Meetinghouse
Meraki Firewall and Switch Installation Guide

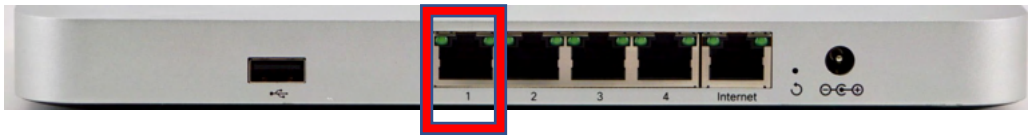
Meraki Managed Firewalls

- Either the MX64, MX67, MX68 or MX68W can be used in a Meetinghouse network.

- MX64: Port 1 should be connected to an SFP port on the Meraki Switch using an SFP Module.* Ports 2, 3, 4 will be disabled.
- MX67: Port 2 should be connected to an SFP port on the Meraki Switch using an SFP Module. * Ports 3, 4, 5 will be disabled.
- MX68 or MX68W: Port 3 should be connected to an SFP port on the Meraki Switch using an SFP Module. * Ports 4 to 10 will be disabled. If using a MX68W leave the internal WiFi off.

*If you don't have an SFP module then connect to one of the Switch Access Ports and configure that switch port to be "LINK" in Church Network Manager. (CNM)

Meraki MX64 Firewall



Meraki MX67 Firewall

Meraki MX68 or MX68W Firewall

Meraki Managed Switches

- ✓ For a successful install, please read the instructions before beginning the switch install or contacting the GSD for assistance. Reading and understanding this guide before you begin is imperative for success.
- ✓ Label cables before disconnecting them from the current unmanaged switches.
- ✓ At least one Meraki managed switch must be installed in every meetinghouse worldwide
- ✓ Most meetinghouses will use a combination of the Meraki switch and current unmanaged switches. If there are enough Meraki ports for all data cables then remove all unmanaged switches.
- ✓ The installer will need access to a mobile computer or an iPad in order to activate and configure the new Meraki switch in Church Network Manager during the Meraki switch installation
- ✓ All wireless access points (APs) in the meetinghouse must connect directly to the new Meraki managed switch. Do not connect Cisco APs into the Meraki Switch. Upgrade Cisco APs to Meraki APs.
- ✓ Order an SPF module when ordering a Meraki Switch.
- ✓ If a second Meraki switch is needed in the same meetinghouse then two additional SFP modules will be needed.
- ✓ You will need a screwdriver and wood screws if you are mounting a switch to a wall, cabinet, or rack
- ✓ You will need a pen or pencil, tape and paper to create a cable mapping sheet of the meetinghouse data drops
- ✓ The Switch installation will be much easier if you have 2 people to identify where each data cable connects. Especially for the Wireless Access Points.
- ✓ The Meraki switch(es) installed in a meetinghouse will be logically tied to the Meraki Firewall in the Meraki Cloud Management application.

MS120-8FP (PoE)

8 Port Meraki Managed Switch

MS120-24P (PoE)

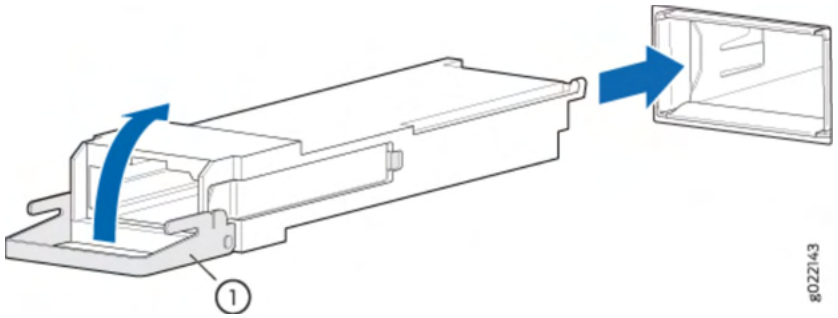
24 Port Meraki Managed Switch

SFP Module -Optics 1000BASET
SFP transceiver module for
Category 5 copper wire

SFP Modules

SFP Module -Optics 1000BASET
SFP transceiver module for
Category 5 copper wire

- Every switch will need a SFP module installed in SFP 9 on the "8 Port switch" and SFP 25 on the "24 Port switch".
- If a second Meraki switch is needed in the same meetinghouse then two additional SFP modules will be needed. Install the extra SFP module in Port 10 of the first Meraki 8 Port switch to connect the two Meraki Switches.
- To install the SFP module- open the lock, insert the module and close the lock. This will lock the SFP module into the switch.
- Connect the data cable to the SFP modules with the lock closed in the locked position.
- To remove an SFP module- open the lock and remove the module from the switch.

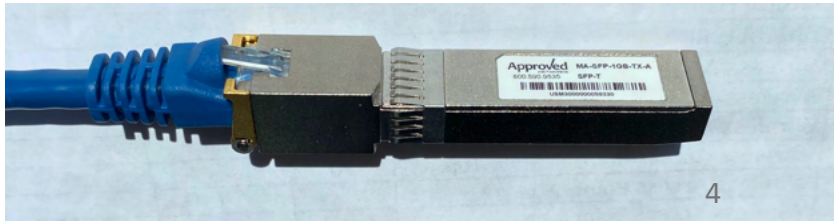


1. Insert the SFP modules into the switch with the lock open and then close the lock

Lock is open

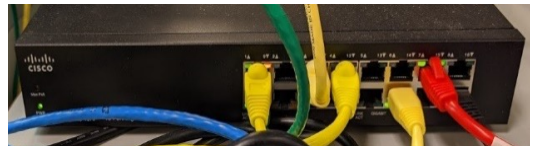
Lock is closed

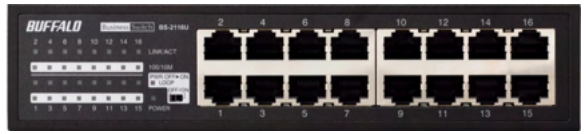
Lock is closed with data cable connected



Steps before installing Meraki Managed Switch (MS120-8FP or MS120-24P)

