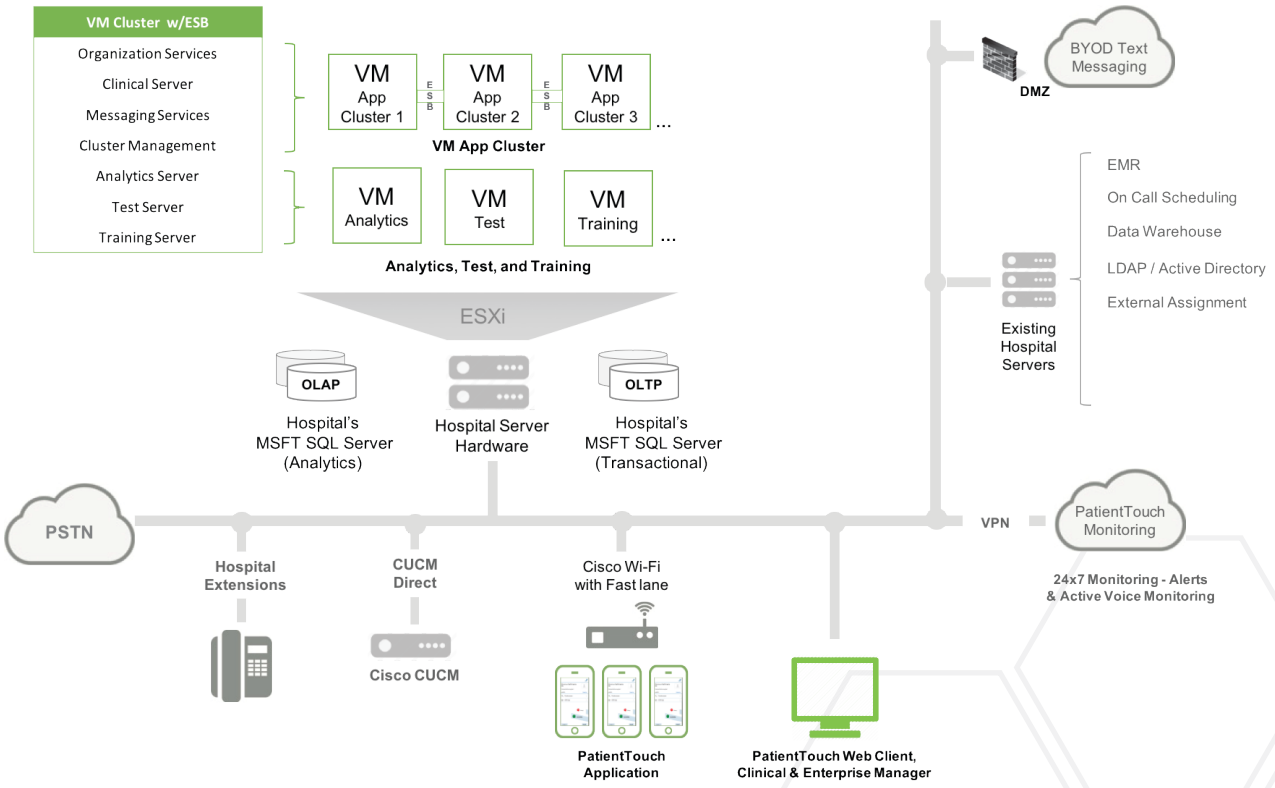
Performance: Enterprise service bus caching, load-balancing, and high-availability clustering ensures clinical-grade performance

Reliability: Active-active server architecture provides failover for business continuity

Scalability: Server clustering simplifies scaling as users, transactions and facilities grow .

Security: The platform surpasses HIPAA-compliance with data encryption at rest and transport

Figure 3 *PatientTouch architecture*



Interoperable with Current IT Investments

PatientTouch integrates with your EMR, IT infrastructure, and clinical systems to provide instant access to real-time care team, patient and clinical data for every member of the care team across your enterprise. Through RESTful APIs, web services, HL7, SIP, TAP, WCTP, and other protocols, PatientTouch enables the following systems:

- ADT
- EMR—medications, lab results, vitals, I/O, nurse documentation
- Nurse call and bed systems
- Alert management systems and middleware
- MDM
- Telemetry and monitoring
- On call, scheduling, and assignment systems
- Active Directory/LDAP
- Telephony PBX and Voice over Wi-Fi
- Direct Cisco Unified Call Manager (CUCM)
- Cisco/Apple Fastlane
- Apple CallKit on iOS 10
- Mobile App Deep Linking—Epic Haiku, Epic Rover, Bernoulli, and more
- Paging and messaging systems

Service and Support

As vendor-managed solution, PatientSafe takes the burden off your teams and partners for every step of your mobility journey. PatientSafe is the only platform vendor in the 2016 KLAS Secure Communications report that can claim that 100% of its customers:

- Would buy from the vendor again.
- Say that the vendor keeps promises.
- Include the vendor in their long term plans.

Professional services:

- Proven implementation methodology honed over years of EMR and mobility integrations
- Team of 20+ professionals with deep clinical, IT and TechOps expertise
- Clinical workflow, wireless, and mobility adoption assessments
- Scope control

Support services:

- 24x7x365 Tier 1 through Tier 3 Call Desk Support
- 76% of incoming calls resolved within first 3 hours
- Proactive Remote Systems Monitoring
- Interface status monitoring
- Systems performance monitoring
- Utilization and compliance rate monitoring

The Results

CLINICAL COMMUNICATIONS

- 86% of users experience improved response times
- 86% of users feel more connected to the care team
- 79% of users see improved communication of patient information
- 67% of clinicians experience fewer interruptions
- 50% improvement in response time to rapid patient deterioration

CLINICAL WORKFLOW

- 97% average compliance across 80+ hospitals
- 60 minutes per nurse per shift saved on documentation and coordination
- 20% reduction in duplicative lab orders
- 15% decrease in STAT order to lab time
- 15% improvement in HCAHPS per medication education to patients

With PatientSafe as your technology partner and PatientTouch as your communications platform, you can significantly decrease costs, increase care team productivity, and improve patient safety and satisfaction across your healthcare enterprise.

Cisco Digital Network Architecture for Healthcare

The Cisco Digital Healthcare Architecture (DHA) for Healthcare 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 the Cisco DHA for Healthcare, 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.

