Meraki

Last updated: 11 April 2018

Training Manual

Certified Meraki Network Operator Certification Program

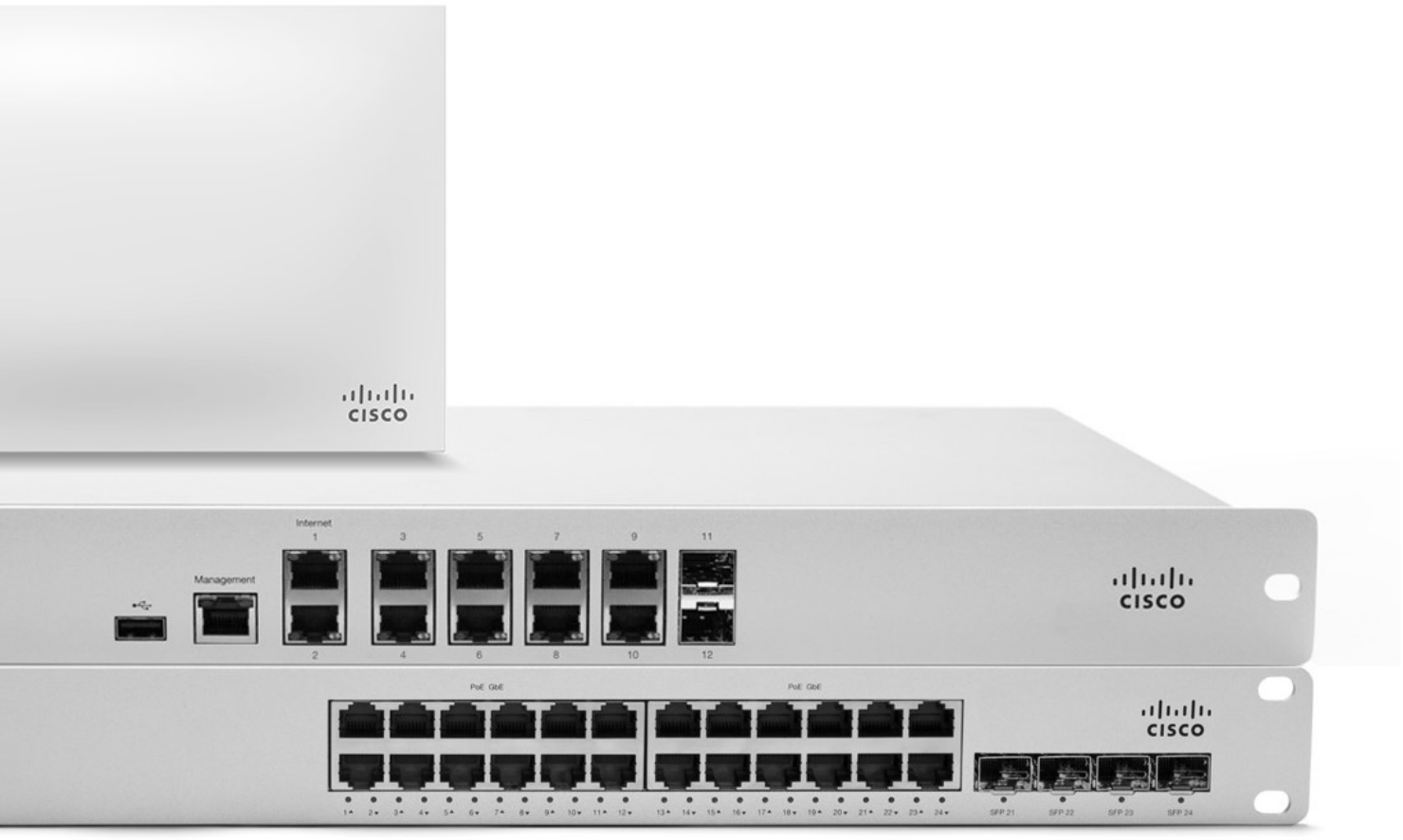


Table of Contents

How to Read the Lab Guide 3

Getting Started 4

- Cisco Spark Chatroom and Collaboration 4
- Lab Credentials / Dashboard Access 8
- Lab Station References (IP Addressing) 10
- CMNO Lab Topology 11

Section A – Full Stack Configuration 12

- Lab 1: Small / Medium Site 12
- Lab 2: Large Site / Campus 18
- Lab 3: Distributed Enterprise 21
- Lab 4: Physical Security 24
- Lab 5: Enterprise Mobility Management 25

Section B – Troubleshooting 28

- Notifying Instructor for Lab Setup 28

Concluding the Lab 32

- Lab Grading / Evaluation 32
- Exiting the Lab 33

Post-training Communications and Resources 34

- Frequently Asked Questions 34

How to Read the Lab Guide

Throughout the lab guide you will see various notations that serve to call out different types of information. These are classified into the following categories:

Important: These are high priority, critical bits of instructions that you must read carefully and pay close attention to performing correctly or they could have an adverse effect on your lab station.

Note: These are typically warnings that usually serve as reminders as they are sometimes easily overlooked or missed.

Hint: These are useful pieces of advice that could help point you in the right direction or help draw your attention to hard-to-find or confusing configurations.

Information: These serve as additional footnotes and reference materials sourced from the official Meraki documentation portal (located at: https://documentation.meraki.com) for various topics or technologies.

