Meetinghouse Network Troubleshooting Guide:

1. **Meraki MX64 Firewall**
2. **Meraki Switches**
   - 8 Port Meraki switches - MS120-8, MS120-8LP, MS120-8FP, MS220-8, MS220-8P
   - 24 Port Meraki switches - MS120-24, MS120-24P
   - 48 Port Meraki switches - MS120-48, MS120-48LP, MS120-48FP
3. **Meraki MR33 Wireless Access Points (APs) and Cisco APs**
   - Only Cisco or Meraki APs added through the TM portal are supported by the GSD, Network Operation, and Network Engineering.

Meraki Firewall Troubleshooting Guide:

After the Meraki switch(es) have been installed the Firewall ports will be configured to the following:
Meraki MX64 Ports:

Port 1 - Connected to an SFP Port on the Meraki Switch
Port 2 - Used during the switch installation to access TM
Port 3 - Disabled and no longer used
Port 4- Disabled and no longer used

1) Check the status indicator light on the Meraki MX64 device
   - **a) Status indicator is solid White**
     - i) Solid white indicates that the firewall has internet connectivity.
     - ii) Compare the serial number of the Meraki firewall in your meetinghouse with the serial number indicated in TM.
       - (1) If they do not match you will need to replace the firewall in TM with the one that is in the building
         - (a) Contact the Global Service Desk for assistance
       - (2) If the serial number does match the one registered to your building in TM then the Meraki firewall is likely functioning properly
         - (a) Connect a laptop or workstation directly to port 2 on the Meraki firewall and verify internet connectivity
         - (b) If you can access the internet when connected directly to port 2 on the firewall you will need to troubleshoot connectivity to the switch
         - (c) If you are unable to access the internet when connected directly to port 2 on the firewall, contact the Global Service Desk
   - **b) Status indicator is blinking white**
     - i) This indicates that the Meraki firewall is updating
       - (1) Generally, this is completed within a few minutes by may take 30 minutes or longer for a new firewall
       - (2) Firewalls typically reboot at the end of an update
       - (3) It is generally best to wait for the device to finish updating and transition to a solid white indicator

(4) The Meraki firewall will function normally during the update process

c) Status Indicator is Orange

i) Indicates that the device is booting
   (1) This is normal for one to two minutes after the device is powered up or rebooted

ii) A persistent Orange indicator, for more than five minutes indicates that the device is not functioning properly and should be rebooted
   (1) If the device continues in this state after rebooting, contact the Global Service Desk

d) Status indicator is cycling through colors (Referred to hereafter as the "Rainbow State")

i) Indicates that the device is fully booted and attempting to communicate with the Meraki cloud management application

ii) Once the device is in contact with the Meraki cloud management application, and has downloaded its current configuration file, the indicator will transition to white
   (1) Occasionally the device will require a reboot and transition back to Orange
   (2) If the indicator continues to alternate between the Rainbow cycle and solid orange every few minutes, it is unable to reach the Meraki cloud management application
      (a) Verify the connection requirements with your Internet Service Provider
         (i) Please contact them to determine if there is a static IP address, or "PPPoE" that needs to be configured (this information may also be recorded in TM)
         (ii) Your ISP may ask you for a "MAC" address, you will find it printed on the label on the bottom side of your Meraki firewall
      (b) If a static IP address or "PPPoE" information is provided by your Internet Service Provider, contact the Global Service Desk for help configuring the firewall with these settings
      (c) If the Internet Service Provider does not provide PPPoE or a static IP address, reboot the Modem or router provided by the Internet Service Provider
      (d) If you are unable to resolve the problem after contacting your internet service provider, contact the Global Service Desk to receive help resetting the Meraki Firewall

Meraki Switch Troubleshooting Guide:

Users, APs and computers are not able to connect to the internet

A Meraki switch is connected to the Meraki Firewall or to another Meraki switch that is connected to the Meraki Firewall and devices still are not able to connect to the internet then do the following:

1) Check the LED status indicator light on the front panel of each Meraki switch:

a) **Solid White Switch Light** – Indicates that the switch is functioning properly

b) If users and APs are not able to connect to the internet and the switch LED indicator is Solid White then verify the following:
   (1) The Meraki switch is connected directly to the Meraki firewall
   (2) For 8 Port Meraki Switches - Switch Port SFP9 should be connected to Port 1 on the Meraki Firewall

(3) For 24 port Meraki switches - Switch Port SFP25 should be connected to Port 1 on the Meraki Firewall
(4) For 48 port Meraki switches - Switch Port SFP49 should be connected to Port 1 on the Meraki Firewall
(5) If an SFP port is not available or an SFP module is not available, then another switch port configured as "Link" in TM may be used to connect to the Meraki Firewall

c) If the Meraki switch is connected to another Meraki switch:
   (1) SFP ports should always be used to connect Meraki switches if they are available
   (2) If an SFP port is not available or an SFP module is not available, then another switch port configured as "Link" in TM may be used to connect to another Meraki Switch.
   (3) Avoid "daisy-chaining" switches whenever possible, there should never be more than one switch between the Meraki firewall and any other Meraki switch

d) **Solid Orange Switch light** – Indicates that the switch is booting or is unable to communicate with the Meraki cloud management application.
   1) After booting the indicator light should transition briefly to the "Rainbow" cycle
   2) After connecting to the Meraki cloud management application the switch may reboot and revert back to an Orange light.
   3) If the LED indicator continuously cycles between the solid Orange and the "Rainbow" state every few minutes, it is not able to communicate with the Meraki Cloud controller:
      (1) Verify the Meraki switch is connected directly to the Meraki firewall
      (2) For 8 Port Meraki Switches - Switch Port SFP9 should be connected to Port 1 on the Meraki Firewall
      (3) For 24 port Meraki switches - Switch Port SFP25 should be connected to Port 1 on the Meraki Firewall
      (4) For 48 port Meraki switches - Switch Port SFP49 should be connected to Port 1 on the Meraki Firewall
      (5) If an SFP port is not available or an SFP module is not available, then another switch port configured as "Link" in TM may be used to connect to the Meraki Firewall.

   4) If the Meraki switch is connected to another Meraki switch:
      (1) SFP Ports should always be used to connect Meraki switches if they are available
      (2) If an SFP port is not available or an SFP module is not available, then another switch port configured as "Link" in TM may be used to connect to another Meraki Switch.
      (3) Avoid "daisy-chaining" switches whenever possible, there should never be more than one switch between the Meraki firewall and any other Meraki switch

   5) If the indicator stays Orange persistently the device should be rebooted
      (1) To reboot the switch: 1) Disconnect the power from the device, 2) wait at least ten seconds, 3) reconnect the power.
      (2) If the Meraki switch is properly connected to the Meraki Firewall and the switch ports are configured correctly in TM and the indicator light remains Orange even after rebooting the switch, then contact the Global Support Desk for assistance resetting the switch to its factory default settings.

e) **Blinking White Switch light**
   (1) Indicates that the Meraki firewall is updating
   (2) Generally, this is completed within a few minutes but may take 30 minutes or longer for a new switch
   (3) Switches typically reboot(will go orange briefly) at the end of an update
   (4) It is generally best to wait for the device to finish updating and transition to a solid white indicator
   (5) The Meraki switch will function normally during the update process

Devices connected to existing switches are unable to access the internet, or are in the wrong zone:

1. Verify that the switch is online, LED indicator on the front of the switch should be solid white.
2. If the LED indicator is not solid white please follow the troubleshooting steps above to restore the switch to normal operation.
3. Verify that each switch port in TM is correctly configured. The default setting for a switch port is "Public."
4. **Devices typically found in the Public Zone include:**
    a. Clerk Computers and unit leader computers
    b. Cisco APs
        i. Any wireless access point that is not managed by TM (use of such devices is not recommended, please contact your facility manager if more wireless access points are required for you building).
    c. Webstats, Sprinkler Controllers, Alarms, etc. that are managed through the internet (Contact your facility manager if you're unsure about any of these devices).
    d. Any resources that should be reachable by wireless users associated to "Liahona"
    e. Printers, and devices used exclusively by wards, stakes, branches, and other local units belong in the Public Zone
    f. AV systems that are meant to be accessed from the public network
    g. Webcast devices
    h. Any devices not belonging to the Facility, Special Purpose, or Workforce Zones as indicated below