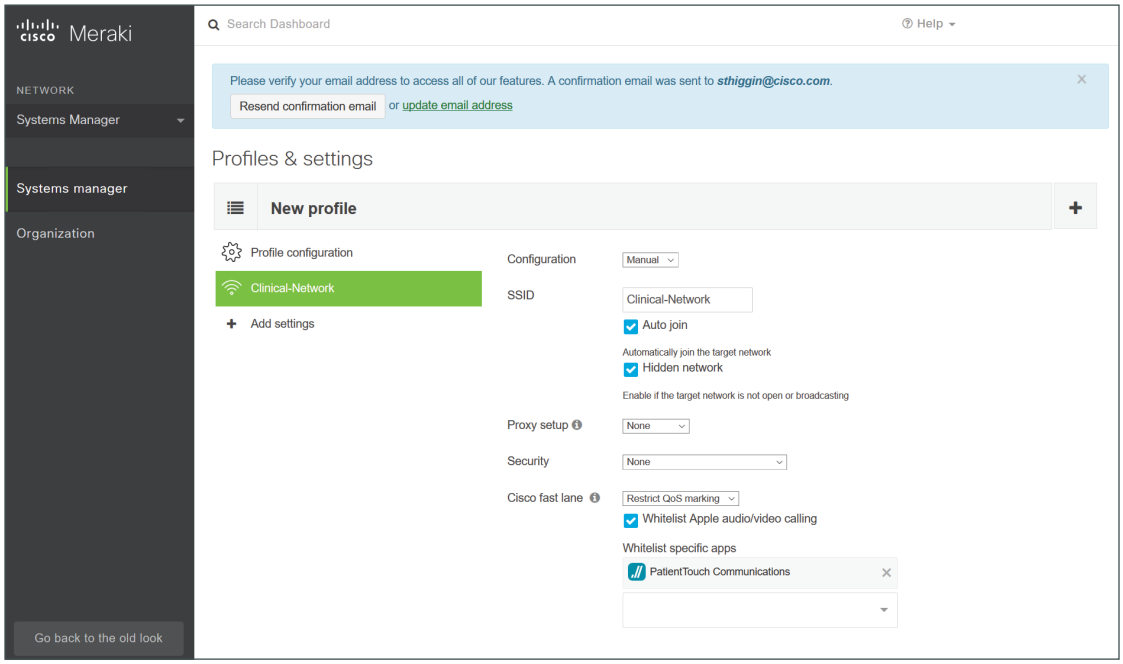
The benefits of using Fast lane and Cisco DHA not only provide optimized voice quality in the case of PatientSafe Solutions, but also include improved battery performance due to the significant reduction in the retransmissions of traffic in a heavily congested cell (See Fast lane Observations—PatientSafe Solutions). 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 our 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, receive end-to-end priority treatment on the network.

Figure 4 *Meraki Mobility Device Manager—whitelist profile*



By default, in the absence of a whitelist, all Fast lane enabled applications receive priority treatment as identified within the Fast lane enabled mobile application. Once the HDO pushes a Wi-Fi profile that contains a Fast lane based whitelist, only those applications contained within the whitelist receive priority service. All applications not in the whitelist 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–PATIENTSAFE SOLUTIONS

This section discusses the tests that were performed in the Cisco RF Validation labs. 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 5 *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 Fastlane. Any delays or retransmissions in transmitting these packets on timed bases are easy to spot by using statistical analysis and inspection.

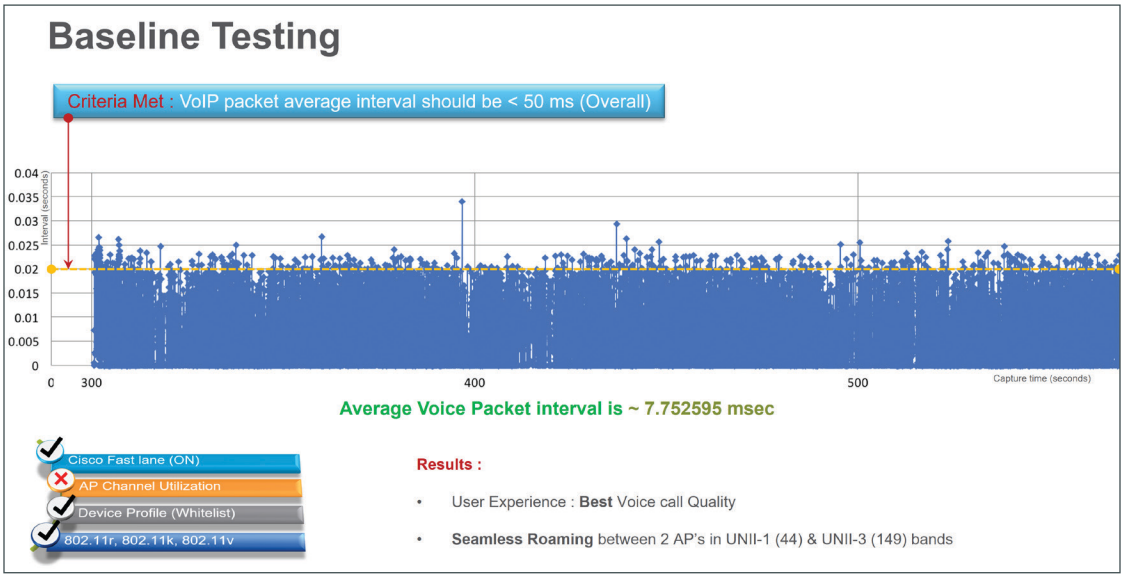
Baseline

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

In Figure 6, 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 does 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 5 above.