Getting Started

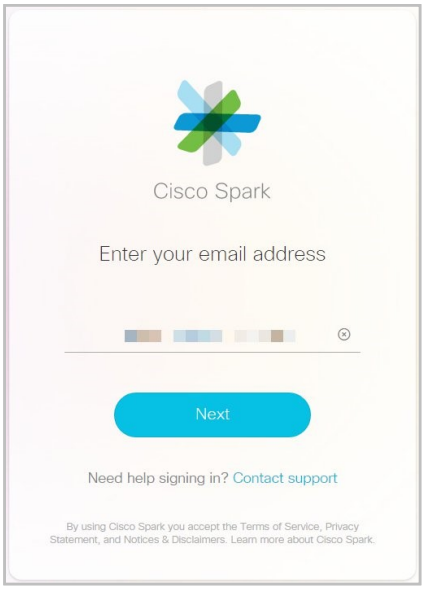
Welcome to the lab portion of the CMNO certification program. In the following sections, you will be utilizing the Meraki Dashboard to perform a series of exercises that will help you become familiar with various aspects of day-to-day network administration and operation. But before you dive into the labs and log into the Dashboard, we must prepare you with the resources necessary to get through the rest of today's training.

Cisco Spark Chatroom and Collaboration

As the CMNO lab instructor has already mentioned, we will be switching from the WebEx room to the Cisco Spark collaboration platform. It is very important that you successfully enter into the Spark chatroom for your CMNO training session because that is where you will be able to communicate with your lab instructor and the other participants during the lab hours.

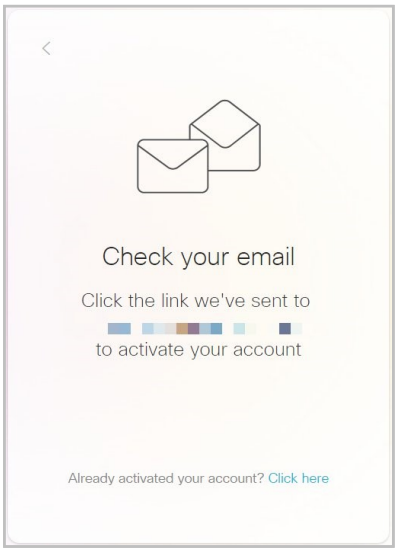
Logging Into / Accessing Cisco Spark

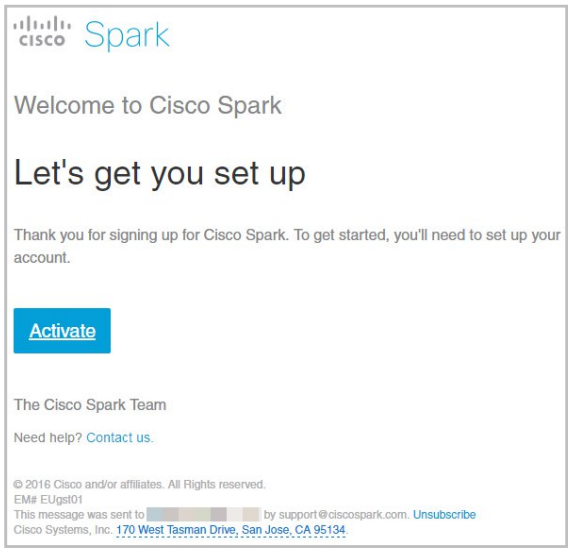
1. The primary method and easiest way of logging into Cisco Spark is by going directly to: https://web.ciscospark.com/signin and logging in with your e-mail address.



Important: The e-mail address must be the same as the one you provided on the CMNO Lab Sign-in form that you just completed recently.

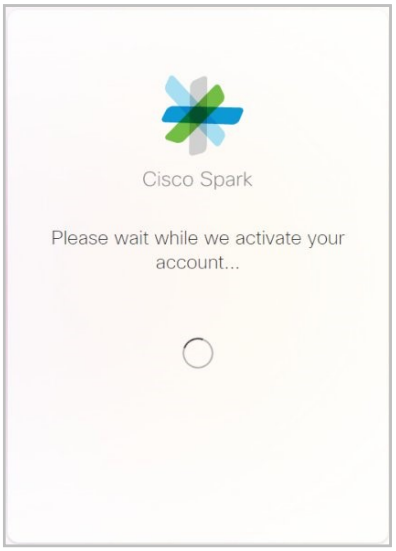
2. If this is your first time using Cisco Spark and you have not yet created an account yet, the service will prompt you to check your inbox for an activation e-mail. Click on the link within the e-mail to activate your account.

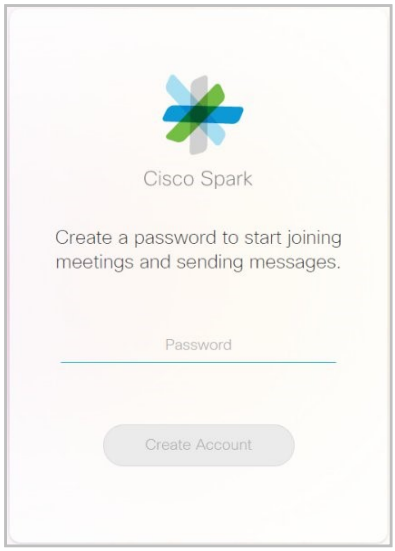


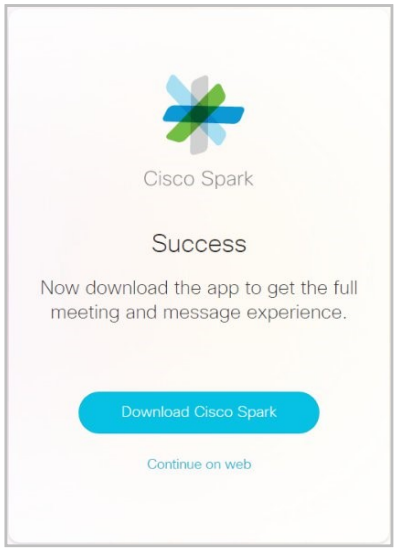


Note: If you've previously already created a Cisco Spark account using this e-mail address, click on the link near the bottom that says "Already activated your account? Click here"

