



Wireless Voice Deployment Guide

This article is a guide to optimize Quality of Service (QoS) for wireless Voice over IP applications on Meraki MR wireless access points. Voice over IP (VoIP) has replaced telephones in enterprise networking with IP-based phones. While the majority of desk phones using VoIP require ethernet, there are many voice applications and wireless VoIP phones that operate over WiFi.

The Meraki MR series of WiFi access points have been tested by Cisco Meraki to provide the highest quality VoIP experience when using Cisco Jabber, Microsoft Lync, Microsoft Skype for Business, Broadsoft, Cisco 7900 Series phones, SpectraLINK phones, Ascom phones, Cisco phones, and Apple iPhones. This guide will provide recommendations for optimizing voice quality followed by product specific recommendations.

Measuring Voice Quality

By following this guide, you can significantly improve quality of service for the wireless voice applications and reduce or eliminate dropped calls, choppy speech, fuzzy speech, buzzing, echoing, long pauses, one-way audio, and issues while roaming between access points.

To develop this guide, we performed testing using Microsoft Lync's Pre-Call Diagnostics Tool. The endpoints used during testing were Macbook Pros running Office 365's Cloud-hosted Skype for Business Online, also known as Lync Online. All tests were performed while connected to an MR32 access point inside Meraki's headquarters in San Francisco, a high density corporate WiFi network. This tool measures 3 key metrics for voice quality:

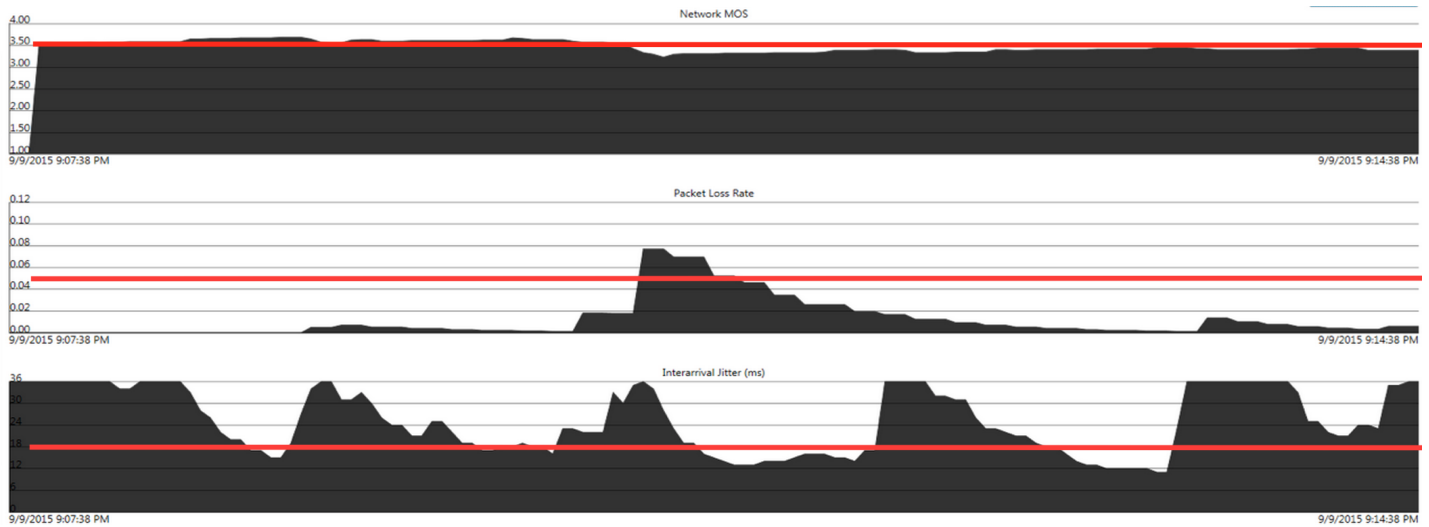
- **Network MOS** - The Network Mean Opinion Score (MOS) is the network's impact on the listening quality of the VoIP conversation. The score ranges from 1 to 5, with 1 being the poorest quality and 5 being the highest quality.
- **Packet Loss Rate** - The packet loss rate is the percent of packets that are lost during transmission.
- **Interarrival Jitter** - Interarrival jitter measures the variation in arrival times of packets being received in milliseconds (ms).

By combining this guide with best practices for configuring your client device configuration, application servers, WAN links, and wired network, you can measure and improve quality voice end-to-end. For more information on configuring your wired network to support Voice, please visit the article on [Configuring MS Access Switch for Standard VoIP deployment](#) article.