Figure 6 *PatientSafe baseline testing*

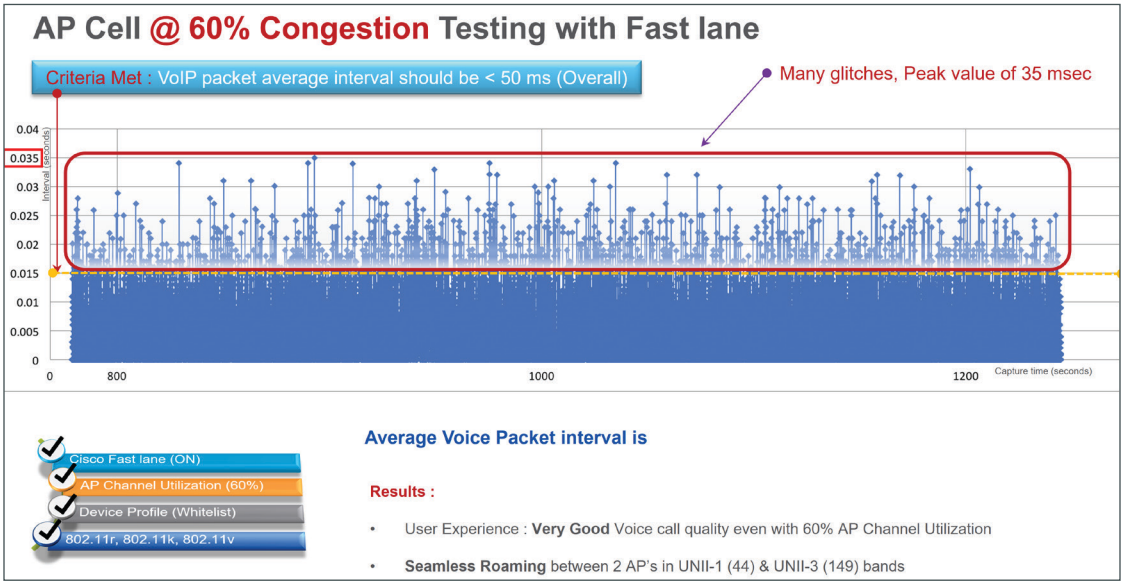


Fast lane with 60% Channel Utilization

The next test was to create a condition with wireless traffic simulators where the area being serviced by AP1 as (shown in Figure 5) 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 and with the PatientTouch 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 the 50 ms objective. These higher delays (max of 35ms) are caused by channel contention and the iPhone under test trying to get access to the channel.

Figure 7 *Fast lane testing with 60% channel utilization*

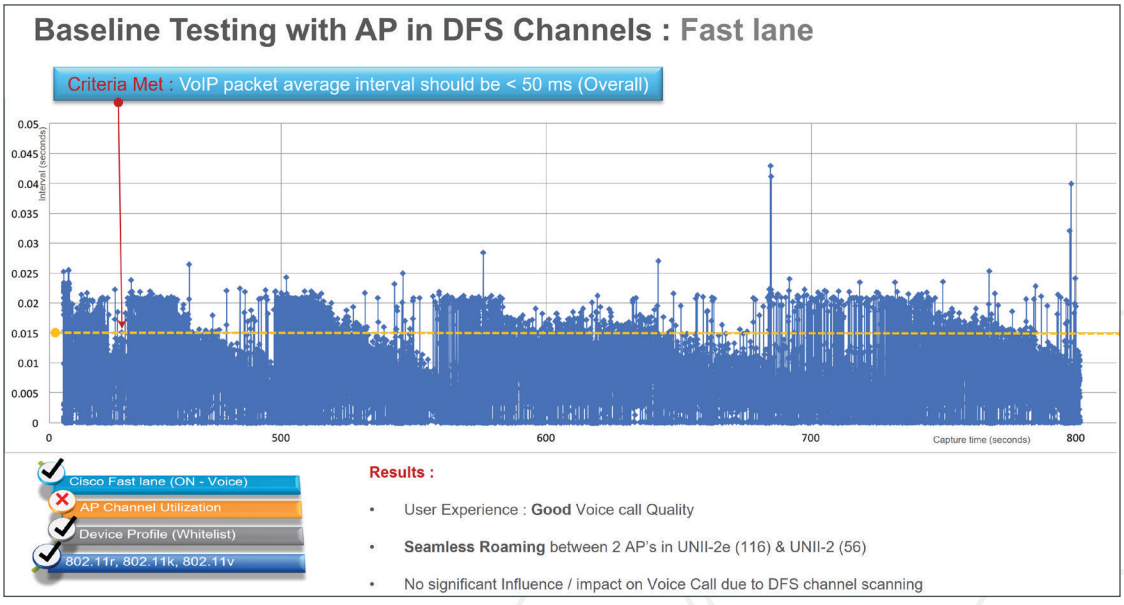


Baseline Fast lane Using DFS Channels

Channels in the UNII-2e and UNII-2 bands (Channels 52-64 and 100-144) share the same frequencies as aviation and weather radar. As a result, the Wi-Fi standard requires that access points operating in these bands perform scans to detect the presence of radar transmissions.

During this operation, no negative effects were encountered. The saw-tooth-based delays in transmission are from the DFS channel scanning, but again, the majority of the voice traffic is being transmitted well under the 50 ms goal.

Figure 8 *Fast lane roaming between DFS Channels*



Disabling Fast lane for the PatientTouch 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.

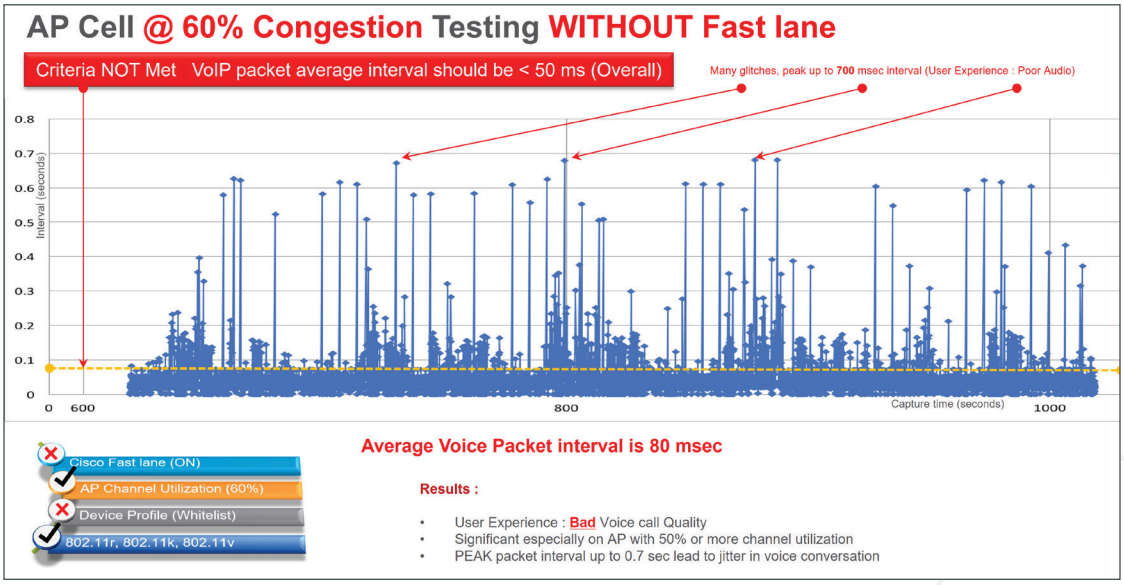
The first is to disable Fastlane. There are a number of ways that this can be accomplished: disabling Fast lane on the Cisco Wireless LAN controller (WLC), using the MDM to push down a whitelist that does not contain the PatientTouch application, switching to an SSID/WLAN that is not listed in the whitelist profile, and so on. In all cases, similar results were obtained during each of the tests performed.

