Voice over IP (VoIP) is a common technology used in enterprise networks, allowing users on a network to make internal and outbound phone calls over the network. This article outlines a number of frequently asked questions regarding VoIP systems and technologies on Cisco Meraki networks, as well as some general troubleshooting tips and tricks.

Common Questions

The following section outlines answers to some common questions regarding VoIP on Cisco Meraki equipment.

How do I deploy VoIP with Cisco Meraki equipment?

Since Cisco Meraki equipment is designed with network standards in mind, VoIP deployments can typically be run alongside the network stack with no issues:

- **MX:** The MX security appliance functions as a standard stateful firewall, performing inter-VLAN routing for the network. Typically, since VoIP traffic is best segregated to its own VLAN, the MX may be configured with a dedicated voice VLAN (assuming the MX is configured as the network's inter-VLAN router).

  If the MX has been configured with multiple uplinks, especially if those uplinks are being aggregated, it may be prudent to ensure that voice traffic is only using a particular interface. This can be accomplished using uplink preferences under **Security appliance > Configure > Traffic shaping.**

  In addition, traffic shaping rules can be implemented to prioritize voice traffic above other traffic types. Furthermore, if the MX is responsible for DHCP and network phones support dynamic configuration options, the MX can be configured to use VoIP-specific DHCP options.

  For some additional reading on relevant MX configuration and features:

  - [Configuring VLANs on the MX](#)
  - [Traffic Shaping for Packet Prioritization](#)
  - [Configuring DHCP Options](#)
  - [Link Aggregation and Uplink Preferences](#)

- **MS:** Cisco Meraki switches are standards-based network switches, designed for the access and distribution layers of the network. On the access layer, access switchports can be configured with a "Voice VLAN," where the MS will use LLDP to advertise the voice VLAN's ID to the connected phone. This may not work for all VoIP hardware; the ideal configuration will depend on the specific phone in use, please refer to your phone documentation to determine optimal configuration at the access layer.

  If a layer-3 MS switch is performing inter-VLAN routing, configuration of a dedicated voice VLAN may be done on that switch.

  For some additional reading on relevant MS configuration and features:
VoIP Deployment on MS Access Switches
Layer 3 Configuration Overview

- **MR:** If some wireless voice infrastructure is needed, additional steps should be taken during wireless deployment to ensure a stable roaming environment. In particular, a wireless site survey is strongly recommended to ensure ideal placement and configuration of APs, thereby allowing for a clean RF environment for your wireless phones to roam.

  If the voice SSID is using enterprise 802.1X authentication (and the technology is supported by the wireless phone hardware), it may be beneficial to enable fast roaming (802.11r) on the MR access points to improve roaming times between access points.

  For some additional reading on relevant MR configuration and features:
  - Performing a Wireless Site Survey
  - Fast Roaming Technologies

---

**What are some VoIP best practices?**

Generally speaking, it is best to stick to the following best practices when deploying a VoIP system on any network:

- **Segregate voice traffic to its own 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.

- **Use traffic shaping to offer voice traffic the necessary bandwidth.**
  Due to the relatively large amounts of data that voice uses on the network, 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 even limit other types of traffic to help out voice.

- **Use Quality of Service to maintain prioritization**
  Many devices support Quality of Service (QoS) tags to maintain traffic priority across the network. It may be beneficial to tag your voice traffic with the appropriate tags, so it can be prioritized anywhere in the network in the event of a saturated link.
  For more information on QoS:
MS Quality of Service Defined

Traffic shaping rules

Rule #1

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

Bandwidth limit
Ignore network per-client limit (unlimited)

Priority
High

DSCP tagging
46 (EF - Expedited Forwarding, Voice)

Add a new shaping rule

• **Understand firewall and NAT configurations**

  In VoIP, there will typically be two types of flows: Bi-directional communication from phones to the Private Branch Exchange (PBX), and bi-directional communication directly between phone peers. Specifics will largely depend on the phone vendor and/or preference. As such, it is highly important to understand what the expected flow of traffic will be, and ensure that all firewalls have been configured accordingly.

  Furthermore, it is important to understand if traffic will pass through some form of NAT, and if so, what type of NAT is in use. The options and limitations of the network may make certain configuration types infeasible.

• **Avoid sending VoIP traffic over non-optimized links**

  As discussed above, VoIP traffic is extremely sensitive to fluctuations in data transmission. As such, plan voice deployments to avoid sending VoIP traffic over links with limited bandwidth/environmental factors (wireless mesh), or over the WAN (lack of control, much more potential for failure).

How do I configure the MX to meet my voice provider's requirements?