Examples of Unmanaged Switches

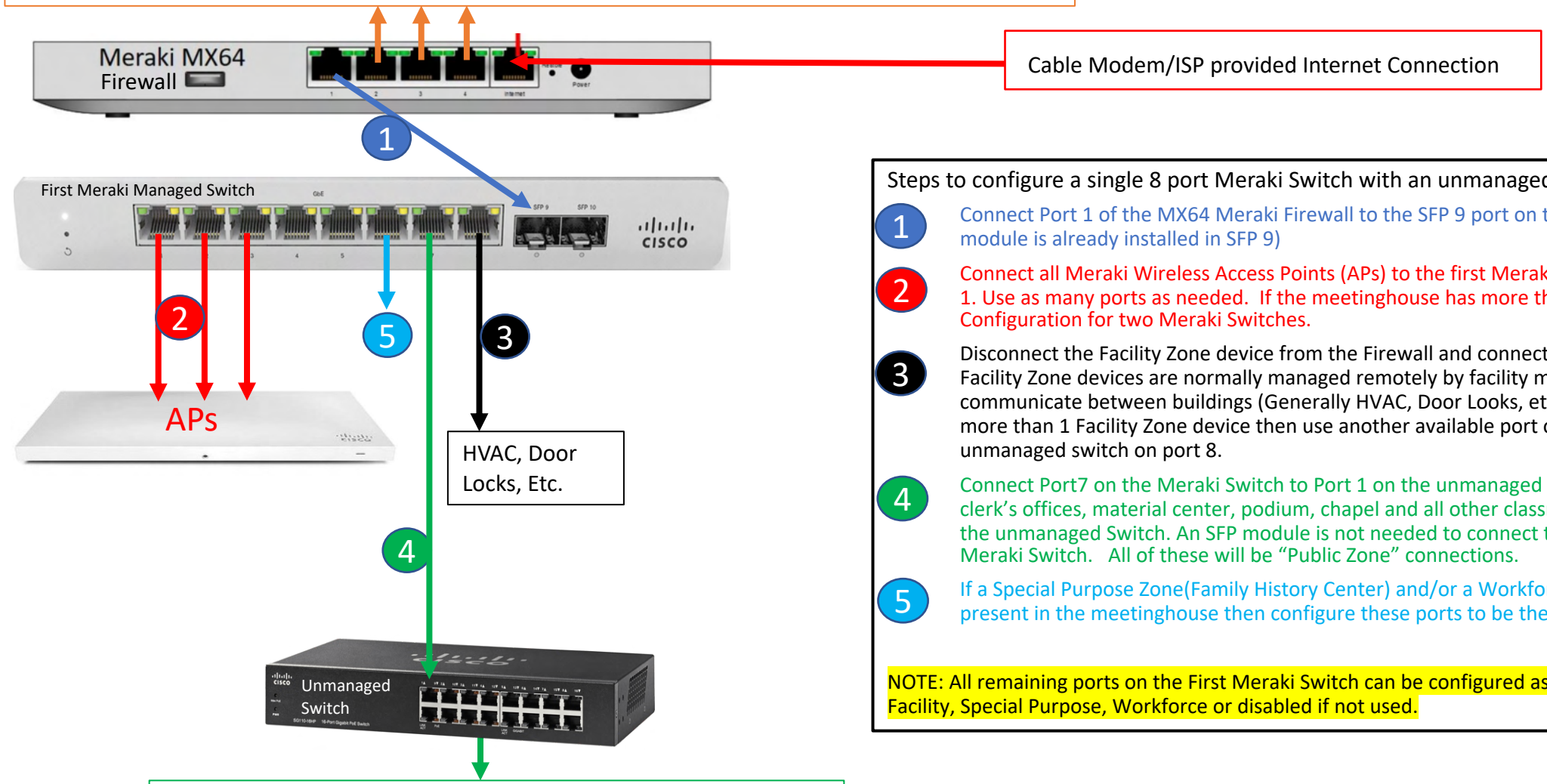




1. Using tags or tape, identify and label the following possible cables connecting to:
    1. Wireless Access Points (tag as AP)
    2. Clerk's and unit Leader's offices (tag as Clerk or BP or SP)
    3. The HVAC, Door locks, and other Facility devices (tag as HVAC or Locks or FAC)
    4. Webcast equipment, Audio/Video distribution systems (tag as AV)
    5. The Family History Center (if present) (tag as FHC)
    6. The Seminary and Institute Teacher Offices and student classrooms (if present) (tag as S&I)
    7. FM office, Mission office, etc... (if present) (tag as FM or Mission)
    8. All other rooms in the meetinghouse (all of these will be public zone)
2. This is a great opportunity to determine if all classroom connections are used or needed. If they are no longer used, then leave the cables disconnected to reduce the number of needed switch ports. If you leave a room disconnected, then add a sticker to the data jack faceplate in that room stating that it is disconnected.
3. After labeling, take photos of the current configuration to inform the troubleshooting process if problems occur during the new switch installation.
    a. It is recommended that you leave a sheet of paper with the cable and port mappings next to the switch. This will facilitate future changes to the network. (example: Port 7 on the switch goes to the Clerk's office, etc.)

Figure 1 - One Meraki MS120-8FP (8 port switch) Configuration

Firewall Port 2 - may be used during Switch installation to access Church Network Manager(CNM)
Firewall Ports 3 and 4 - will be disabled. (nothing should be connected to Firewall Ports 2, 3, 4 after the switch installation is completed)



All ports will be "Public Zone". APs will not function when connected to an unmanaged Switch. Connect unit leader and clerk's offices, Material Center, podium and all other classrooms to this unmanaged Switch.

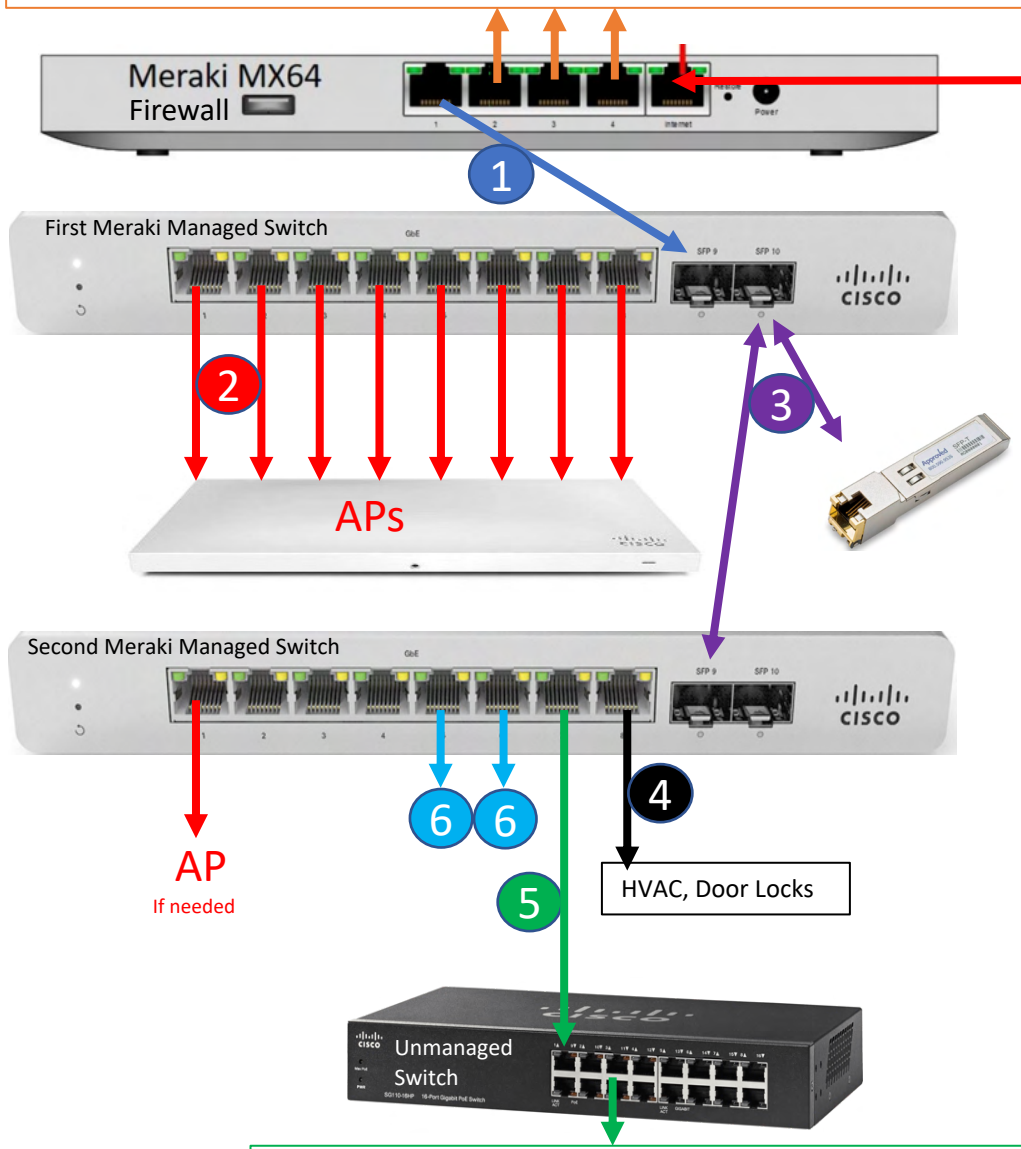
Steps to configure a single 8 port Meraki Switch with an unmanaged Switch:

1. Connect Port 1 of the MX64 Meraki Firewall to the SFP 9 port on the new Meraki Switch (The SFP module is already installed in SFP 9)
2. Connect all Meraki Wireless Access Points (APs) to the first Meraki Switch starting with Port 1. Use as many ports as needed. If the meetinghouse has more than 4 APs then see Figure 2 – Configuration for two Meraki Switches.
3. Disconnect the Facility Zone device from the Firewall and connect to Port 8 on the Meraki Switch. Facility Zone devices are normally managed remotely by facility managers, or need the ability to communicate between buildings (Generally HVAC, Door Looks, etc.) If the meetinghouse has more than 1 Facility Zone device then use another available port on the Meraki Switch or use an unmanaged switch on port 8.
4. Connect Port7 on the Meraki Switch to Port 1 on the unmanaged switch. Connect unit leader and clerk's offices, material center, podium, chapel and all other classrooms in the meetinghouse to the unmanaged Switch. An SFP module is not needed to connect the unmanaged switch to the Meraki Switch. All of these will be "Public Zone" connections.
5. If a Special Purpose Zone(Family History Center) and/or a Workforce Zone(Seminary, Institute) is present in the meetinghouse then configure these ports to be the correct zone.

NOTE: All remaining ports on the First Meraki Switch can be configured as needed to be AP, Link, Public, Facility, Special Purpose, Workforce or disabled if not used.

Figure 2 - Two Meraki MS120-8FP (8 port switches) Configuration

Firewall Port 2 - may be used during Switch installation to access Church Network Manager(CNM)
Firewall Ports 3 and 4 - will be disabled. (nothing should be connected to Firewall Ports 2, 3, 4 after the switch installation is completed)



Cable Modem/ISP provided Internet Connection

Steps to configure two 8 port Meraki Switches with an unmanaged Switch:

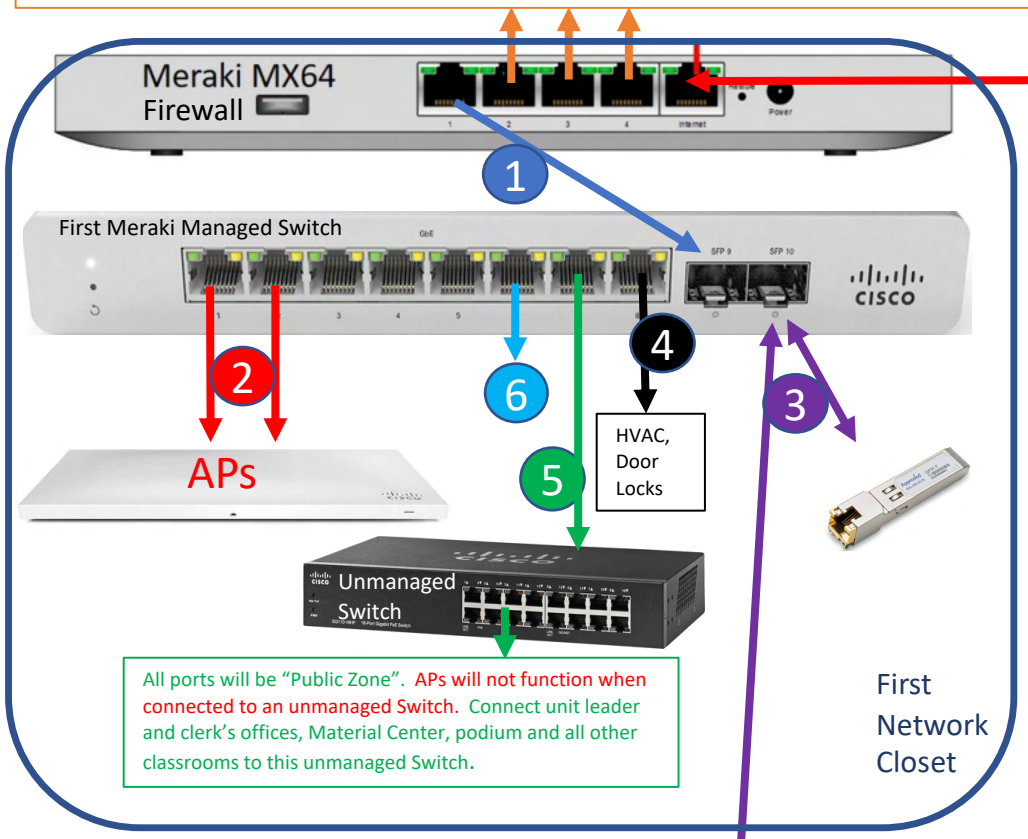
1. Connect Port 1 of the MX64 Meraki Firewall to the SFP 9 port on the new Meraki Switch (the SFP module is already installed in SFP9)
2. Connect all Meraki Wireless Access Points (APs) to the first Meraki Switch starting with Port 1. Use as many ports as needed. If you have more than 8 APs then connect the additional APs to the second Meraki Switch.
3. Install an SFP Module into Port 10 on the first Meraki Switch and connect it to Port 9 on the second Meraki Switch.
4. Disconnect Facility Zone devices from the Firewall and connect these to Port 8 on the Meraki Switch. Facility Zone Devices are normally managed remotely by facility managers, or need the ability to communicate between buildings (Generally HVAC, Door Looks, etc.) If the meetinghouse has more than 1 Facility Zone device then use another available port on the Meraki Switch or an unmanaged Switch on port 8.
5. Connect Port7 on the second Meraki Switch to Port 1 on the unmanaged Switch. Connect unit leader and clerk's offices, material center, podium, chapel and all other classrooms in the meetinghouse to this unmanaged Switch. An SFP module is not needed to connect the unmanaged switch to the Meraki Switch. All of these will be "Public Zone" connections.
6. If a Special Purpose Zone(Family History Center) and/or a Workforce Zone(Seminary, Institute) is present in the meetinghouse then configure these ports to be the correct zone.