Voice quality before this guide

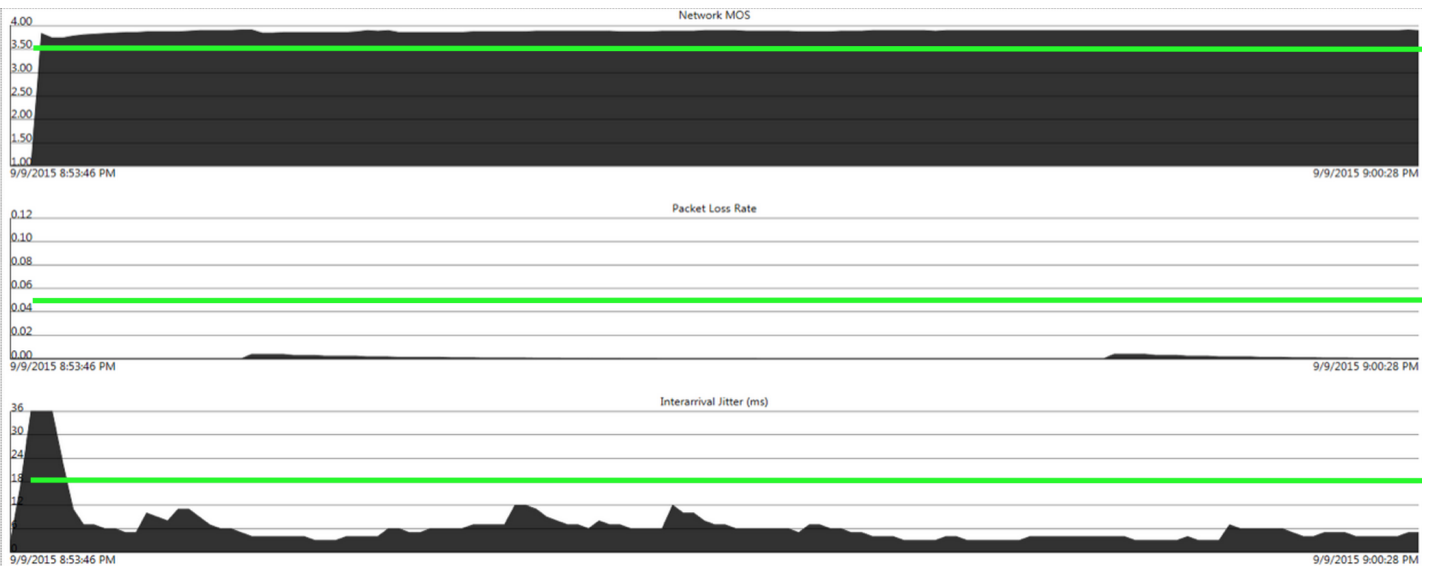
With the default settings on the MR, we see the baseline for quality. Voice calls with Lync on this network would be acceptable to some users, but not acceptable to others. The results of the Lync testing show that the Network Mean Opinion Score (MOS) drops below 3.5. Values dropping below 3.5 are termed unacceptable by many

users. The packet loss jumps to 8 percent during a period of network congestion simulated by running a speed test. Jitter fluctuates from 12 milliseconds to over 36 milliseconds. Cisco recommends a target of 10 ms of jitter and no more than 50 ms of jitter. Jitter is handled using buffering in voice/video applications, adding a small delay. The human ear normally accepts up to about 140 milliseconds of delay without noticing it.



Voice quality after this guide

After making the changes exactly as described in this guide, we see a significant improvement in voice quality. The MOS score approaches 3.9, the packet loss is near zero, and the jitter is consistently below 6 milliseconds and always below 12 milliseconds. As the call starts, traffic shaping kicks in automatically with prioritization and QoS tagging. A speed test was performed with no impact to the voice traffic - packet loss increased to 0.5% during the congestion.



Wireless Voice Best Practices

A Cisco Meraki wireless network has the intelligence built-in with deep packet inspection to identify voice and video applications and prioritize the traffic using queuing and tagging to inform the rest of the network how to handle your voice traffic. Below is a summary of the best practices to provide the best voice quality over wireless.