In Figure 9, the vertical scale has been reduced by a factor of 10, now starting at .1 second (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 and finally by 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 PatientTouch application on the Wi-Fi network.

Figure 9 *Fast lane disabled, 60% utilization*

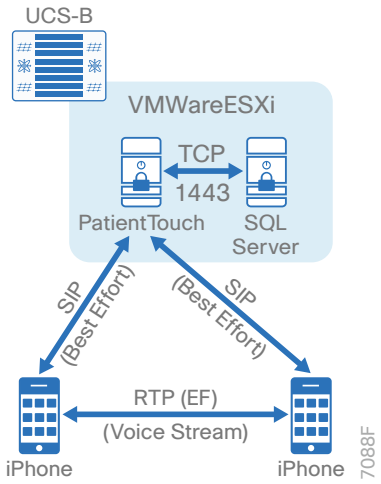


PATIENTSAFE SOLUTIONS–FAST LANE

PatientTouch 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 PatientSafe server and iPhone handsets when placing or receiving a voice call with the PatientTouch application

Figure 10 *PatientTouch call flow diagram*



In most deployment scenarios, call control requests are forwarded to the PatientTouch 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 *PatientSafe Solutions–PatientTouch voice QoS recommendations*

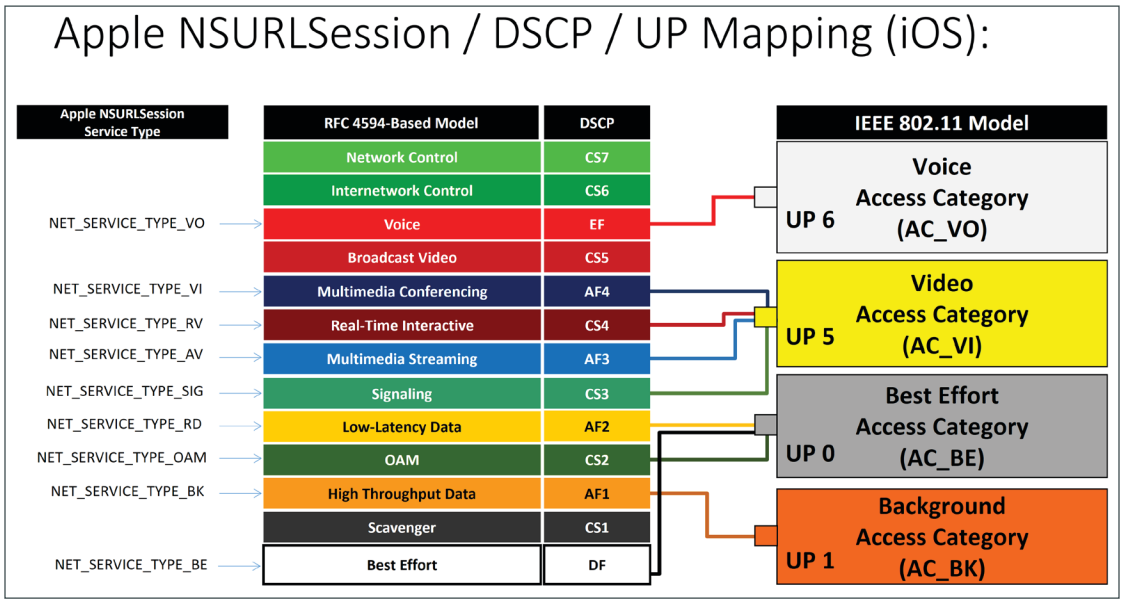
	IP protocol	Apple NSURLsession classification	Recommended DSCP QoS marking	Resulting 802.11e Layer 2 marking
SIP signaling	TCP or UDP port 5060	NET_SERVICE_TYPE_SIG	CS3	UP 5
RTP stream	UDP	NET_SERVICE_TYPE_VO	EF	UP 6

PatientSafe Solutions also support integration directly with Cisco CUCM. When integrating with CUCM directly, unless a Cisco COP file for PatientTouch is present in your implementation, each PatientTouch device appears to CUCM as a 3rd party SIP line side device. Alternatively, a turnkey SIP Trunk integration between a PatientTouch Voice appliance and CUCM is available and provides equivalent and proven call and service quality without having to manage PatientTouch devices within CUCM. For the Fast lane testing, other than codec selection, the use of one call control over another has no bearing. PatientSafe Solutions' highly versatile audio codec selection scales from low bitrate narrowband speech to high fidelity stereo music, providing unmatched interactive speech quality.

There are operating modes that would allow the RTP voice stream to hairpin through the server providing call control, but none of the testing performed with PatientSafe Solutions used this call flow. 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 PatientSafe Solutions; 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. Essentially, the figure below shows this marking from beginning to end, provided there is no further remarking of traffic elsewhere in the network.

Figure 11 *End-to-End QoS Mapping*



Fast lane Deployment Details

This section describes the steps necessary to implement Fast lane with the PatientSafe PatientTouch 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 PatientTouch mobile application for the iPhone
2. Ensure Apple iOS Version
3. Verify Cisco WLC

This table lists the 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
PatientTouch for iPhone	4.1.0 RC1
Apple iOS	10.0 or higher (10.2.1)
Cisco wireless LAN controller	8.3.112.0 or higher

Procedure 1 Verify PatientTouch mobile application for the iPhone

Step 1: Verify that the PatientSafe Solutions–PatientTouch application is version 4.1.0 RC1.

Step 2: Ensure that all previously deployed versions of PatientTouch 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.