3. The service should direct you to creating a password that meets the minimum complexity. Once finished, click Create Account. Upon account creation, you will be presented with 2 options of logging into Spark. You may download the Cisco Spark desktop client or continue with using the web browser-based version of the client.



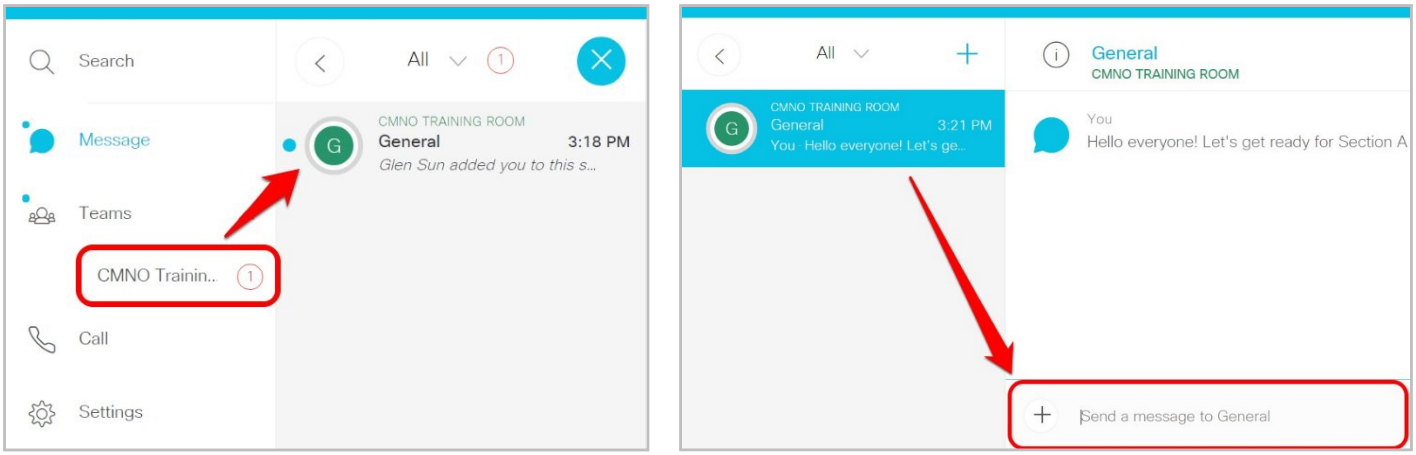




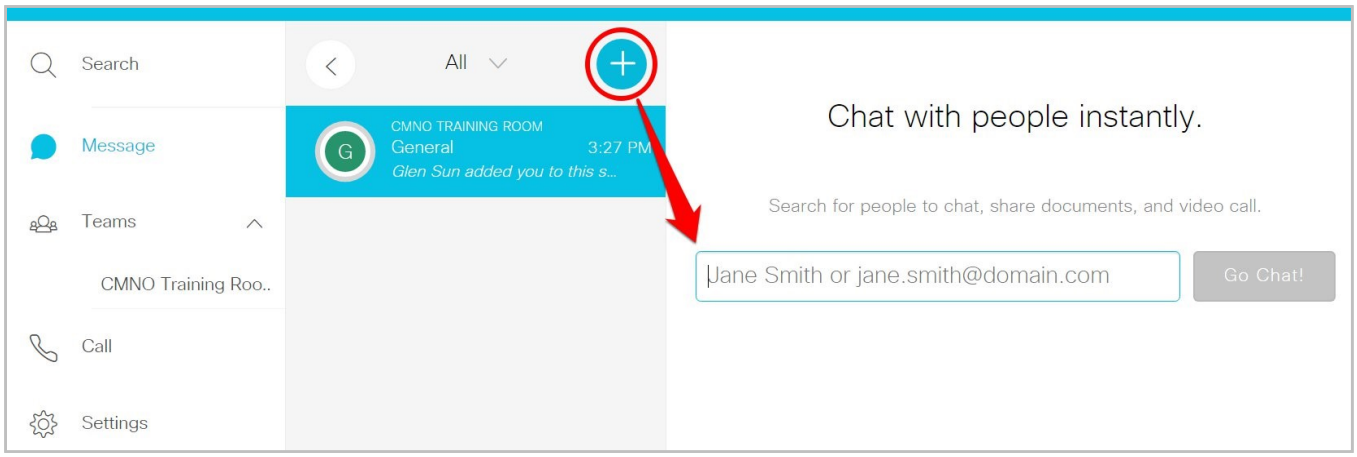
Using Cisco Spark (Web Client)

1. If you choose to use the web browser-based Cisco Spark client, proceed by entering your name and continuing directly to the Spark chatroom lobby.