1. Perform a [pre-install RF survey](#) for overlapping 5 GHz voice-quality coverage with -67 dB signal strength in all areas.
2. If possible, create a new SSID dedicated to your voice over IP devices.
 - a. Set Authentication type to '[Pre-shared key with WPA2](#)'
 - b. Set WPA encryption mode to '[WPA2 only](#)'.
 - c. Enable '[802.11r](#)' fast roaming.
 - d. Enable '[5 GHz band only](#)'.
 - e. Set Minimum bitrate to '[12 Mbps](#)' or higher.
3. Enable [Bridge mode](#). If you cannot provide a VLAN across the entire floor, use [Layer 3 roaming](#).
4. Enable '[VLAN tagging](#)' and assign a VLAN dedicated to wireless voice. If you cannot dedicate an SSID to voice, assign a VLAN dedicated to wireless.
5. Set a '[Per-client bandwidth limit](#)' to 5 Mbps with '**Speed Burst**' to limit all non-voice traffic
6. Set a '[Per-SSID bandwidth limit](#)' to unlimited.
7. Enable '[Traffic shaping](#)' on the SSID to prioritize all voice traffic
 - a. Create a traffic shaping rule for '**All voice & video conferencing**'
 - b. Add '**Custom expressions**' for the IP and ports used by your servers hosting Microsoft Lync / Skype for Business, Jabber, or Spark
 - c. Set the Per-client bandwidth limit to '**Ignore SSID per-client limit (unlimited)**' from the drop down.
 - d. Set PCP to '6'
 - e. Set DSCP to '**6 (WMM Voice)**'
8. [Verify the Voice VLAN](#) is tagged correctly.
9. Verify your uplinks and [Switches have Quality of Service defined](#) with the maximum PCP and DSCP values
10. Verify DSCP trust is enabled on switch ports to APs and uplinks
11. Verify your Windows Group Policy to ensure your devices are tagging application traffic with DSCP (not on by default)
12. Verify your voice server configuration to ensure Microsoft Lync / Skype and Call Manager have DSCP enabled (not on by default)

Summary of 802.11 Standards

All Meraki MR series access points support the most recent 802.11 standards implemented to assist devices to roam between access points and ensure voice calls maintain a quality user experience.

- [802.11r](#): Fast BSS transition to permit fast and secure hand-offs from one access point to the other in a seamless manner
- [802.11i](#): Enabling client devices authenticated via 802.1x to authenticate with decreased latency whilst roaming

- [802.11k](#): assisted roaming allows clients to request neighbor reports for intelligent roaming across access points.
- 802.11e: Wireless Multimedia Extensions (WMM) traffic prioritization ensures wireless VoIP phones receive higher priority.
- WMM Power Save: maximizes power conservation and battery life on devices without sacrificing Quality of Service.
- 802.11u: Hotspot 2.0 also known as Passpoint is a service provider feature that assists with carrier offload.

Pre-Install Survey

The design and layout of access points is critical to the quality of voice over WiFi. Configuration changes cannot overcome a flawed AP deployment. In a network designed for Voice, the wireless access points are grouped closer together and have more overlapping coverage, because voice clients should roam between access points before dropping a call. Designing with smaller cells and lower power settings on the access point are key elements to ensure the overlapping coverage from neighboring APs/cells. Set a clear requirement based on the device type when performing a survey.

Pre-site surveys are useful for identifying and characterizing certain challenging areas and potential sources for interference, such as existing WiFi networks, rogues, and non-802.11 interference from sources such as microwave ovens and many cordless telephones. Post-site surveys should be performed at least 48 hours after installation to allow the network to settle on channel and power settings.

- Prefer 5 GHz coverage for voice applications due to the lower noise floor compared to 2.4 GHz
- Verify an AP can be seen from the phone at -67 dBm or better in all areas to be covered
- Verify that the AP sees the phone at -67 dBm or better in all areas as well
- Signal to Noise Ratio should always 25 dB or more in all areas to provide coverage for Voice applications
- Channel utilization should be under 50%

For more guidelines on site surveys read our article on [Performing a Wireless Site Survey](#). For more detailed guidelines on designing RF specifically for Cisco Voice over WiFi please read Cisco's [Voice over WLAN Guide](#).

Network Configuration

Making the changes described in this section will provide a significant improvement in voice quality and user satisfaction by following the best practices for configuring your SSIDs, IP assignment, Radio Settings, and traffic shaping rules.

Add a dedicated Voice SSID

Voice optimization typically requires a different configuration including access control and traffic shaping to address device specific recommendations. You should create a separate Voice SSID for devices dedicated to voice applications. While this is not a requirement, we recommend to create a separate network to follow this guide. In networks with VoIP handsets from two different manufacturers, it is common to create two voice SSIDs.



If you plan to deploy more than 4 SSIDs please read our guide on the [Consequences of Multiple SSIDs](#).

Authentication type

Voice over WiFi devices are often mobile and moving between access points while passing voice traffic. The quality of the voice call is impacted by roaming between access points. Roaming is impacted by the authentication type. The authentication type depends on the device and its supported auth types. It's best to choose the auth type that is the fastest and supported by the device. If your devices do not support fast roaming, Pre-shared key with WPA2 is recommended. WPA2-Enterprise without fast roaming can introduce delay during roaming due to its requirement for full re-authentication. When fast roaming is utilized with WPA2-Enterprise, roaming times can be reduced from 400-500 ms to less than 100 ms, and the transition time from one access point to another will not be audible to the user. The following list of auth types is in order of fastest to slowest.