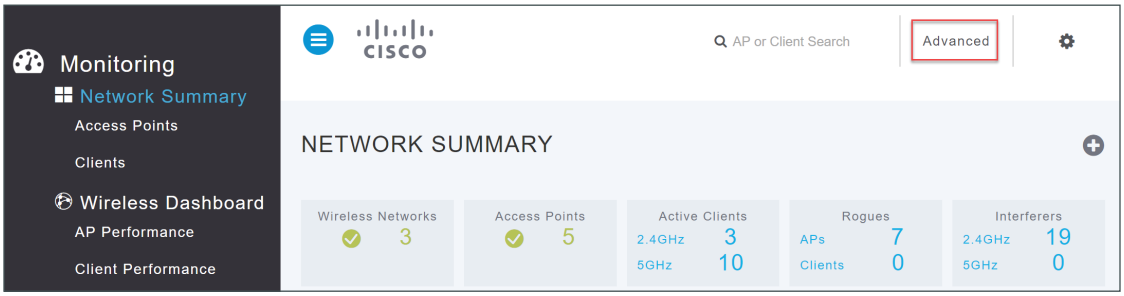
Step 1: On the iPhone, select **Settings > General > About** and note the version.

Procedure 3 Verify Cisco WLC

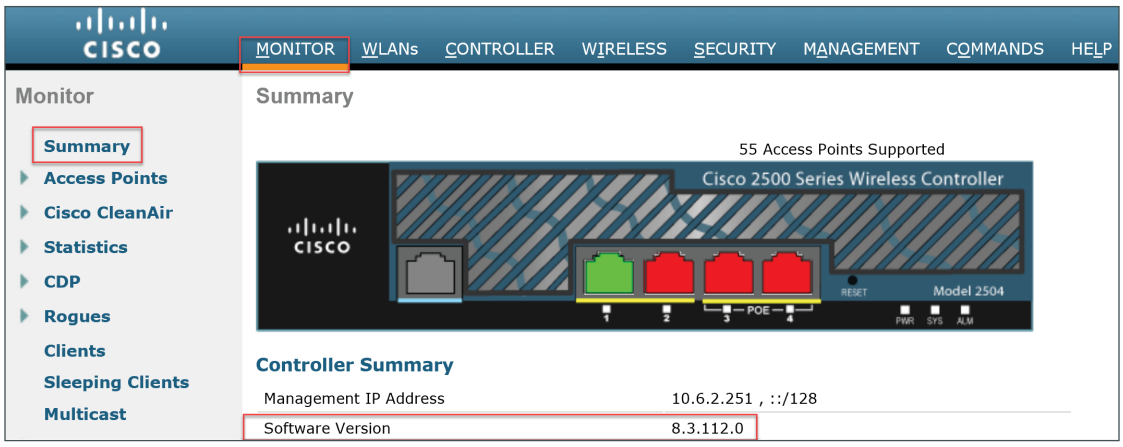
The Cisco WLC must be running release 8.3 or higher. As of the time of this writing (March 2017), the recommended release is 8.3.112.0.

Step 1: Logon 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 or higher.



PROCESS

Mobility Device Manager

1. Access Mobility Device Manager

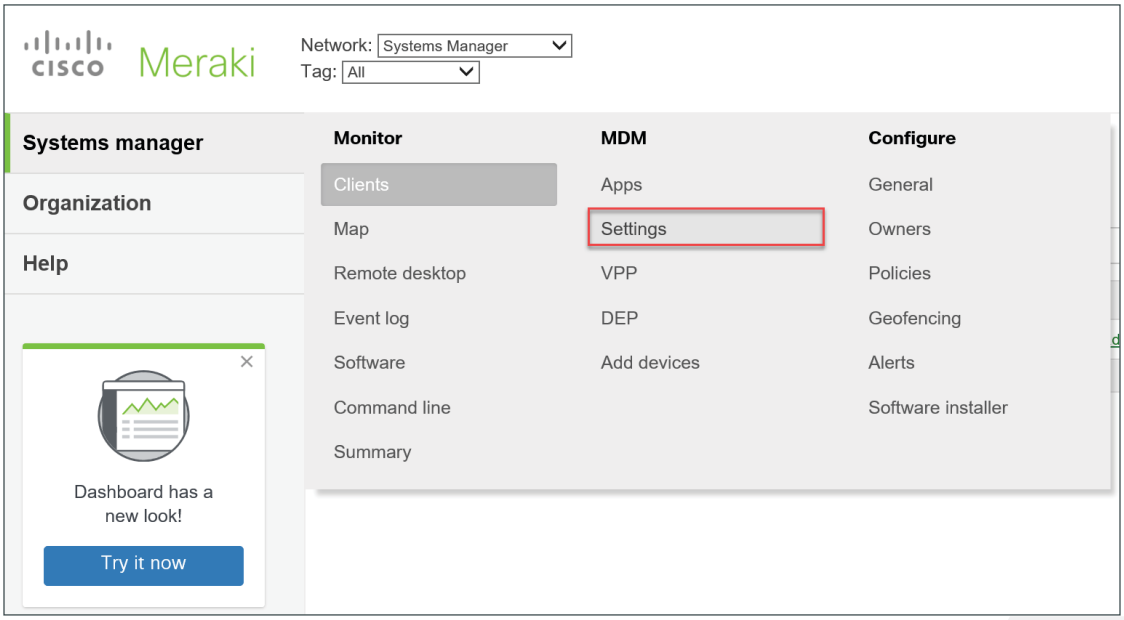
There are a number of different MDMs available on the market. It is beyond the scope of this guide to describe the use of each MDM product and version. Instead, it shows the major steps required. Accomplishing these steps on your specific MDM product is required.

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

Procedure 1 Access Mobility Device Manager

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

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

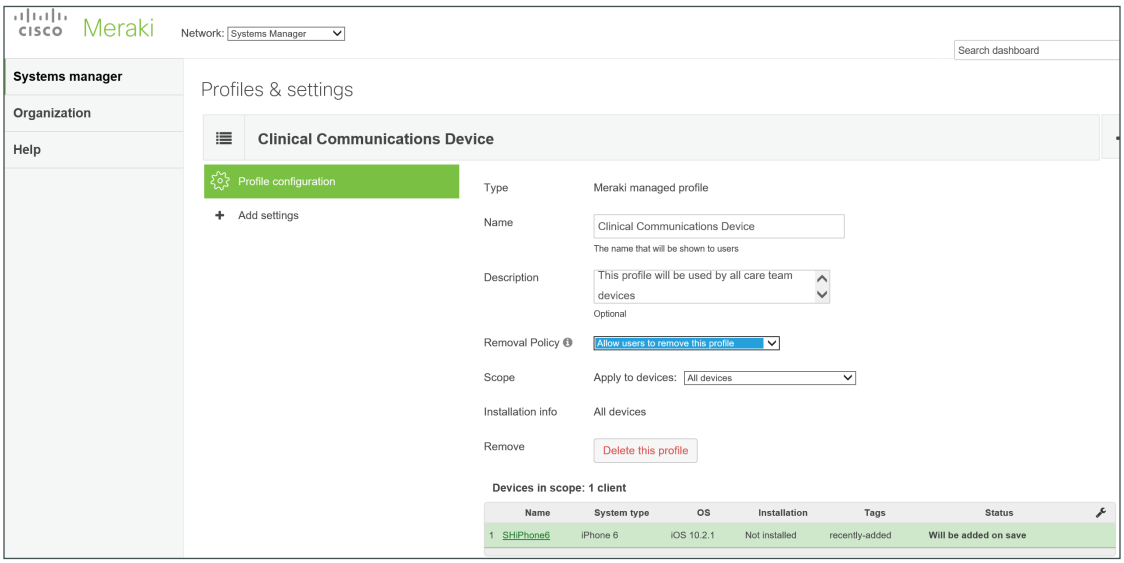


Step 3: If no profile exists within the Meraki System Manager, create a profile by clicking **Create a profile.**