2. You should notice that there is a notification for a new team invitation for the CMNO training group waiting for you. Click on the training room to begin chatting with the other CMNO participants and the instructor.



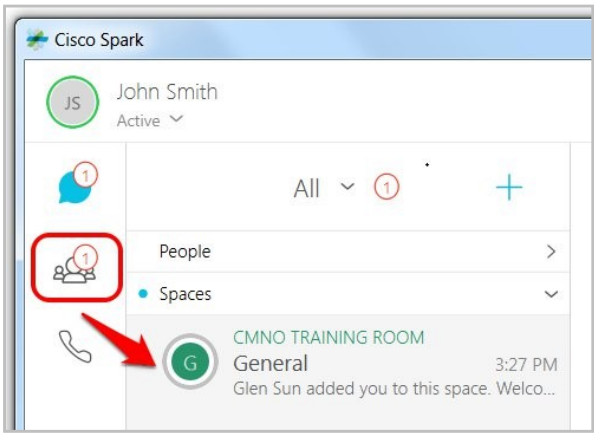
3. To chat directly with the lab instructor, click on the + icon near the top to open up the search field. Type in the instructor's name and begin a direct 1:1 instant message session with them.

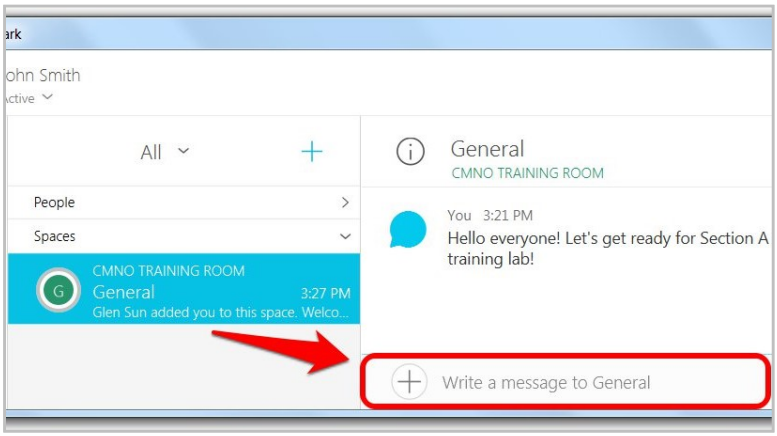


Using Cisco Spark (Desktop Client)

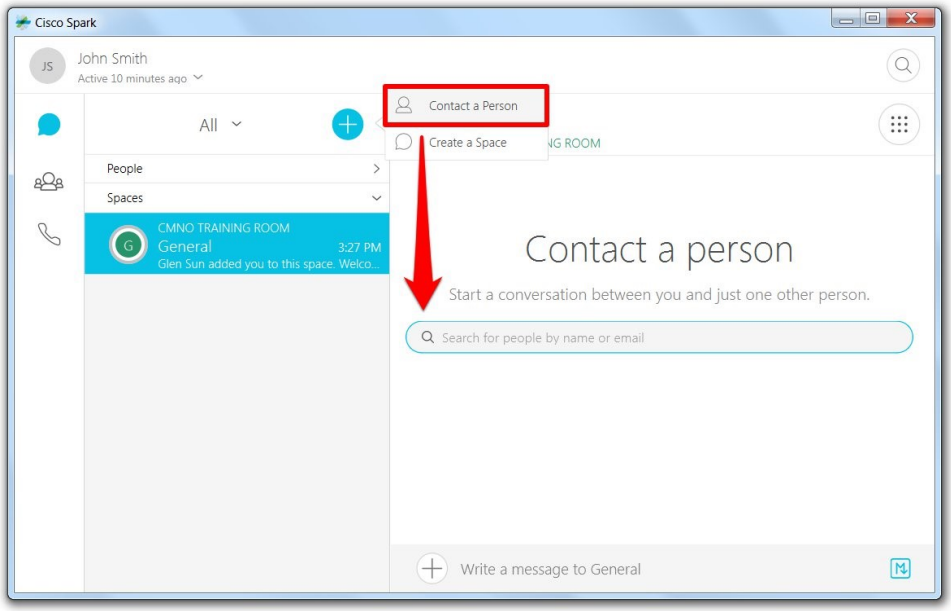
1. If you choose to download and install the desktop Cisco Spark client, launch the program after it has finished installing and log in using the same e-mail address as previously provided on the CMNO Lab Sign-In form.

2. Once logged in, you should see a notification for a new team invitation for the CMNO training group waiting for you. Click on the training room to begin chatting with the other CMNO participants and the instructor.