1. Open (no encryption)
2. Pre-shared key with WPA2 and Fast roaming
3. WPA2-Enterprise with Fast roaming
4. Pre-shared key with WPA2
5. WPA2-Enterprise

WPA2 only for Encryption mode

Voice devices can benefit from having a single type of encryption used. By default, SSIDs on Cisco Meraki access points that are configured as WPA2 will utilize a combination of both WPA1 TKIP and WPA2 AES encryption. WPA2 (AES) is recommended and required in order to utilize caching or fast roaming. The WPA encryption setting is SSID specific, and can be found on the Wireless > Configure > Access control page.

- If all Voice devices support WPA2, the 'WPA2 only' option is recommended for Voice over IP devices.
- If the device does not support AES, it is also possible to force TKIP only. Please [contact Cisco Meraki support](#) to configure this option.

For step-by-step instructions on changing the WPA encryption mode, see our document on [Setting a WPA Encryption Mode](#).

WPA encryption mode

WPA2 only

802.11r

Enabled

802.11r fast roaming

Enabling 802.11r is recommended to improve voice quality while roaming. The 802.11r standard was designed to improve [VoIP](#) and voice applications on mobile devices connected to Wi-Fi, in addition to or instead of cellular networks. When mobile devices roam from one area to another, they disassociate from one access point and reassociate to the next access point. Enabling 802.11r benefits VoIP devices by reducing the roaming time spent changing between access points. Some client devices are not compatible with Fast BSS Transition (802.11r). You may wish to check your devices for compatibility.

This feature can be enabled from the Configure > Access control page under Network access > 802.11r. If this option does not appear, a [firmware update may be required](#). For more details on 802.11r, refer to our guide on [Fast Roaming Technologies](#)

Layer 2 and Layer 3 Roaming

Bridge mode is recommended to improve roaming for voice over IP clients with seamless Layer 2 roaming. In bridge mode, the Meraki APs act as bridges, allowing wireless clients to obtain their IP addresses from an upstream DHCP server. Bridge mode works well in most circumstances, particularly for [seamless roaming](#), and is the simplest option to put wireless clients on the LAN. To configure the client IP assignment modes please refer to our document on [SSID Modes for Client IP Assignment](#).

When using Bridge mode, all APs on the same floor or area should support the same VLAN to allow devices to roam seamlessly between access points. Using Bridge mode will require a DHCP request when performing a Layer 3 roam between two subnets. For example, when a user on a VoIP call roams between APs on different VLANs without layer 3 roaming, the user's session will be interrupted as the external server must re-establish communication with the client's new IP address. During this time, a VoIP call will noticeably drop for several seconds, providing a degraded user experience.

Large wireless networks with multiple VLANS per floor may require IP session roaming at layer 3 to enable application and session persistence while a mobile client roams across multiple VLANs. With layer 3 roaming enabled, a client device will have a consistent IP address and subnet scope as it roams across multiple APs on different VLANs/subnets. If Layer 3 roaming is required on your network, please refer to our [article on Layer 3 Roaming](#).



Note: It is strongly recommended to consult with a Cisco Meraki SE or Cisco Partner when considering layer 3 roaming options.



NAT mode is not recommended for Voice over IP: With NAT mode enabled, your devices will request a new DHCP IP address on each roam. Moving between APs in NAT mode will cause the connection to break when moving AP to AP. Applications requiring continuous traffic streams such as VoIP, VPN or media streams will be disrupted when roaming between APs.

Segregate traffic on a Voice VLAN

Voice traffic tends to come in large amounts of two-way UDP communication. Since there is no overhead on UDP traffic ensuring delivery, voice traffic is extremely susceptible to bandwidth limitations, clogged links, or even just non-voice traffic on the same line. Separating out your voice traffic allows it to function independently of other network traffic, and allows for more granular control over different types of traffic.

If a voice VLAN is specified on a Meraki MS switch, the port will accept tagged traffic on the voice VLAN. In addition, the port will send out LLDP and CDP advertisements recommending devices use that VLAN for voice traffic. The VLAN tagged on the wireless access point should match the Voice VLAN on your wired network. For more information, please visit the article on [Configuring MS Access Switch for Standard VoIP deployment](#) article.