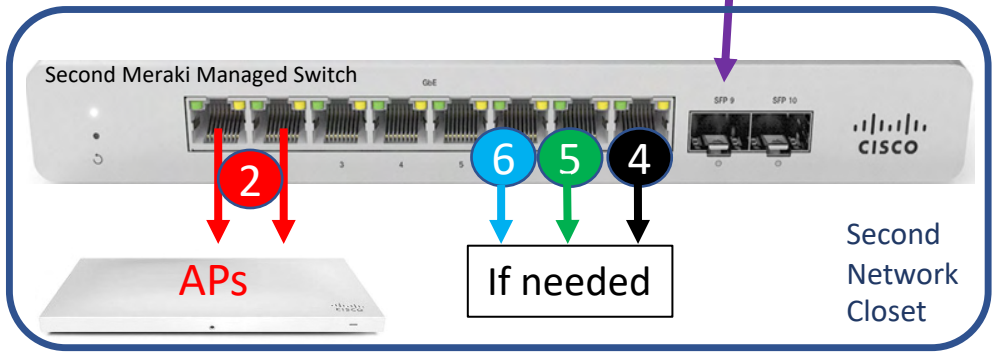
NOTE: All remaining ports on the First and Second Meraki switches can be configured as needed to be AP, Link, Public, Facility, Special Purpose, Workforce or disabled if not used.

All ports will be "Public Zone". APs will not function when connected to an unmanaged Switch. Connect unit leader and clerk's offices, Material Center, podium and all other classrooms to this unmanaged Switch.

Figure 2.1 - Two Meraki MS120-8FP (8 port switches) Configuration in multiple network closets

Firewall Port 2 - may be used during Switch installation to access Church Access Manager(CNM)
Firewall Ports 3 and 4 - will be disabled. (nothing should be connected to Firewall Ports 2, 3, 4 after the switch installation is completed)





Cable Modem/ISP provided Internet Connection

Steps to configure two 8 port Meraki Switches in 2 closets with an unmanaged Switch:

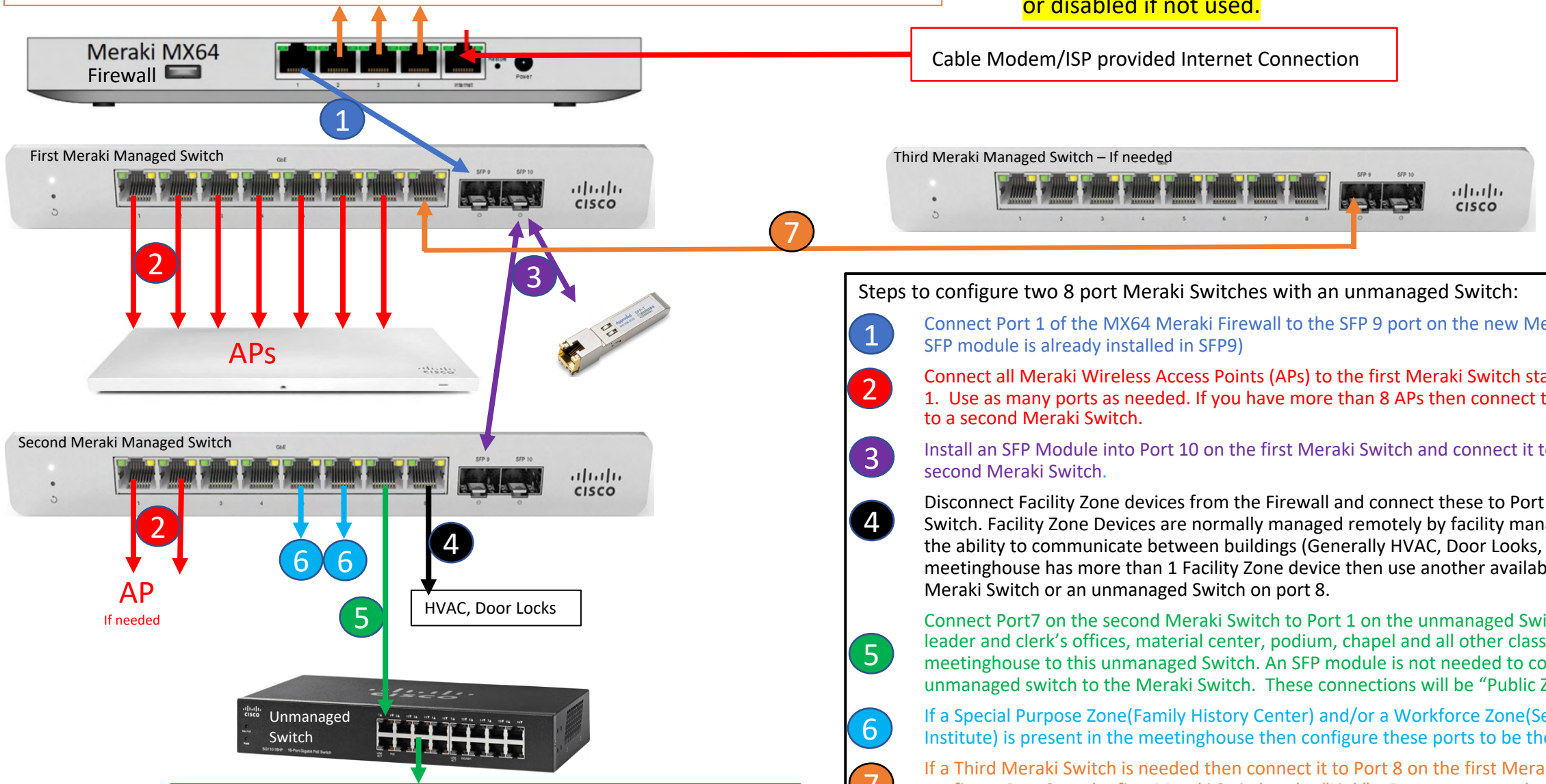
1. Connect Port 1 of the MX64 Meraki Firewall to the SFP 9 port on the new Meraki Switch (the SFP module is already installed in SFP9)
2. Connect all Meraki Wireless Access Points (APs) to the first Meraki Switch starting with Port 1. Use as many ports as needed. If you have APs in the second network closet then connect the additional APs to the second Meraki Switch in that closet.
3. Install an SFP Module into Port 10 on the first Meraki Switch and connect it to Port 9 on the second Meraki Switch. This patch cable will be need to span between the closets.
4. Disconnect Facility Zone devices from the Firewall and connect these to Port 8 on the Meraki Switch. Facility Zone Devices are normally managed remotely by facility managers, or need the ability to communicate between buildings (Generally HVAC, Door Looks, etc.) If the meetinghouse has more than 1 Facility Zone device then use another available port on the Meraki Switch or an unmanaged switch on port 8.
5. Connect Port7 on the first Meraki Switches to Port 1 on the unmanaged Switch. Connect unit leader and clerk's offices, material center, podium, chapel and all other classrooms in the meetinghouse to this unmanaged Switch. An SFP module is not needed to connect the unmanaged switch to the Meraki Switch. These connections will be "Public Zone"
6. If a Special Purpose Zone(Family History Center) and/or a Workforce Zone(Seminary, Institute) is present in the meetinghouse then configure these ports to be the correct zone.