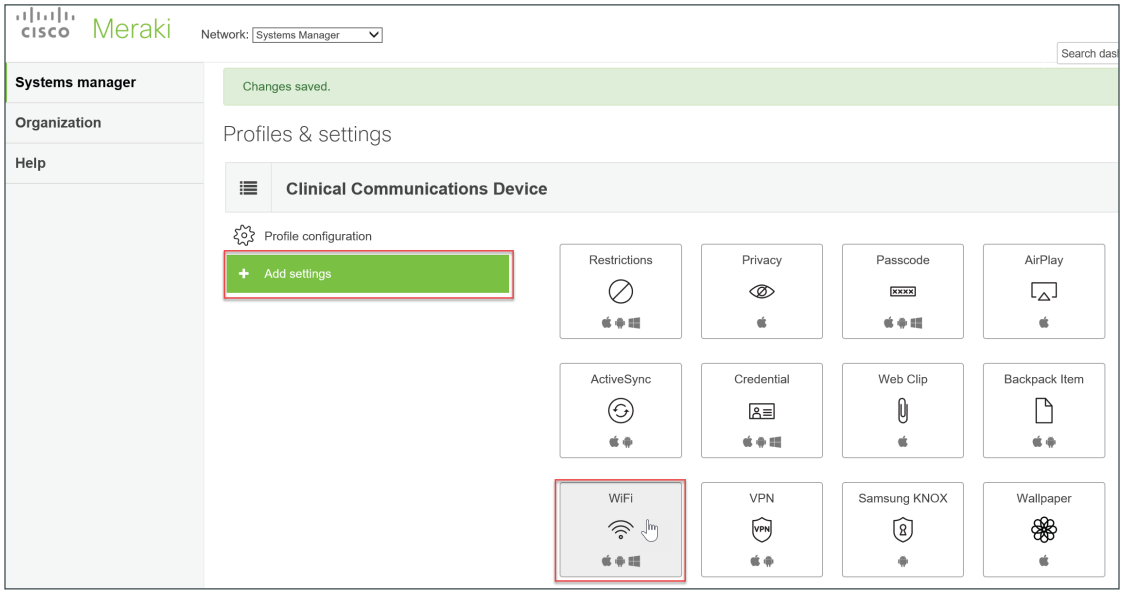
Step 4: Depending on your installation type (Meraki Managed Profile with or without Apple User Scoping), click **Create new profile.**

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**.

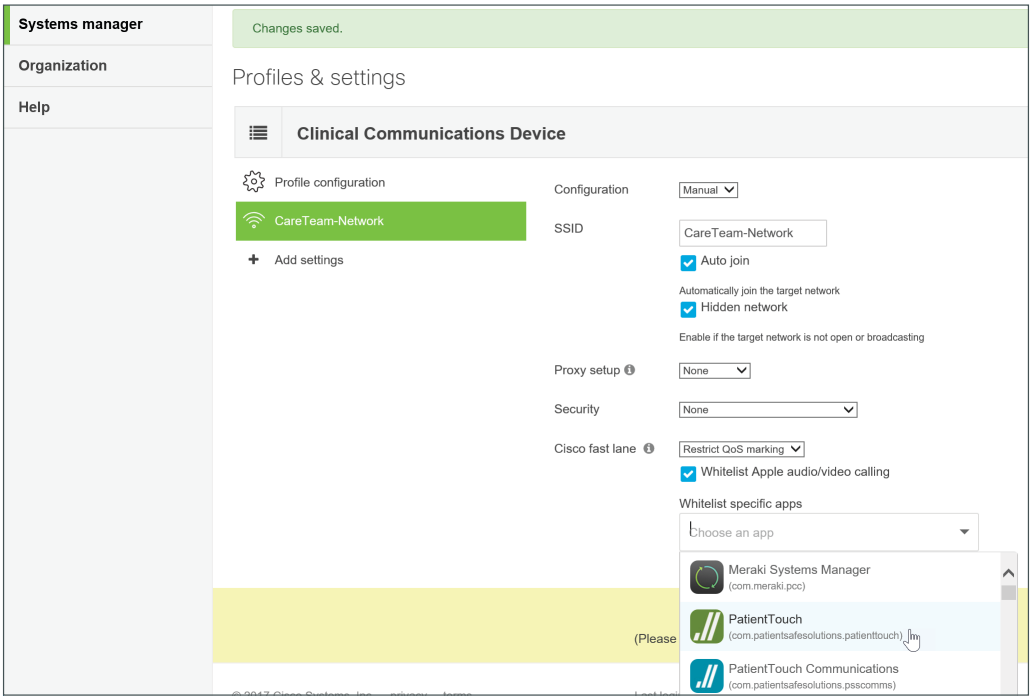


Step 6: Select the **Add settings** option to create a specific Wi-Fi policy, and then select the WiFi icon.