VLAN tagging ⓘ

Bridge mode and layer 3 roaming only

Use VLAN tagging 

VLAN ID ⓘ

AP tags	VLAN ID	Actions
All other APs	<input type="text" value="132"/>	

[Add VLAN](#)

Band selection

The 2.4 GHz band has only 3 channels that do not overlap, while the 5 GHz band has up to 19 individual channels in the US. A wireless network will provide the best quality of service for wireless voice when designed correctly to support 5 GHz coverage for voice. This can be configured under [Access Control > Wireless options > Band selection > '5 GHz band only'](#). After configuration, testing should be performed in all areas of your environment. If you do not have proper 5 GHz coverage after a post-install site survey, you can manually increase the power on the 5 GHz radio in [Radio Settings > Channel Planning](#).

- Dual band operation (2.4 GHz and 5 GHz)
- 5 GHz band only
 - 5 GHz has more capacity and less interference than 2.4 GHz, but legacy clients are not capable of using it.
- Dual band operation with Band Steering
 - Band Steering detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients.

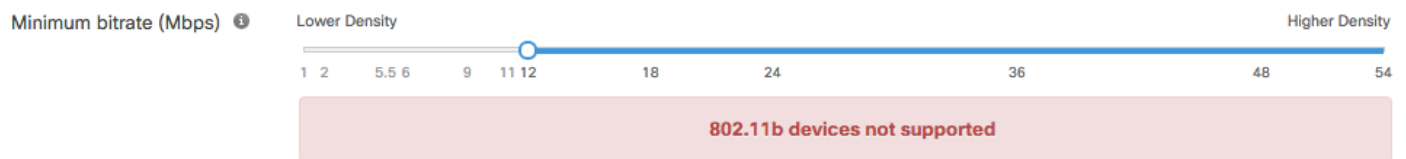
If you do not have a dedicated Voice SSID, enable '**Dual-band with band steering**' to enable your voice devices to use both 2.4 GHz channels and 5 GHz. Devices will be steered to use the 5 GHz band. For more details refer to the [Band Steering Overview](#) article. With a dual-band network, client devices will be steered by the network. However, to improve voice quality, please follow our guide on [configuring wireless band preference on client devices](#).

If you have devices that only support a 2.4 GHz network such as 802.11bgn devices, please contact [Meraki Support](#) to enable a 2.4 GHz only network.

Minimum bitrate

For Voice networks, **12 Mbps** is recommended as the minimum bitrate. Increasing this value requires proper coverage in the RF planning. An administrator can improve the performance of clients on the 2.4 GHz and 5GHz band by disabling lower bitrates. Adjusting the bitrates can reduce the overhead on the wireless network and also in some cases improve roaming performance.

This feature is configured under the Configure tab on the Access Control page on a per SSID basis. Management and Data frames will be sent out at the lowest selected rate. Clients must use either the lowest selected rate or a faster one.



Keep in Mind that selecting bitrates 12Mbps and above will prevent 802.11b clients from joining.

As you increase the minimum bitrate, clients need a higher signal to noise ratio to join and use the AP.



The highest recommended setting is 24Mbps unless specifically advised by a Cisco partner. Most environments and designs do not provide a great enough signal to noise ratio for the client to reliably decode all frames sent at a higher rate.

Bandwidth limits

Consider placing a per-client bandwidth limit on the rest of your network traffic. Prioritizing voice will have a greater impact if all other applications are limited. For more details refer to the article [Configuring Bandwidth Limitations and Enabling Speed Burst on Wireless Networks](#).

1. Go to **Wireless > Configure > Firewall & traffic shaping** and choose your SSID from the *SSID* drop down menu at the top of the screen.
2. Set a '**Per-client bandwidth limit**' to 5 Mbps with '**Speed Burst**'. This will apply to all non-voice application traffic. ***This step in the guide is optional.***

3. Set a '[Per-SSID bandwidth limit](#)' to unlimited.

Traffic shaping rules

Per-client bandwidth limit 5 Mbps [details](#) Enable SpeedBurst ⓘ

Per-SSID bandwidth limit ⓘ unlimited [details](#)



SpeedBurst enables a bursts of four times the allotted bandwidth limit for five seconds.

Traffic shaping rules

Use traffic shaping to offer voice traffic the necessary bandwidth. It is important to ensure that your voice traffic has enough bandwidth to operate. As such, traffic shaping rules can be implemented to allow voice traffic to use additional bandwidth, or limit other types of traffic to help prioritize voice traffic.

1. Go to **Wireless > Configure > Firewall & traffic shaping** and choose your SSID from the *SSID* drop down menu at the top of the screen.
2. Click the drop down menu next to *Shape traffic* and choose **Shape traffic on this SSID**, then click **Create a new rule**.
3. Click **Add +** and select '**All voice & video conferencing**'
4. Set Per-client bandwidth limit to '**Ignore SSID per-client limit (unlimited)**' and click Save changes.