NOTE: All remaining ports on the First and Second Meraki switches can be configured as needed to be AP, Link, Public, Facility, Special Purpose, Workforce or disabled if not used.

Figure 3 - Three Meraki MS120-8FP (8 port switches) Configuration

Firewall Port 2 - may be used during Switch installation to access Church Network Manager(CNM)
Firewall Ports 3 and 4 - will be disabled. (nothing should be connected to Firewall Ports 2, 3, 4 after the switch installation is completed)

NOTE: All remaining ports on the Meraki switches can be configured as needed to be AP, Link, Public, Facility, Special Purpose, Workforce or disabled if not used.

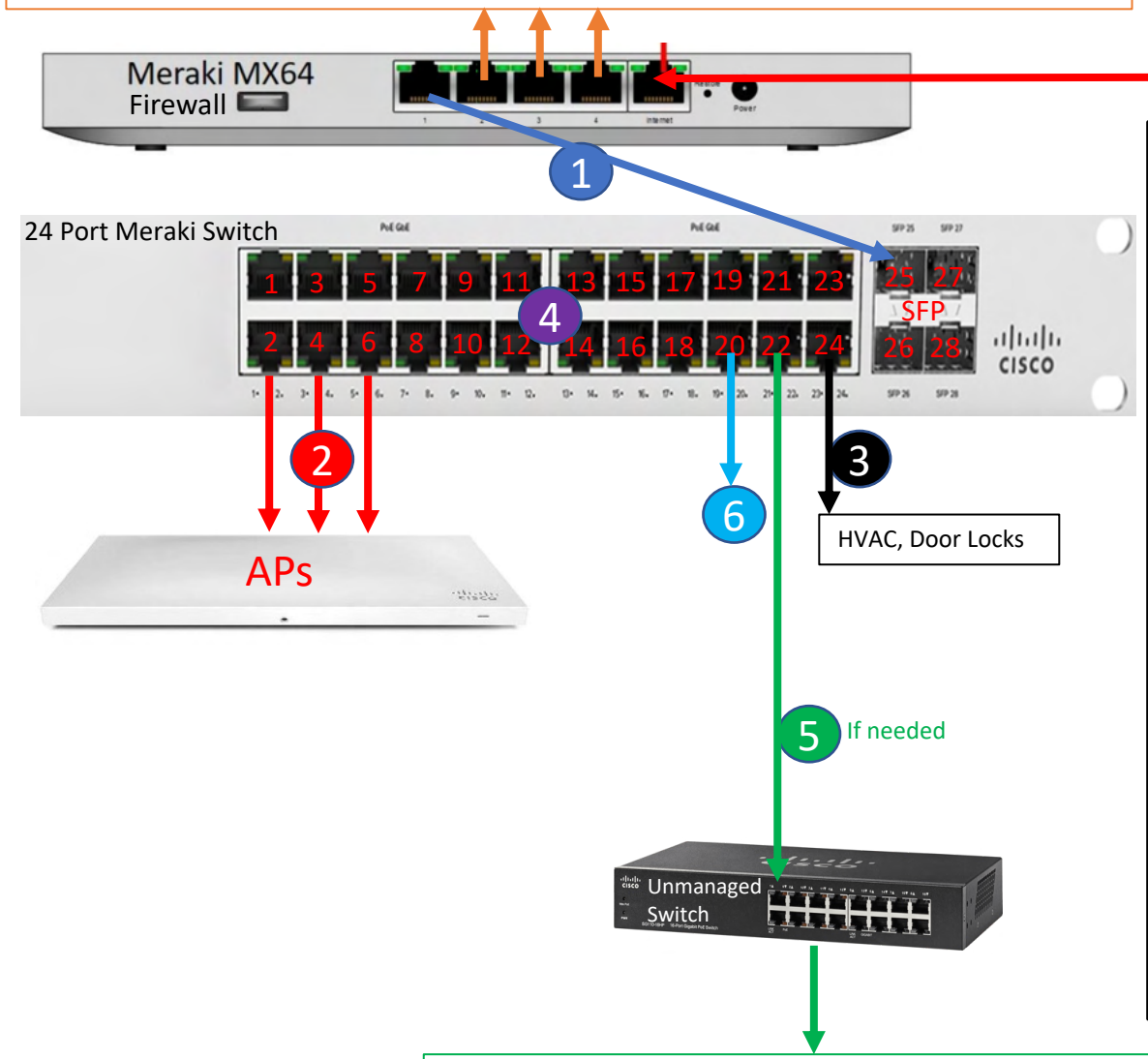


Steps to configure two 8 port Meraki Switches with an unmanaged Switch:

1. Connect Port 1 of the MX64 Meraki Firewall to the SFP 9 port on the new Meraki Switch (the SFP module is already installed in SFP9)
2. Connect all Meraki Wireless Access Points (APs) to the first Meraki Switch starting with Port 1. Use as many ports as needed. If you have more than 8 APs then connect the additional APs to a second Meraki Switch.
3. Install an SFP Module into Port 10 on the first Meraki Switch and connect it to Port 9 on the second Meraki Switch.
4. Disconnect Facility Zone devices from the Firewall and connect these to Port 8 on the Meraki Switch. Facility Zone Devices are normally managed remotely by facility managers, or need the ability to communicate between buildings (Generally HVAC, Door Looks, etc.) If the meetinghouse has more than 1 Facility Zone device then use another available port on the Meraki Switch or an unmanaged Switch on port 8.
5. Connect Port7 on the second Meraki Switch to Port 1 on the unmanaged Switch. Connect unit leader and clerk's offices, material center, podium, chapel and all other classrooms in the meetinghouse to this unmanaged Switch. An SFP module is not needed to connect the unmanaged switch to the Meraki Switch. These connections will be "Public Zone".
6. If a Special Purpose Zone(Family History Center) and/or a Workforce Zone(Seminary, Institute) is present in the meetinghouse then configure these ports to be the correct zone.
7. If a Third Meraki Switch is needed then connect it to Port 8 on the first Meraki Switch and configure Port 8 on the first Meraki Switch to be "Link". Do not connect the third Meraki Switch to the second Meraki Switch.