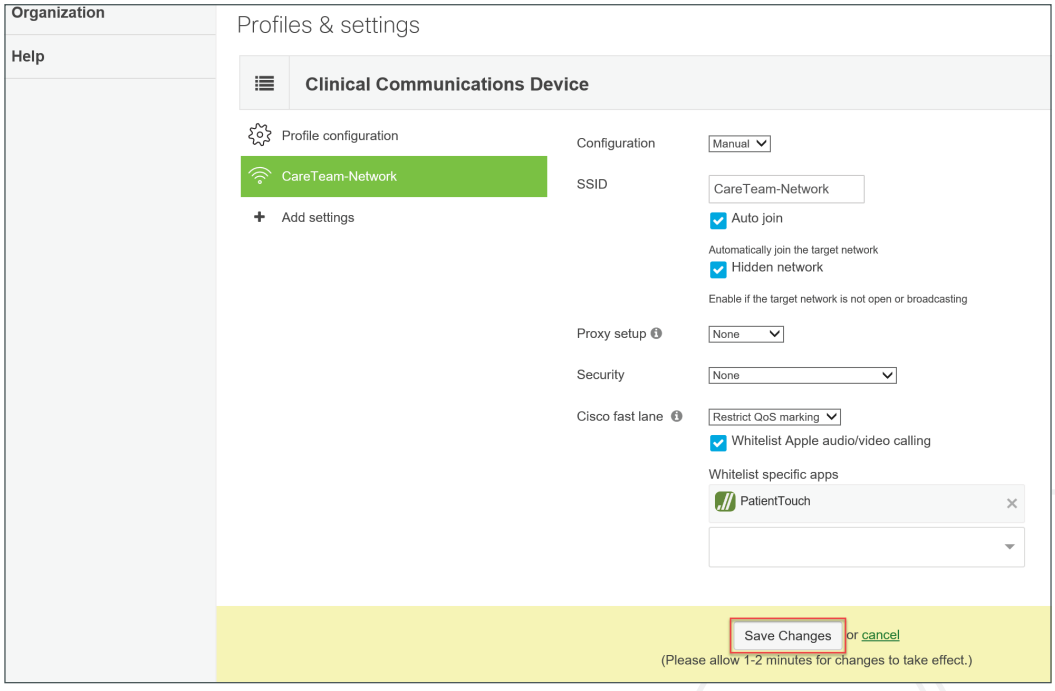
Step 7: Specify the SSID that the Clinical Communication end users will use to connect to the Wi-Fi network (example: CareTeam-Network). Optionally select **Auto Join** if you want the mobile device to automatically join the network. If the network is hidden from SSID advertisement, select **Hidden Network**. Select the appropriate security level for this SSID. Under **Cisco Fastlane**, 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: Select **Save Changes.**



PROCESS

Verifying End-to-End QoS

1. 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 PatientSafe application suite
- Any WAN link hub or spoke routers
- Hypervisor-based QoS

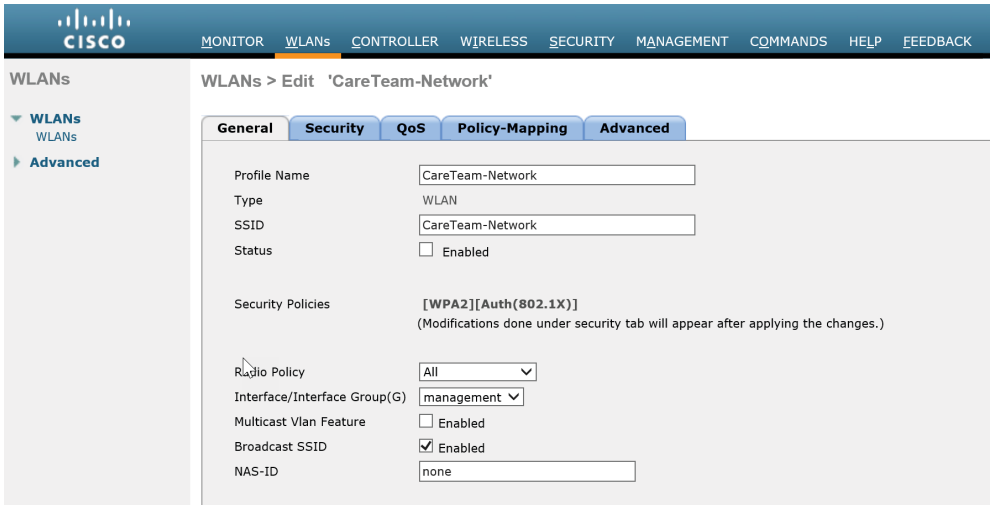
It is beyond the scope of this document to investigate and provide guidance on each infrastructure component in the list above. Because the WLC is a key component to Fastlane, the following section provides guidance on the WLC QoS configuration. For all other infrastructure components listed above, it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

Procedure 1 WLC QoS

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

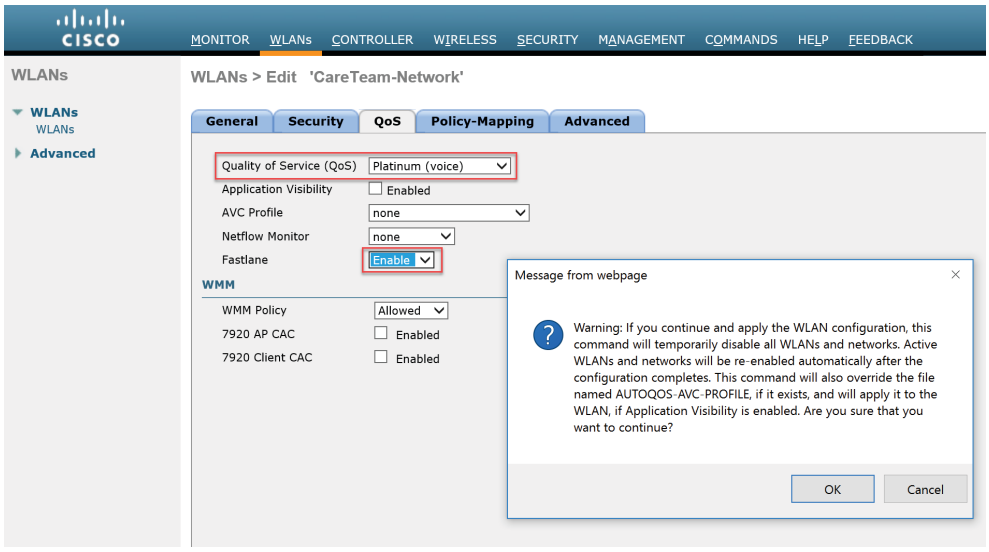
Step 2: On the WLC menu, select **MONITOR**, click **Advanced**.

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).



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

You have two options for verifying that Fast lane is operational. The first is to use the Cisco Fast Traffic application to ensure that Fast lane has been enabled on the WLAN being used by the Clinical Communication team.

The second and more precise option is to perform an RF packet capture of an iOS device that has the Patient-Touch 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.