Rule #1

Definition

This rule will be enforced on traffic matching any of these expressions.

All VoIP & video conferencing × [Add +](#)

Per-client bandwidth limit

Ignore SSID per-client limit (unlimited) ⇅

PCP / DSCP tagging

7 (highest priority) ⇅ / 7 (WMM Voice) ⇅

PCP, DSCP, and WMM tagging

Many devices support Quality of Service (QoS) tags to maintain traffic priority across the network. Meraki MR access points support WMM to improve the performance of real-time data such as voice and video. WMM improves the reliability of applications in progress by preventing oversubscription of bandwidth. WMM accomplished this by enhancing the prioritization of traffic using the access categories: voice, video, best effort, and background data.

1. Go to **Wireless > Configure > Firewall & traffic shaping** and choose your SSID from the *SSID* drop down menu at the top of the screen.

2. Under the traffic shaping rule for '**All voice & video conferencing**', set the **PCP / DSCP tagging** values to the highest value and click Save changes.
3. Set PCP to '**6**' or the setting recommended by your device/application vendor
4. Set DSCP to '**6 (WMM Voice)**' or the setting recommended by your device/application vendor



For QoS prioritization to work end to end, ensure that upstream networking equipment supports QoS prioritization as well. The PCP and DSCP tags applied on the wireless access point should match the wired network configuration to ensure end-to-end QoS. For more information, please visit the article on [Configuring MS Access Switch for Standard VoIP deployment](#) article.

Custom traffic shaping

If your voice traffic does not match the built-in application signatures or is not listed, you can create your own signature for traffic shaping.

1. Add the IP and ports used by your servers hosting Microsoft Lync / Skype for Business, Jabber, Spark, or other voice application.
 - a. In the **Definition** field click **Add +** and **Custom expressions**
 - b. In the text field, enter the IP address of each of your voice servers for example **172.16.1.123** or a range of server IPs **172.16.1.0/24**
 - c. Also, add your servers as source addresses by using the CIDR notation **localnet:172.16.1.123/32** for an individual server, or **localnet:172.16.1.0/24** for a range of IPs.
 - d. Click the **Add +** button again when finished.
2. If you have a dedicated voice SSID and dedicated voice VLAN add the local subnet of the client devices.
 - a. In the **Definition** field click **Add +** and **Custom expressions**
 - b. In the text field, enter **localnet:192.168.0.1/16** indicating the source subnet of your client devices in [CIDR](#) notation.
 - c. Click the **Add +** button again when finished.
3. Set Per-client bandwidth limit to '**Ignore SSID per-client limit (unlimited)**' and click Save changes.

Product Specific Recommendations

Cisco Meraki works closely with device manufacturers, for example Apple, to provide them with their own access points for interoperability testing. Meraki performs our own testing across the entire spectrum of devices and our customer support team handles and reports bugs quickly. This section will provide recommendations based on real-world deployments by Meraki customers combined with the best practices developed by Meraki and the vendors mentioned below.

Microsoft Lync / Skype for Business

This section will provide guidance on how to implement QoS for Microsoft Lync and Skype for Business. Microsoft Lync is a widely deployed enterprise collaboration application which connects users across many types of devices. This poses additional challenges because a separate SSID dedicated to the Lync application may not be practical. When you install Microsoft Lync Server / Skype for Business, Quality of Service (QoS) will not be enabled for any devices used in your organization that use an operating system other than Windows. For more guidance on deploying Lync over Wi-Fi, please read Microsoft's deployment guide, [Delivering Lync 2013 Real-Time Communications over Wi-Fi](#).

Meraki's deep packet inspection can intelligently identify Lync calls made on your wireless network and apply traffic shaping policies to prioritize the Lync traffic - using the SIP Voice protocol. In addition to the Meraki built-in signatures for Skype and SIP, you should also identify each Lync server by IP and any custom ports used by your Lync clients or servers. Follow these steps to configure your traffic shaping rules for Lync / Skype.