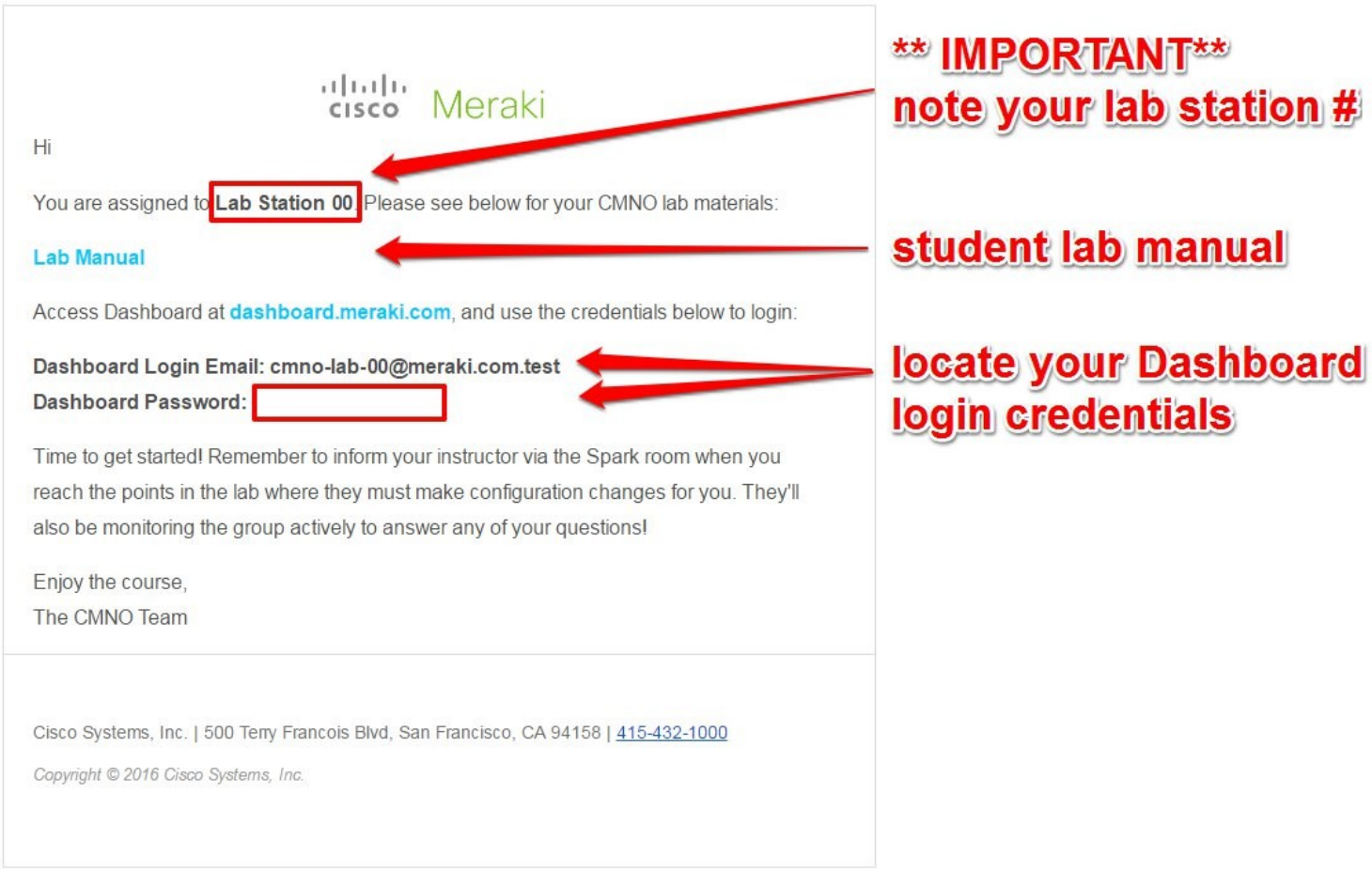
3. To chat directly with the lab instructor, click on the + icon near the top to open up the search field. Type in the instructor's name and begin a direct 1:1 instant message session with them.



cisco Meraki

Lab Credentials / Dashboard Access

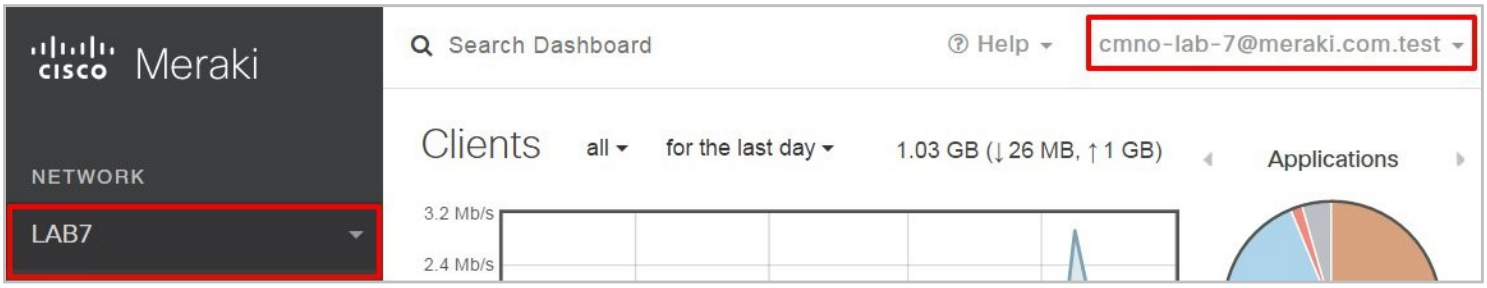
By now, every CMNO participant should have received an e-mail from the CMNO programs that looks similar to the one shown below. Please take note of the various important information in this e-mail:



Note: If you are not able to access the student lab manual by clicking on the link in the e-mail, it is likely due to a possible security policy on your computer that is blocking a URL re-direct. The alternate method is to access the student lab manual (a PDF file) is through the direct URL located below:
CMNO Lab Guide: https://drive.google.com/file/d/0B5M7a9ghT4HdbldDX2RwWkltSU0/view

As you log into Dashboard, you should pay close attention to ensure that you are working within the right lab network. For example, if you have been assigned to **Lab Station #7** then you should see very clearly at the top that you are signed in using the right user account and working in the right lab station network.