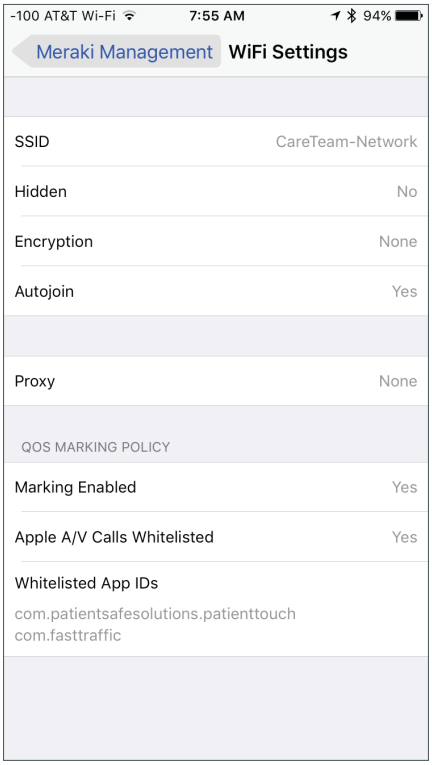
Procedure 1 Verify Fast lane is operational

Option 1: Use the Fast traffic App

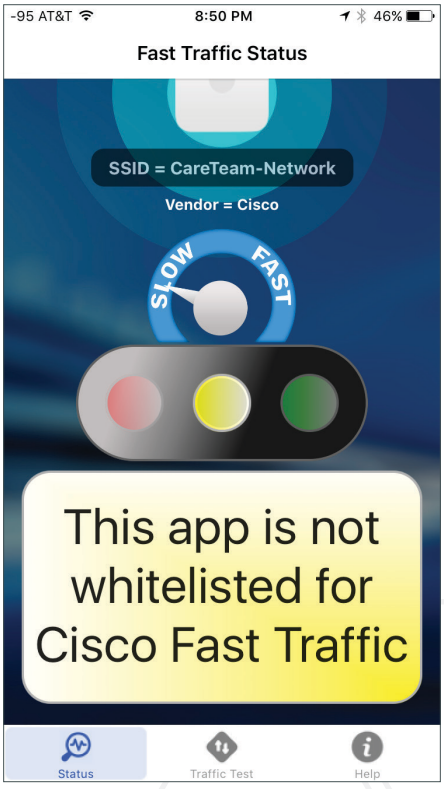
Step 1: From the Apple App Store, download and install the Cisco Fast Traffic application on to an iOS device.

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

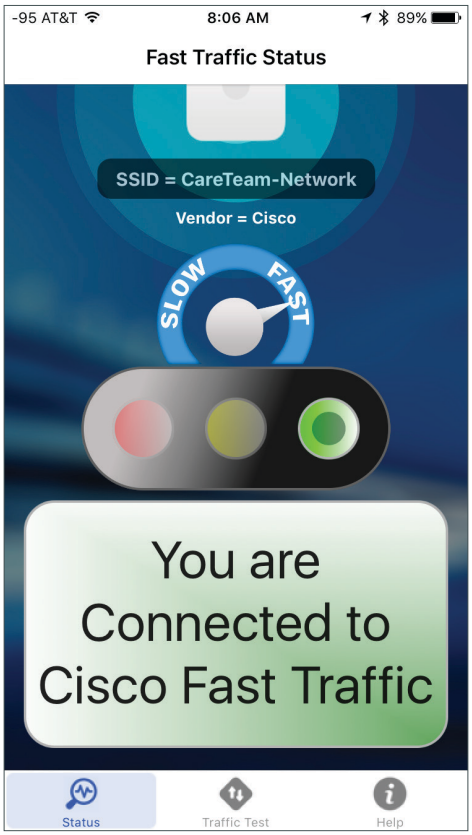
Step 3: On the iOS device, verify that the Wi-Fi policy is correct by navigating to **Settings > General > Device Management > Meraki Management > More Details > WiFi Settings.**



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 White List, 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 iOS device is associated.

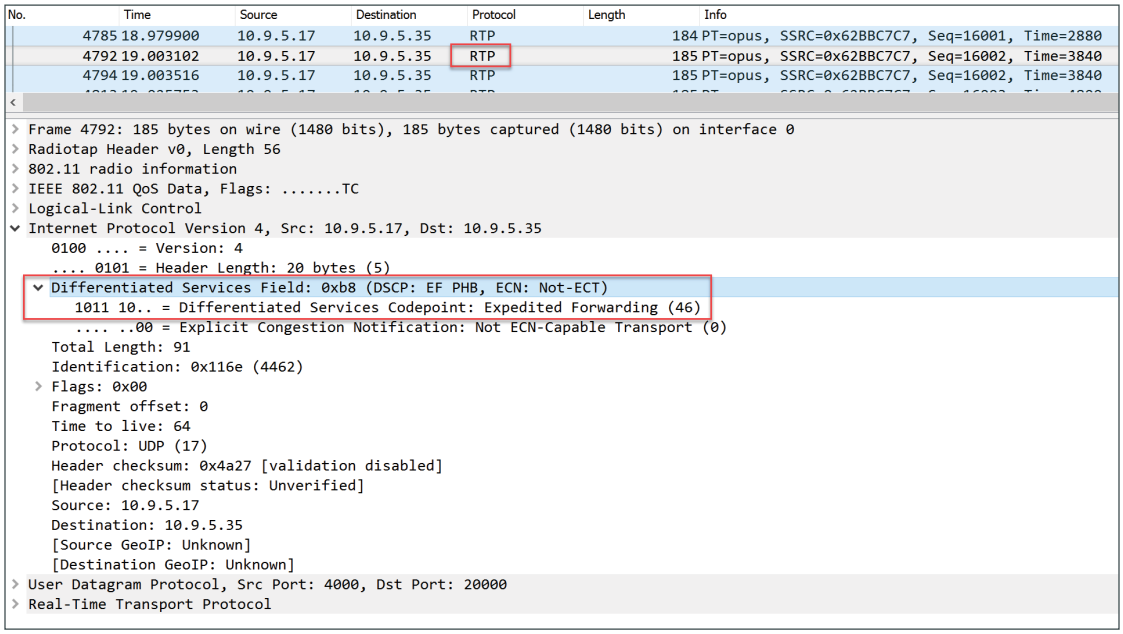
Step 3: From the WLC, determine which channel is in use by the access point.

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 PatientTouch application and place a call to any other handset.

Step 6: Stop the capture, and using WireShark or other 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)



Tech Tip

Creating a blacklist that does not contain the PatientSafe 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	PatientTouch	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.