1. Go to **Wireless > Configure > Firewall & traffic shaping** and choose your SSID from the *SSID* drop down menu at the top of the screen.
2. Click the drop down menu next to *Shape traffic* and choose **Shape traffic on this SSID**, then click **Create a new rule**.
3. Consider setting a '**Per-client bandwidth limit**' to 5 Mbps with '**Speed Burst**'. This will apply to all non-voice application traffic
4. Set Per-client bandwidth limit to **unlimited**
5. Create a traffic shaping rule for **All voice & video conferencing > 'Skype' and 'SIP (Voice)'**
6. Set the Per-client bandwidth limit to '**Ignore SSID per-client limit (unlimited)**' from the drop down.
7. Set PCP to '**6**'. The 802.1p parameter is no longer supported in Lync Server 2013. The parameter is still valid for backward compatibility with Microsoft Lync Server 2010; however, it has no effect on devices used with Lync Server 2013.
8. Set DSCP to '**6 (WMM Voice)**'
9. Add '**Custom expressions**' for the IP and ports used by your servers hosting Microsoft Lync / Skype for Business
 - a. For Cloud-hosted Lync / Skype, add the domain names from the table below
 - b. Add the Port numbers from the table below or your own list of assigned port numbers
 - c. Add the IP address of each of your on-premise Lync servers
10. You can test that DSCP markings are applied using the Meraki packet capture tool.

Lync Online / Skype for Business Online servers	On Premise Lync / Skype for Business Servers
<ul style="list-style-type: none"> • lync.com 	<ul style="list-style-type: none"> • 172.16.1.123 (Destination IP)

<ul style="list-style-type: none"> • <code>skype.com</code> • <code>outlook.com</code> • <code>onmicrosoft.com</code> • 5060-5064 • <code>cloudapp.net</code> • 5070-5072 • <code>sharepoint.com</code> • 5086-5087 • <code>officedn.microsoft.com</code> • 8058-8061 • <code>microsoftonline.com</code> • 49152-57500 • <code>microsoftonline-p.com</code> • <code>verisign.com</code> 	<ul style="list-style-type: none"> • <code>172.16.1.0/24</code> (Destination IP range) • <code>localnet:172.16.1.123/32</code> (Source IP) • <code>localnet:172.16.1.0/24</code> (Source IP range)
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



The ports provided in the above table are the standard ports provided by Microsoft. Enabling QoS Configuration of the client device to modify the port ranges and assign the DSCP value 46. Microsoft's best practices include configuring the port ranges on both your servers and client devices. For details on enabling QoS, refer to Microsoft's article [Managing Quality of Service \(QoS\) in Lync Server 2013](#).

Cisco 7925G Phones

Cisco 7925G, 7925G-EX, and 7926G VoIP phones require specific settings to inter-operate with Meraki MR access points configured with WPA2-PSK association requirements. For more in-depth information on integrating Cisco 792xG with MR Access Points, see the [Cisco Unified Wireless IP Phone 792xG + Cisco Meraki Wireless LAN Deployment Guide](#).

1. Cisco recommends to set band selection to **5 GHz only**.
2. Do not utilize the Dual band operation with Band Steering option. If the 2.4 GHz band needs to be used due to increased distance, select Dual band operation (2.4 GHz and 5 GHz) should be selected.
3. Set the Minimum bitrate to 11 Mbps or higher.
4. Since voice and video RTP streams utilize the same UDP port range, it is recommended to use a different SSID for any video capable devices or do not apply the policy specified below.
5. By default, Cisco Meraki access points currently tag voice frames marked with DSCP EF (46) as WMM UP 5 instead of WMM UP 6 and call control frames marked with DSCP CS3 (24) as WMM UP 3 instead of WMM UP 4.
 - a. To tag voice frames as WMM UP 6, create a traffic shaping matching UDP ports 16384-32767 and select 6 (WMM Voice). With this rule, downstream RTP frames will be marked as DSCP 54.
 - b. To tag call control (SCCP) frames as WMM UP 4, create a traffic shaping matching TCP port 2000 and select 4 (WMM Video). If secure SCCPS is utilized, then match on TCP port 2443.


Rule #1

Definition

This rule will be enforced on traffic matching *any* of these expressions.

host 16384 - 32767  

Per-client bandwidth limit

Ignore SSID per-client limit (unlimited) 





PCP / DSCP tagging

Do not set PCP tag  / 6 (WMM Voice) 

Rule #2

Definition

This rule will be enforced on traffic matching *any* of these expressions.

SCCP (Skinny Call Control Protocol)  port 2000 
port 2443  

Per-client bandwidth limit

Ignore SSID per-client limit (unlimited) 

PCP / DSCP tagging

Do not set PCP tag  / 4 (WMM Video) 

Below is the QoS and port information for voice and call control traffic used by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G. For a full list of ports and protocols used by Cisco phones refer to the [Cisco Unified Communications Manager TCP and UDP Port Usage Guide](#).

Traffic Type	DSCP	PCP (802.1p)	WMM	Port Range
Voice (RTP, STRP)	EF (46)	5	6	UDP 16384 - 32767
Call Control (SCCP, SCCPS)	CS3 (24)	3	4	TCP 2000, TCP 2443



Cisco Unified Communications Manager only uses the port range 24576-32767 although other devices use the full range 16384 - 32767.