Figure 4 - One Meraki MS120-24P (24 port switch) Configuration

Firewall Port 2 - may be used during Switch installation to access CNM
Firewall Ports 3 and 4 - will be disabled. (nothing connected to Ports 2, 3, 4 after the switch installation is completed)



Steps to configure a 24 port Meraki Switch with an (if needed) unmanaged Switch:

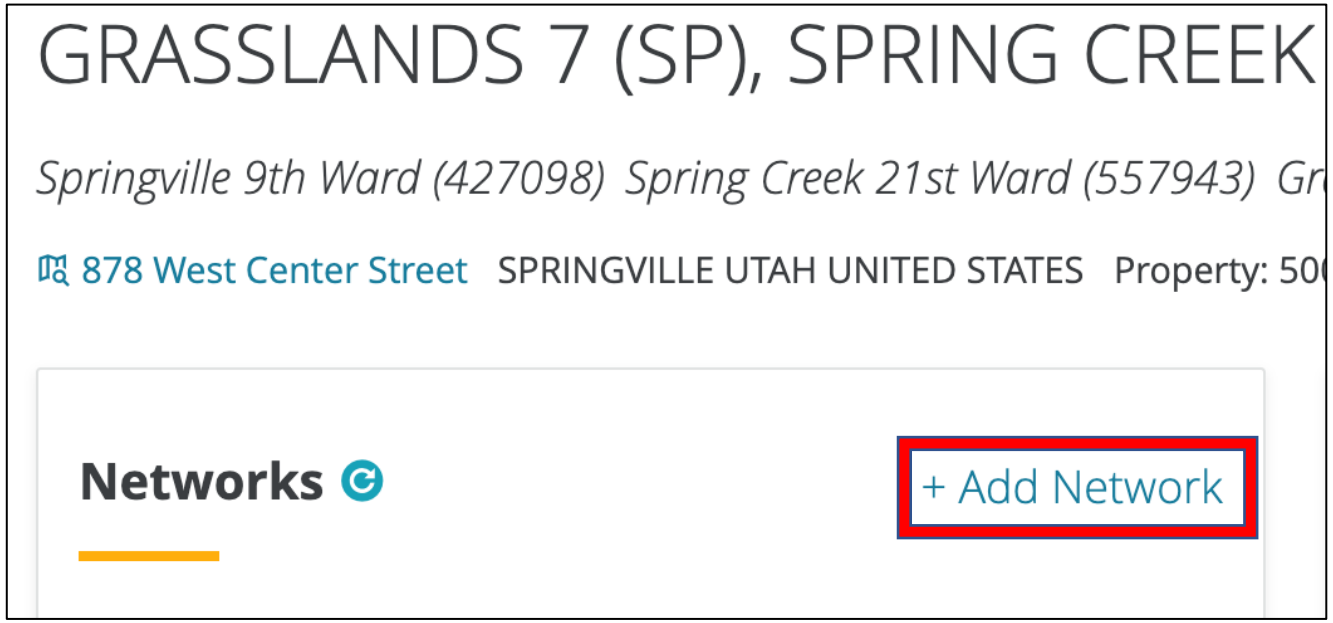
1. Connect Port 1 of the MX64 Meraki Firewall to port SFP 25 on the new Meraki Switch (The SFP module is already installed in SFP 25)
2. Connect all Meraki Wireless Access Points (APs) to the first Meraki Switch starting with Port 1. Use as many ports as needed.
3. Disconnect Facility ZTMone devices from the Firewall and connect these to Ports 23 and 24 on the Meraki Switch. Facility Zone Devices are normally managed remotely by facility managers, or need the ability to communicate between buildings (Generally HVAC, Door Looks, etc.) If the meetinghouse has more than 1 Facility Zone device then use another available port on the Meraki Switch or an unmanaged Switch on port 24.
4. All remaining available ports on the Meraki 24 Port Switch can be configured to AP, Link, Public, Facility, Special Purpose, Workforce or disabled. Move as many cables from the unmanaged Switch to the new Meraki 24 Port Switch as possible. Most of these will be "Public Zone" ports for local unit leader and clerk's offices, material center, podium, and all other classrooms in the meetinghouse.
5. If needed – Connect Port 22 on the Meraki Switch to Port 1 on the unmanaged Switch. Connect any remaining unit leader and clerk's offices, material center, podium, chapel and all other classrooms in the meetinghouse to this unmanaged Switch. An SFP module is not needed to connect the unmanaged switch to the Meraki Switch. These connections will be "Public Zone"
6. If a Special Purpose Zone(Family History Center) and/or a Workforce Zone(Seminary, Institute) is present in the meetinghouse then configure these ports to be the correct zone.

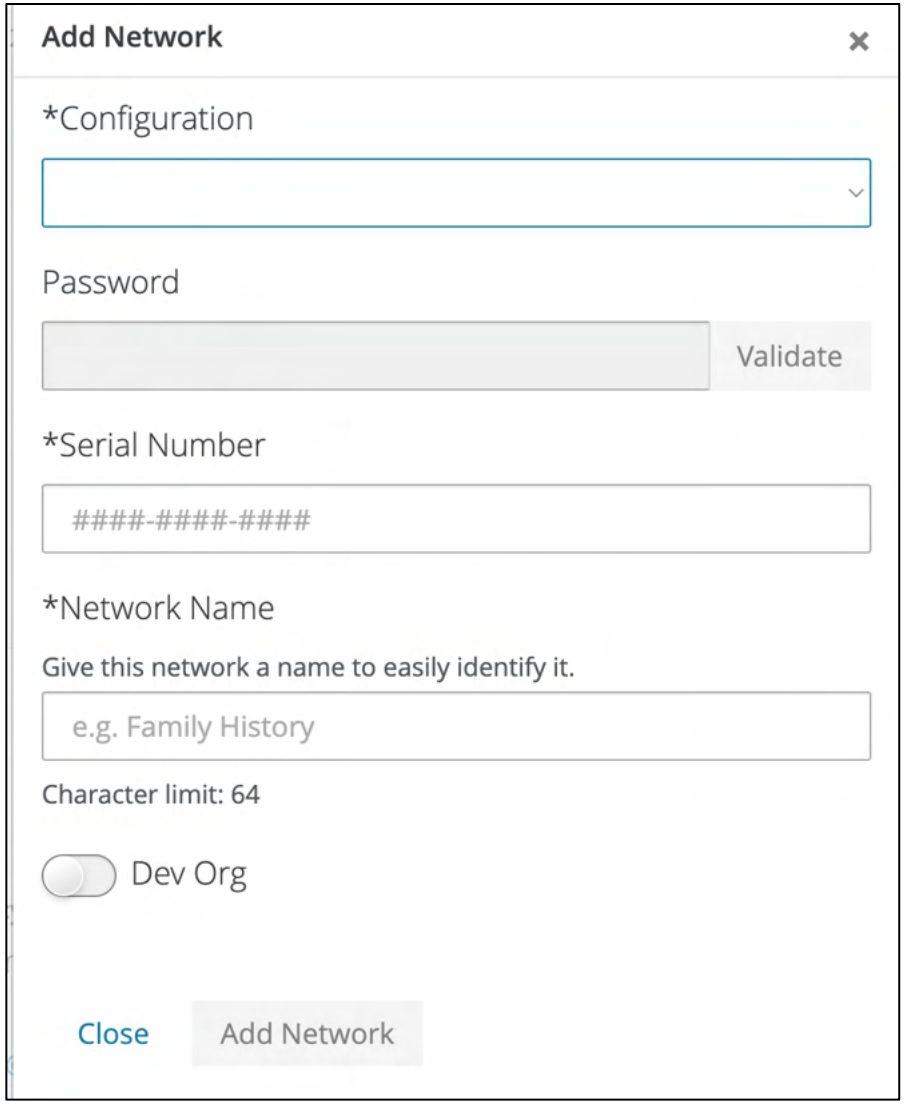
NOTE: All remaining ports on the Meraki switch can be configured as needed to be AP, Link, Public, Facility, Special Purpose, Workforce or disabled if not used.