Verification for Lab Station #7 (new navigation)



Hint: The Cisco Meraki Dashboard is compatible with the most recent version of Firefox, Internet Explorer, and Chrome web browsers. However, the most recommended browser is Chrome as it provides the best and most consistent user interface experience. It should also be noted that MV security camera streaming is not supported on Windows 7 + Internet Explorer 11.

Lab Station References (IP Addressing)

Throughout the lab exercises, you will occasionally see instructions that reference your lab station number. These references appear as a green "**n**" whereby it should be immediately replaced by your lab station number:

Example Instruction: Rename the MX's name as "MX [**n**]"

- Lab Station 7's results: MX [7]
- Lab Station 18's results: MX [18]

A similar but slightly different instruction may tell you to add your lab station number – again referenced as "**n**" – to an existing value. This should be treated as a simple add (+) operation, as illustrated in the following example:

Example Instruction: Use the following as the subnet: 10.0. [10 + **n**] .0/24

- Lab Station 7's correct results: 10.0.17.0/24 (10 + **7** = 17)
- Lab Station 18's correct results: 10.0.28.0/24 (10 + **18** = 28)

Important: It would be incorrect if a *concatenation* were to be used, such as 10.0.107.0/24 for Lab Station 7 or 10.0.1018.0/24 for Lab Station 18 – these are incorrect and possibly invalid IP addressing values.

This type of replacement applies not just to subnets but also to IP addressing and VLAN instructions in the lab guide. Here are some more examples:

Example Instruction: Use the following as the IP address: 10.0. [150 + **n**] .1

- Lab Station 7's correct results: 10.0.157.1 (150 + **7** = 157)
- Lab Station 18's correct results: 10.0.168.1 (150 + **18** = 168)

Example Instruction: Configure the access port to be in VLAN [600 + **n**].

- Lab Station 7 would configure the port to be in VLAN 607 (600 + **7** = 607)
- Lab Station 18 would configure the port to be in VLAN 618 (600 + **18** = 618)

CMNO Lab Topology

The following diagram depicts the general topology of the CMNO lab architecture. The design of the network is the same for all lab pods/stations throughout all lab sections and exercises.