Apple iPhones

Apple and Cisco have created partnership to better support iOS business users by optimizing Cisco and Meraki networks for iOS devices and apps. For more information on this partnership, [please see Apple's website](#). Meraki's group policies can be easily configured to optimize Apple devices on a Meraki network. First create a group policy you would like to apply to Apple devices.



1. Browse to **Network-wide > Configure > Group Policies**, scroll down and click **Add Group**.
2. Under traffic shaping, create a new rule, and add **All VoIP & video conferencing**
 - a. Set the Per-client bandwidth limit to **Ignore network per-client limit**
 - b. Set PCP to **6 (highest priority)** and DSCP to **6 (WMM Voice)**.

3. Create a second rule, and add **All Video & music**
 - a. Set the Per-client bandwidth limit to **Ignore network per-client limit**
 - b. Set PCP to **5** and DSCP to **5 (WMM Video)**.

1  

Definition

This rule will be enforced on traffic matching any of these expressions.

All VoIP & video conferencing  

Per-client bandwidth limit

ignore network per-client limit (unlimited) 

unlimited  [details](#)

PCP / DSCP tagging

7 (highest priority)  / 7 (WMM Voice) 

2  

Definition

This rule will be enforced on traffic matching any of these expressions.

All Video & music  

Per-client bandwidth limit

ignore network per-client limit (unlimited) 


unlimited  [details](#)

PCP / DSCP tagging

5  / 5 (WMM Video) 













[Add a new shaping rule](#)

To apply your new Apple device group policy, browse to **Wireless > Access Control** and enable **Assign group policies by device type**. Click **Add group policy for a device type** for each Apple device type (iPhone, iPad, iPod, and Mac OS X) and assign the Apple device group policy you created. Click save and your optimization is complete.

Assign group policies by device type 

Enabled: assign group policies automatically by device type 

Groups for device types

Device type	Group policy	Actions
iPhone 	Apple Optimized 	
iPad 	Apple Optimized 	
iPod 	Apple Optimized 	
Mac OS X 	Apple Optimized 	

[Add group policy for a device type.](#)

Vocera Badges

Vocera badges communicate to a Vocera server, and the server contains a mapping of AP MAC addresses to building areas. The server then sends an alert to security personnel for following up to that advertised location. Location accuracy requires a higher density of access points. In a high density deployment, you may need to reduce the transmit power of each AP manually to as low as 5 dB on all supported radios. Vocera provides additional documentation on deploying WLAN best practices to support Vocera badges. For more information download their document on [Vocera WLAN Requirements and Best Practice](#)



Some models of Vocera badges do not support 5 GHz or WPA2 AES encryption and require WPA1 TKIP. Please [contact Cisco Meraki support](#) to configure a WPA1 TKIP on your network.

Service Provider WiFi

Service providers are using WiFi to offload data from cellular networks to meet the ever-increasing demands of mobile device users. Two technologies enabling WiFi to meet this demand are WiFi calling and Hotspot 2.0.

WiFi Calling

Mobile network operators (MNOs) now allow their customers to place phone calls over Wi-Fi to save roaming costs and leverage WiFi coverage in buildings with poor cellular coverage. WiFi calling is expected to be supported by majority of mobile devices and MSPs by the end of 2015.

An Enterprise WiFi infrastructure handles more than just carrier voice traffic, and this limited spectrum is shared by other applications and services like Video streaming & Web Conferencing. The requirements for voice in terms of latency and jitter warrants a network with proper end-to-end QoS design & Voice optimizations that would optimize delivery of WiFi calling packets in the presence of other applications.

Hotspot 2.0

Hotspot 2.0 also known as Passpoint is a service provider feature that assists with carrier offloading. Part of the 802.11u amendment to the 802.11 standard additional information is included in Hotspot 2.0 configured SSIDs that Hotspot 2.0 client devices can analyze use to determine if it is able to join the network automatically.

Managed Service Providers (MSPs) can now take enable of Hotspot 2.0 options on the Cisco Meraki MR access points. Meraki allows MSPs to customize the Hotspot 2.0 SSID advertisements to allow their subscribers to easy roam between networks. Hotspot 2.0 options are only available to qualified Managed Service Providers. Please contact [Cisco Meraki Support](#) to check eligibility.

Troubleshooting VoIP

We have created a detailed article focused on troubleshooting VoIP on Meraki. Please visit the article: [VoIP on Cisco Meraki: F.A.Q. and Troubleshooting Tips](#)