All ports will be "Public Zone". APs will not function when connected to an unmanaged Switch. Connect any remaining unit leader and clerk's offices, Material Center, podium and all other classrooms to this unmanaged Switch.

Activating the Meraki Firewall MX64, MX67, MX68 in CNM

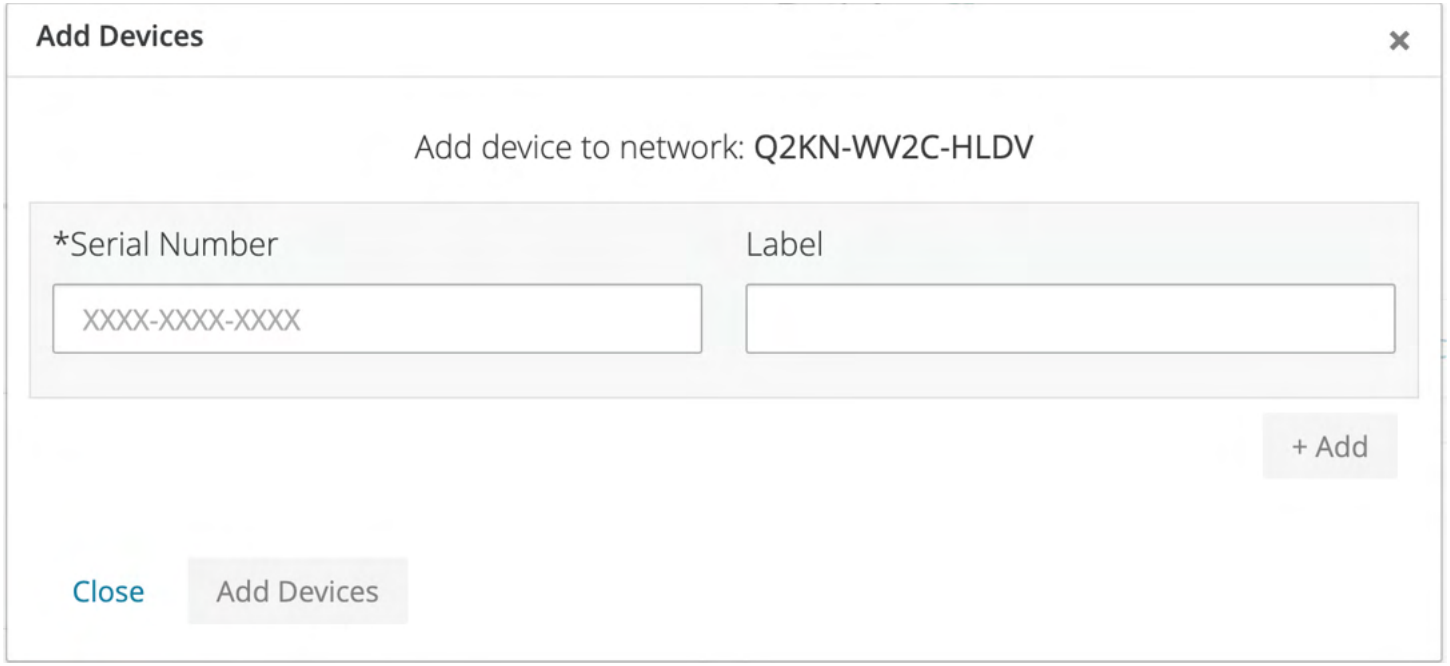
1. Remove the Meraki Firewall from the box and enter the Serial Number(SN) into Church Network Manager (CNM)
    1. To access CNM enter http://cnm.churchofjesuschrist.org into the brower's address bar
    2. Login to CNM using your LDSAccount Username and Password
2. Locate the Meetinghouse page in CNM:
    1. Click “+Add Network”
    2. Select the Meetinghouse configuration
    3. Password not needed for meetinghouse configurations
    4. Enter the new Firewall’s Serial Number into the ”Serial Number" field from the bottom of the firewall
    5. Give the Network a name
    6. Click “Add Network”



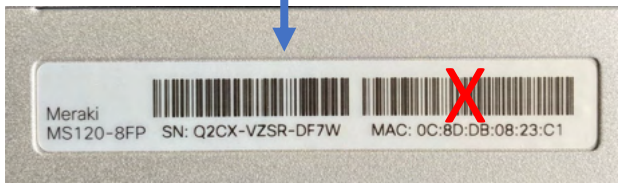


Activating the Meraki Managed Switch in CNM

1. Remove the Meraki Switch from the box and enter the Serial Number(SN) into CNM
2. To locate the Switches page in CNM:
    1. Locate the meetinghouse name where you are installing the new Meraki Switch
    2. Click on the Firewall serial number of the correct meetinghouse
        - IMPORTANT NOTE - Verify you are adding the switch to the correct Firewall by matching the SN on the Firewall to the SN on this CNM page
        - If the Serial Numbers do not match then call the GSD. The Firewall must have been activated at the incorrect meetinghouse
    3. Click on the ”MENU” in the upper righthand corner and then click on ”Add Devices” from the drop-down menu
    4. Enter the new Switch's Serial Number into the Serial Number field and provide a switch label
    5. Click ”Add Devices”



Switch Serial Numbers (SN) are located on the switch back panel



Steps after installing the Meraki Firewall and/or Meraki Switch

1. Verify that the Meraki Firewall has a white light
    1. Orange = Firewall is booting up or may not find access to the internet if light stays orange
    2. Rainbow cycle = Firewall is communicating with the Meraki cloud
    3. Blinking White = Firewall is functional and updating firmware from the Meraki cloud
    4. Solid White = Firewall is online and ready