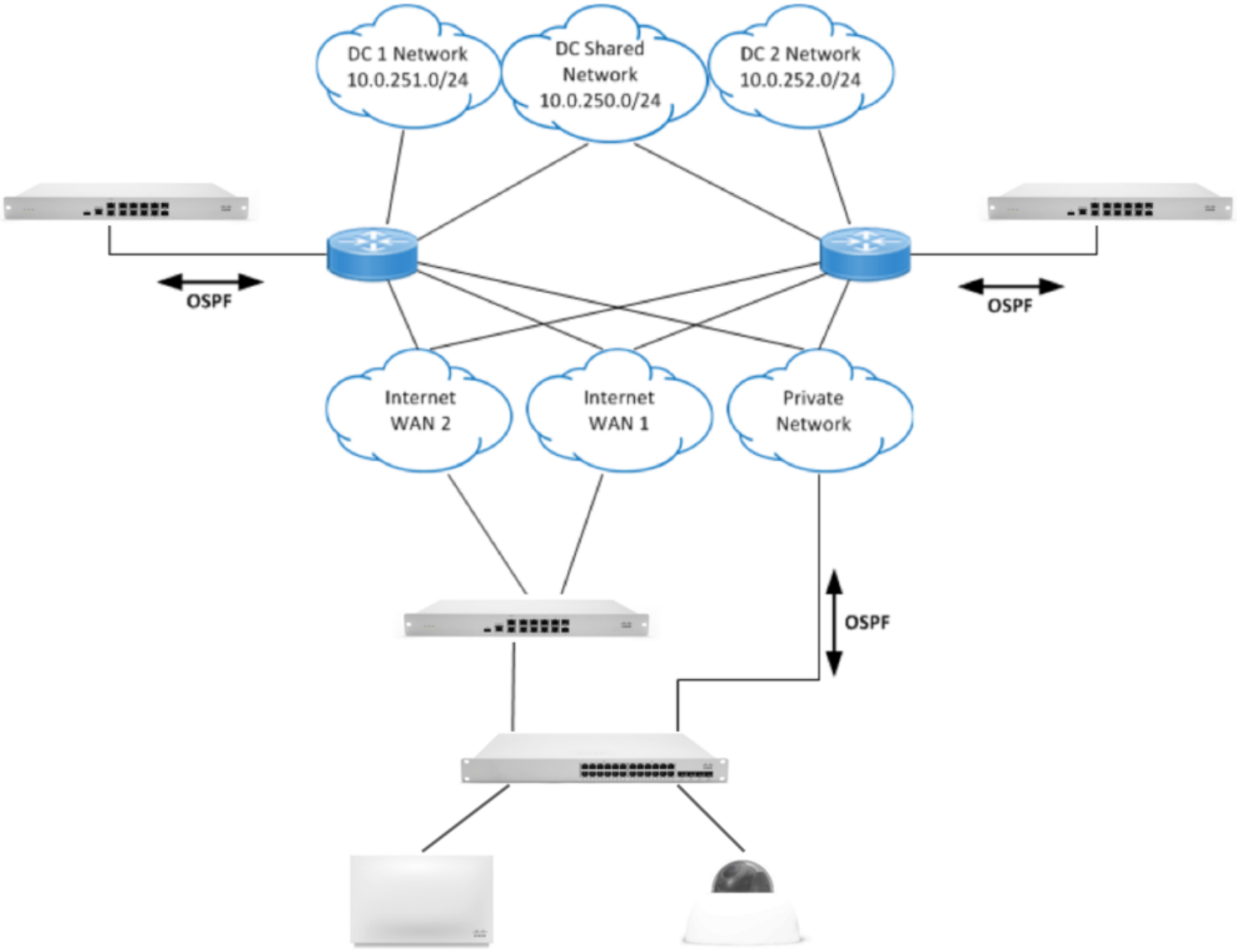


Figure 1: CMNO Lab Topology Diagram

Section A – Full Stack Configuration

In this first section of the lab, you will be setting up an entire stack of Meraki devices that represent various real-world architectures. As you progress through the labs, the exercises will have you evolve the network in ways that take advantage and utilize different features in order to address various needs of an organization.

Lab 1: Small / Medium Site

Exercise 1.1 – Initial MX Setup

1. Begin by first verifying that your MX appliance is operational (i.e. both WAN uplinks are healthy, MX is in good health status, firmware & configuration are up to date, etc.) on the **Monitor > Appliance status** page.

2. By default, the MX's name will appear as its MAC address - look for and click on the pencil icon which will allow you to change/edit the name. Proceed to rename the MX's name as "MX [**n**]" where **n** is your station number.

3. In a similar fashion, proceed to add/edit a physical (geographic) address. This can be your actual address, or one that you make up.

4. You will now proceed to set up the MX with various VLANs to be utilized by a variety of different traffic types. Navigate to **Configure > Addressing & VLANs** and proceed to enable VLANs and add the following local VLANs as per the information in the table below:

Important: Do not remove or change VLAN 1 (native/untagged VLAN) which is configured by default.

Name: Corp VLAN ID: 10	Subnet: 10.0. [10 + **n**] .0/24 MX IP: 10.0. [10 + **n**] .1
Name: Voice VLAN ID: 30	Subnet: 10.0. [30 + **n**] .0/24 MX IP: 10.0. [30 + **n**] .1

Name: Video VLAN ID: 50	Subnet: 10.0. [50 + **n**] .0/24 MX IP: 10.0. [50 + **n**] .1
Name: Guest VLAN ID: 100	Subnet: 10.0. [100 + **n**] .0/24 MX IP: 10.0. [100 + **n**] .1

5. Conclude your MX configuration by reserving a pool of IP addresses within VLAN 10 (Corp) for the addresses within the range of .150 through .250.

Hint: Navigate to the DHCP page for your security appliance and scroll down to the Corp VLAN to look for "Reserved IP ranges" where you can then make the above requested address reservations.

Exercise 1.2 – Setting up Security Policies on the MX

1. On your security appliance, create a Layer 7 firewall rule to completely block BitTorrent.

2. Take advantage of the MX's ability to traffic shape by enforcing a per-client bandwidth limit of 5 Mbps.

3. Add a new traffic shaping rule for Netflix and also Pandora - choose a limit of 1 Mbps down, 500 Kbps up on this rule with a "Low" priority.

4. Create another traffic shaping rule for all VoIP & video conferencing traffic – ignore network bandwidth restrictions for this rule and ensure the applications are treated as "High" priority.

5. Turn on (enable) content filtering for your MX by adding "Adult and Pornography" as a website category that will be blocked.

Additional Reading: To learn more about traffic classification, shaping, and prioritization, reference the following knowledge base document:
https://documentation.meraki.com/MX-Z/Firewall_and_Traffic_Shaping/Traffic_Shaping_Settings

6. Turn on (enable) Advanced Malware Protection within the threat protection mechanisms available for your MX. Also proceed to enable Intrusion Prevention and enforce a "Balanced" ruleset.

Exercise 1.3 – Interconnect All Sites with Auto VPN

1. Proceed to configure site-to-site VPN between your site (your lab station) with the other sites (other lab stations) by leveraging Auto VPN. To do this, start by going to **Configure > Site-to-site VPN** page and configuring your site as a hub – there is no need to configure an exit hub at the moment because we are deploying a split-tunnel VPN topology.

2. Proceed by enabling VPN for only the Corp and Voice networks/subnets. Look for the column "Use VPN" and select yes/no from the menu to enable/disable desired subnets.

3. Verify connectivity by pinging the data center core switch (10.0.250.1) from your MX and observe the latency from your site to the data center.

Hint: From your MX's appliance status page, click on the Tools tab to find the ping tool.

4. Navigate to **Monitor > VPN Status** to verify connectivity to other branches.

Hint: If you don't see site-to-site peers listed, try clicking the "View old version" link on the right hand side and you can then verify connectivity to other branches.

Exercise 1.4 – Initial Switch Setup

1. Begin by first verifying that your MS switch is online and operational (i.e. MS is in good health status, firmware & configuration are up to date, etc.) – you should see only one switch listed on the **Monitor > Switches** page.

2. By default, the MS's name will appear as its MAC address - look for and click on the pencil icon which will allow you to change/edit the name. Proceed to rename the MS's

name as “MS [n]” where n is your station number.