If using an external voice provider, a number of requirements/questions may be presented about the network. The following questions are commonly posed by voice providers regarding network capabilities:

• **Can Application-Level Gateway be enabled on the MX?**

  ALG is a technology that allows stateful firewalls to dynamically assign ports and broker communication through a NAT. The MX security appliance is a full-featured stateful firewall that does not have any ALG functionality. Depending on the PBX involved, there are several ways to establish communication without requiring ALG, please refer to your PBX documentation for options to deal with NAT.

• **Can the UDP timeout value be changed?**

  The MX does have a simple UDP timer function, which will drop a traffic flow after an extended period of inactivity. This timer cannot currently be changed. However, a timeout would require both peers to be completely silent for an extended period of time in order to take effect. UDP communication between peers on an active call, for example, is...
highly unlikely to be dropped due to a timeout.

• **How are inbound connections handled?**
  The MX is a stateful firewall, so most inbound communication will only be allowed as a response to an established outbound conversation. Inbound communication can be explicitly allowed by means of port forwarding or 1:1 NAT/1:Many NAT rules, whereby a specific internal device is associated with a public port/IP. When considering how to implement a VoIP solution, it is important to note who will be initiating what communication; if an internal phone initiates a connection to an external PBX, the stateful firewall will allow the PBX's response back into the network. However, if an external PBX attempts to initiate a connection to an internal phone, it will be blocked unless there is a port forwarding or NAT rule allowing that communication.

For more information on port forwarding and NAT rules on the MX, please refer to the following articles:
  - Configuring 1:1 NAT
  - 1:1 NAT vs. Port Forwarding

---

**Troubleshooting**

The following section outlines some common VoIP issues that may arise, and some recommended troubleshooting steps to narrow down the issue.

**Audio only goes one way**

Consider that voice communication typically happens as two simultaneous UDP streams, one for each direction of communication. These are two separate streams, as opposed to a single two-way stream. If communication in one direction is not making it to the peer, then the symptom is usually that only one party can hear the other's audio.

To address this issue, check the following:

• Trace the flow of traffic, and check any firewalls to ensure they are not blocking traffic.

• If a stateful firewall like the MX is passing traffic between the two peers, ensure there are appropriate mechanisms in place to allow inbound communication (1:1 NAT, port forwarding, etc).

• If it's unclear exactly where the traffic is being dropped, determine based on the symptoms which direction of traffic seems to be failing, and take packet captures at network hops to see where the flow stops.

• If the PBX is configured to require an ALG (discussed above), and that traffic is going through an MX, it may be dropped in one direction. In this case, refer to the PBX-specific documentation for means to address NAT without ALG.

**Poor audio quality**

Due to the sensitive nature of VoIP traffic, low voice quality (or "jitter") may be experienced due to interruptions in traffic flow or bandwidth limitations.

To improve voice quality, ensure that the following best practices are in place:

• Make sure voice traffic is segregated to its own voice VLAN, so normal data cannot interfere.

• Check the network's bandwidth limitations and ensure there's enough bandwidth (as recommended/required by the
voice system).

- Use traffic shaping/QoS where necessary, in the event that a link on the network is being saturated.
- Take packet captures to get an idea of call quality, and where it is degraded. Many capture analysis tools, including Wireshark, have the ability to perform RTP analysis.

Take note of the "symptoms" exhibited in a poor quality phone call. Specific traits of the call can help narrow down the issue. Please refer to this guide for a breakdown of different call quality symptoms.

### Phones can't get an IP address/configuration

Typically, VoIP equipment will get a dynamic configuration from a TFTP server or other service on the network. This will commonly be levied by a DHCP server, where leases to VoIP endpoints will include voice-specific DHCP options. In the event that the phone fails to connect to the network/get a working configuration, consider the following recommended steps:

- If a separate voice VLAN is being used, ensure that phones are being put on the appropriate VLAN by means of an access port, voice VLAN configuration on the port, or even configured on the phone itself.
  - If this is being done, ensure that a DHCP server is up-and-running on that VLAN, and configured with the appropriate scope and options.
- If phones have a working IP configuration on the network (or a static assignment is given for test purposes) and are told to get their VoIP configuration from some other server, ensure that the server is online and reachable from the voice VLAN.

### Additional Resources

The following articles provide additional information not covered in this article, and may be helpful as a reference:

- [Cisco Meraki VoIP Deployment Guide](#)
- [Compatibility with Cisco 7925G VoIP Phone](#)
- [Troubleshooting: VoIP Phone Not Detecting Voice VLAN on MS Switch](#)
- [Verifying Voice and Data VLAN Tags](#)