5. **Devices that belong in the Facility Zone should be connected to switch ports configured for "Facility" in TM. Devices typically found in the facility zone include:**
    a. Webstats (some HVAC controllers are managed over the internet and may be placed in the "Public" zone, contact your facility manager to determine which zone your HVAC gear belongs in)
    b. Door locking systems
    c. Sprinkler Controllers
    d. Fire Alarms
    e. AV Equipment
    f. Any system that is managed remotely over the network by the Facility Manager.

6. **Devices that belong in the Special Purpose Zone should be connected to switch ports configured for "Special" in TM**.
    a. The Special Purpose Zone is generally deployed to support Family History Centers in meetinghouses. Any equipment associated with the Family History Center should be connected to the Special Purpose Zone.

7. **Devices that belong in the Workforce Zone should be connected to switch ports configured for "Workforce."**
    a. Workforce zones are only found in meetinghouses where Church employees have permanent dedicated workspace.
    b. "Workforce" should not be used to connect unmanaged switches, if there are not enough ports on the Meraki switch(es) to accommodate all of the switchports that are needed for Workforce users then additional Meraki switches should be added.

Wireless Access Points (AP) Troubleshooting Guide

- Only Cisco or Meraki APs added through the TM portal are supported by the GSD, Network Operation, and Network Engineering.

1) Meraki Access Points:

a) Access Points are offline, wireless is unavailable, or wireless users are unable to access the internet
   i) Verify that the Meraki Firewall is powered up and indicates that it is online.
      (1) Check the status indicator light and verify that it is solid white or blinking white.
         (a) If the Meraki firewall is not online, follow the process outlined in the Meraki firewall troubleshooting guide.
   ii) Verify that the Meraki Switch(es) is(are) powered up and indicate that they are online.
      (1) Check the status indicator light and verify that it is solid white or blinking white.
         (a) If the Meraki switch is not on-line, please follow the process outlined in the Meraki switch troubleshooting guide.
   iii) Verify that Meraki APs are in use and connected directly to a Meraki switch (Meraki MR33 or Legacy Cisco 1602 devices provided by CHQ are the only supported wireless solutions for meetinghouses).
      (1) Check the AP status light (follow this process for each Meraki AP in question):
         (a) Orange indicates that the device is booting. The orange light comes on as soon as the AP is powered up and may remain orange for a few minutes while it is booting.
            (i) Normal condition immediately after booting.
            (ii) From orange the next state is normally the Rainbow.
         (b) Rainbow (in this state the light will transition through several colors) indicating that the device is initializing its configuration and pulling information from Meraki's cloud controllers.
            (i) Under normal operation, once the AP has initialized and downloaded its configuration the next state is solid Green.
         (c) Blinking Blue indicates that the device is updating.
            (i) This is not a normal circumstance but does indicate that the AP is able to communicate with the internet and the Meraki cloud.
            (ii) Once the update is complete the AP will reboot and return to normal operation.
         (d) Green indicates that the AP is operational, but no clients are associated to it.
         (e) Solid Blue indicates that the AP is operational and has associated clients.
      (2) Status lights indicating error or problems with the AP:
         (a) An indicator that is permanently orange indicates that the device is not booting properly.
            (i) Power cycle the device by disconnecting it from the Meraki switch and reconnect it.
            (ii) If the error persists, contact the GSD.
         (b) An indicator that is continuously cycling between orange and rainbow indicates a problem with internet connectivity.
            (i) Verify that the device is connected directly to the Meraki switch. APs must be directly to the Meraki switch for proper functionality.
            (ii) Make sure that the port on the Meraki switch is properly configured for as an AP port in the TM switch management tool.
            (iii) If the AP is connected to a properly configured port on a Meraki switch and still cycling between Orange and Rainbow status lights, perform a factory reset on the AP.
            (iv) If the error persists, contact the GSD.
      (3) Status lights on the AP indicate normal operation (Solid Blue), but users are not able to reach the splash page or access the internet:

(a) Verify that users are joined to “Liahona” and not another SSID. Liahona is the only supported SSID for public access using Meraki APs.
(b) Verify that the user’s IP address is properly configured:
    (i) All devices connecting to meetinghouse networks should be set up for dynamic (DHCP) addressing.
        1. When connected to “Liahona” user ip addresses should be in the range 192.168.108.2-255, 192.168.109.0-255, 192.168.110.0-255, or 192.168.111.0-254.
        2. The default gateway on user devices should be 192.168.108.1.
        3. The subnet mask should be 255.255.252.0.
        4. DNS Servers must be set to 8.34.34.91, 8.34.34.92, 8.34.34.93, 8.35.35.91, 8.35.35.92, or 8.35.35.93. Other DNS servers are not permitted.
    (ii) Use the IP Address Reservation Tool in TM any time that a static reservation is needed.
    (iii) If the IP address is static and the above IP address requirements are not true for the client device(s), there is likely a rogue DHCP server on your network.
        1. Only one DHCP server can serve a network at any given time. You will need to find any devices acting as DHCP servers and remove or disable them.
    (iv) Incorrect IP addresses may also indicate that the meetinghouse network is being “spoofed”. This occurs when someone else creates a wireless network nearby using the same SSID and password hoping to get users to join unknowingly so that their experience can be impacted, or personal data compromised.
        1. Power off all APs in the meetinghouse and see if the SSID is still present.
(c) Verify that the AP is connected to the Meraki switch, and that the switch port is set to “AP” in the TM switch management tool.
    (i) Power injectors and in line switches are not permitted. Meraki APs must connect to Meraki switches to function properly.
    (ii) APs connected to switch ports configured for “Public”, “Special”, “Facility”, or “Workforce” may have normal status lights, but client traffic will not pass properly through the switch.

Users connect to the network and are unable to communicate on the network:

1. Verify that all Meraki hardware is online (white indicator lights on firewalls and switches, green or blue indicator lights on wireless access points)
2. Check the IP address settings on the devices that are unable to access the internet:
    1. For devices connected to the Public zone:
        1. IP Address – 192.168.X.Y
            - X is some number ranging from 108 to 111
            - Y is some number between 1 and 255.
                - If X is equal to 108, Y cannot be equal to 1
                - If X is equal to 111, Y cannot be equal to 255
        2. Subnet Mask – 255.255.252.0
        3. Default Gateway – 192.168.108.1
        4. DNS Servers – Vary depending upon the filter policy at the site:
            - Managed – 8.34.34.101, 8.35.35.101
            - Moderate – 8.34.34.102, 8.35.35.102
            - Strict – 8.34.34.103, 8.35.35.103
        5. If devices are unable to reach a DHCP server they will usually show an IP address beginning with 169

- Verify that Meraki APs are connected only to the Meraki switch(es), most switches found in meetinghouses cannot support the type of connection required for the Meraki APs in our current meetinghouse network design
- Verify that the ports on the Meraki switch used for wireless access points are configured for "AP" in TM

2. For devices connected to Special Purpose zones, Facility zones, and Workforce zones:
    6. IP addresses will vary from site to site, refer to TM to determine what IP address range your devices should use.
3. Rogue DHCP servers are the most common cause of invalid IP addresses:
    1. Most wireless routers and access points purchased from retail providers have a built in DHCP server built in which is enabled by default
    2. It is only permissible to have one DHCP server running on a given network
    3. Locate any other potential DHCP servers (i.e. wireless extender/repeater, 3rd party router installed downstream from firewall)
4. If Public zone users are getting IP addresses in the ranges that are indicated for Workforce, Special Purpose, or Facility zone, you have a wireless access point connected to the wrong zone
    4. Remove all wireless access points that are not managed by TM (i.e. wireless extender/repeater, 3rd party router installed downstream from firewall) from the network
    5. Meraki APs should not have this problem
        - Contact the Global Service Desk once you have verified that there are no wireless access points other than those indicated in TM
    6. The pool of IP addresses is much smaller in these zones than in the public zone, allowing wireless users to connect to any of these may cause the pools to become exhausted and prevent wireless users from accessing the network