2. If the Firewall light is not Blinking or Solid White then review the Meetinghouse Network Troubleshooting guide

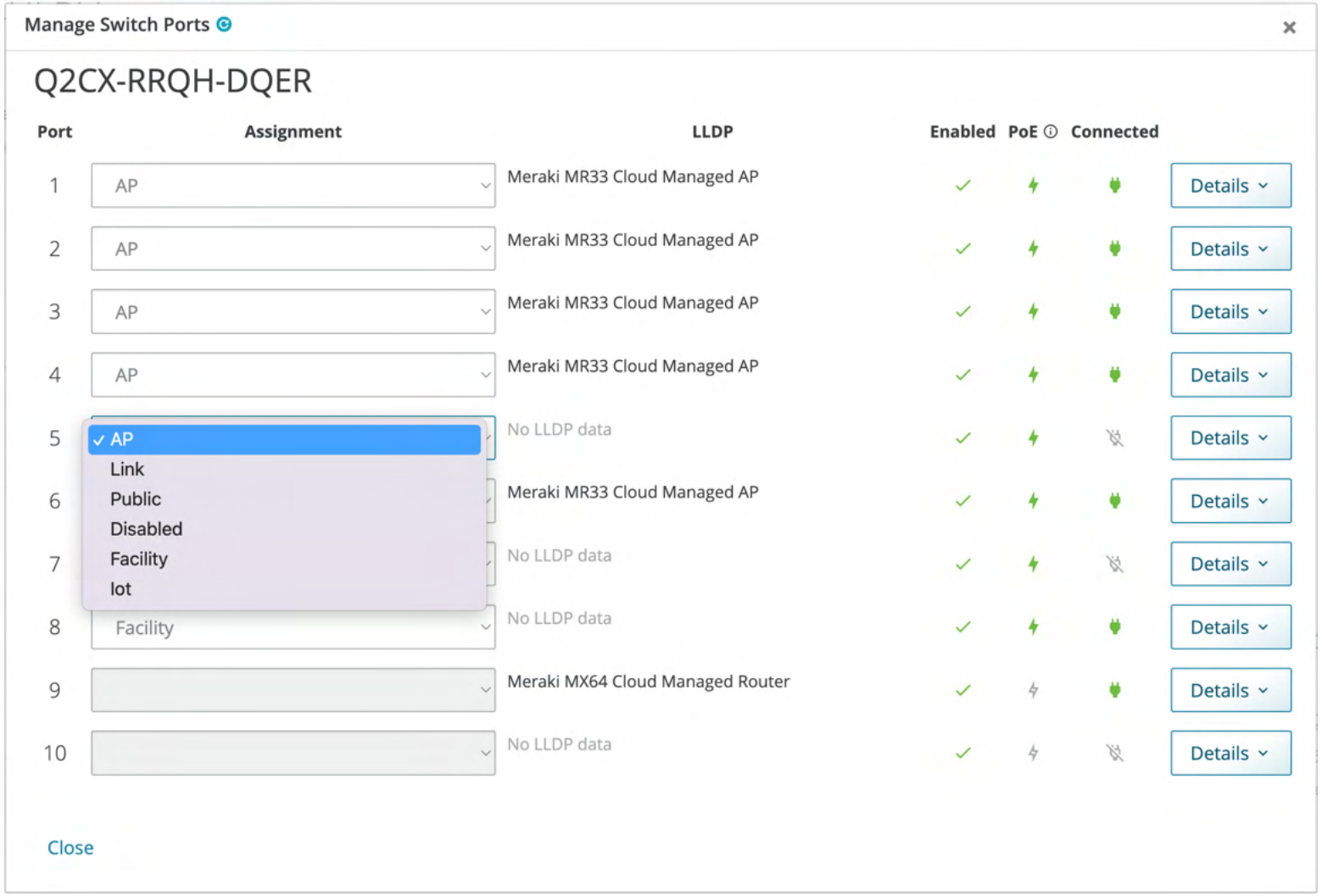
3. Verify that the Meraki Switch has a flashing or solid white light
    1. Orange = switch is booting up or may not find access to the internet if light stays orange
    2. Rainbow cycle = communicating with the Meraki cloud
    3. Blinking white = switch is functional and updating firmware from the Meraki cloud
        1. The switch will reboot once the firmware is installed(light will go back to orange)
    4. Solid White = Complete and ready

4. If the Switch Light is not Blinking or Solid White then then review the Meetinghouse Network Troubleshooting guide

5. Once the light on the new Meraki Switch is solid white then configure each port in CNM (see the next page)

Configure each Meraki Switch Port in CNM

1. Configure each switch port by clicking on the three dots next the Meraki Switch and select Ports from the menu.



AP – use this for Meraki Wireless Access Points(APs) only. Meraki APs must be connected to the Meraki Switch.

Link - only use if the SFP ports are unavailable on the first Meraki Switch and an additional Meraki Switch is needed.

Public Zone – Clerk's and Unit Leader's offices, Material Center, Podium, Chapel, and all classrooms in the Meetinghouse

Workforce Zone - Seminary and Institute Teacher Offices, FM offices, Family Services offices, or any port that is being used by a Church employee

Disabled - unused port or a port that you don't want to be used without authorization

Facility Zone - Devices that are managed remotely by facility managers, or need the ability to communicate between buildings (Generally HVAC, Door Looks, etc.) Prior to installing the Meraki switch these devices were connected to Port 4 on the Meraki Firewall. Do not leave these devices connected to the Firewall ports.

Special Purpose Zone - Family History Center

Now that the Switch is activated in CNM and each Switch port is properly configured in CNM:

Note: we have learned that in some cases, the switch indicator light will return to a solid orange state for several minutes. The switch should eventually return to a solid white light.

1. Verify that the Meraki Wireless Access Points (AP) lights are Green or Blue:
    1. Orange - AP is booting (permanent Orange suggests hardware issue)
    2. Rainbow - AP is initializing/scanning
    3. Blinking Blue - AP is upgrading
    4. Green - AP is ready with nothing connected
    5. Blue - AP is ready with clients connected
    6. Blinking Orange - AP can't find uplink to switch
2. If the AP lights are not Green or Blue, then then review the Meetinghouse Network Troubleshooting guide.
3. Both the wireless Liahona network and wired clerk computers should be able to access ComeUntoChrist.org
4. If the Network is not working, then review the Meetinghouse Network Troubleshooting guide

When is a second or third Meraki Switch needed

A second or third Meraki Switch will be needed if:

1. Installing an 8 Port switch and the meetinghouse has more than 4 Wireless Access Points(APs). (Access Points must be connected to the Meraki switch)
2. If the total number of needed Zones and APs is more than 8
3. If a third Meraki Switch is needed then it must be connected to an available port(1-8) on the first Meraki Switch. Configure the Port on the First Meraki Switch as a "Link" Do not connect the third Meraki Switch to the second Meraki Switch.
4. If the meetinghouse has multiple network closets then each closet will need a Meraki Switch but the second and third Meraki Switches must be connected to the Meraki Switch is that is connected to the Meraki Firewall.

- The second Meraki Switch will connect to port SFP 10 on the first Meraki switch. You will need to put an SFP module in Port 10. SFP modules will be shipped to you or you can order additional SFP modules from eMarket (Part # MA-SFP-1GB-TX-A)

•Heat Concern- Do Not Stack

- Do not stack electronic devices on top of or under the Firewall
- Do not stack the 8 Port Meraki Switches on or under another electronic device if possible
- The 8 port switch and Firewall need open space around it to stay cool
- Stacking directly on other devices creates a lack of heat dissipation which can lead to failures
- The 24 Port switch has a fan inside to keep it cool. You can stack switches on top of it.