3. In this deployment, switch ports 15-18 will be designated specifically for voice (VoIP) traffic. Navigate to the Switch ports page and proceed to implement the following settings:
    - Tags: VoIP
    - PoE: Enabled
    - Type: Access
    - VLAN: 1
    - Voice VLAN: 30

4. On the switch ports page, you will be able to see the various devices that the network has identified through the discovery protocol packets if the column for “CDP/LLDP” has been added (if not, click the + icon on the top right of the table and check the box for “CDP/LLDP” to see that information). This is one of the several ways to identify various devices and where they are currently plugged into your wired infrastructure.

5. Identify the port that your MV21 security camera is connected to and proceed to configure this port with the following settings:
    - PoE: Enabled
    - Type: Access
    - VLAN: 50

Important: Now that these ports have been configured with proper VLAN designations, we need to ensure that the connected device pulls a new IP address on their respective, correct VLANs. We will force this action by performing a power cycle through the actions in the next step.

6. While on the **Monitor > Switch ports** page, check the boxes next to the port for your MV21 camera. Click the Edit button at the top of the table to open up the various configurations options and proceed to disable the port – look for the field named “Enabled” and select “disabled” from the drop-down menu. Click “Update 1 port” to process this action and the port should then shut down.

7. Wait a minimum of 30-60 seconds before reversing the process to re-enable the port. Select the port and “enabled” it with the drop-down menu to bring the port back up. This

should complete the process of cycling the device and it should now have an IP address in the correct VLAN.

Exercise 1.5 – Creating a Port Schedule

1. An energy-saving port schedule will need to be created/implemented in order to automatically turn off our VoIP phones during non-business hours to reduce our energy usage. Create a new schedule named "VoIP Power Saving" that will turn off ports during non-business hours (assume a Monday-Friday work schedule of 8:00 – 19:00).

2. Apply the "VoIP Power Saving" port schedule to the VoIP switch ports (15-18) from the **Monitor > Switch port** page.

Hint: For faster and more efficient bulk configuring, simply search do a search for the "VoIP" tag you created earlier and it should return just those 4 ports. Check the boxes next to these 4 ports and click "Edit" to configure them all simultaneously.

Exercise 1.6 – Initial Wireless Setup

1. Begin by first verifying that your MR access point is online and operational (i.e. MR is in good health status, firmware & configuration are up to date, etc.) – you should see only one AP listed on the **Monitor > Access points** page.

2. By default, the MR's name will appear as its MAC address - look for and click on the pencil icon which will allow you to change/edit the name. Proceed to rename the MR's name as "MR [**n**]" where **n** is your station number.

3. Navigate to **Configure > SSIDs** and proceed to enable as well as rename two SSIDs. Rename the first SSID as "Corporate" and the other as "Guest" – be sure to save your changes before leaving the page.

Hint: You should rename/repurpose the default SSID (usually named "LabX – Wireless WiFi") as one of the two SSIDs you are creating.

---

4. To configure settings for these SSIDs, go **Configure > Access control** where you must first make sure that the “Corporate” SSID has been selected from the SSID drop-down menu at the top. This SSID need to have the following settings:
   - Association Requirements: PreShared Key with WPA2, password: Meraki123
   - Client IP Assignment: Bridge mode
   - VLAN tagging: enabled, VLAN ID: 10

5. Switch to the “Guest” SSID by using the drop-down menu at the top, and give this SSID the following settings:
   - Splash page: Click-through
   - Client IP Assignment: Bridge mode
   - VLAN tagging: enabled, VLAN ID: 100

6. Because we are using a click-through splash page for our guest wireless network, we will want to have them re-authenticate every 30 minutes. Navigate to **Configure > Splash page** and change the frequency to every half hour.

7. Finally, we want to ensure that our wireless guest users have no way of accessing any of the internal local network resources while also restricting their usage. Go to **Configure > Firewall & traffic shaping** and make the following configurations on the “Guest” SSID:
   - Edit the default Layer 3 firewall by adjusting the policy to deny access to the Local LAN for all wireless clients that might try to access the LAN
   - Add three Layer 7 firewall rules to block P2P, File sharing, and Gaming services
   - Limit the per-client bandwidth to 1 Mbps

Lab 2: Large Site / Campus

Exercise 2.1 – Enable and Configure Routing on the Switch

1. Before we enable and configure OSPF routing on our network, we will first need to add some layer 3 interfaces. These will be created on the **Configure > Routing and DHCP** page of your switch. Add interfaces and create them using the following information:

Switch: (your switch) Name: Corp Subnet: 10.0. [10 + **n**] .0/24	Interface IP: 10.0. [10 + **n**] .201 VLAN: 10 Default Gateway: 10.0. [10 + **n**] .1 DHCP settings: Do not respond to DHCP requests
Switch: (your switch) Name: Legacy Subnet: 10.0. [150 + **n**] .0/24	Interface IP: 10.0. [150 + **n**] .1 VLAN: 150 DHCP settings: Run a DHCP server
Switch: (your switch) Name: OSPF Subnet: 192.168. [100 + **n**] .0/24	Interface: 192.168. [100 + **n**] . [**n**] VLAN: [600 + **n**] DHCP settings: Do not respond to DHCP requests

Additional Reading: To learn more about layer 3 routing capabilities on Meraki switches, reference the following knowledge base document:
https://documentation.meraki.com/MS/Layer_3_Switching/MS_Layer_3_Switching_Overview

2. Proceed by navigating to your MX security appliance's **Configure > Addressing & VLANs** page and create a static route to the "Legacy" subnet. This should have the following settings:
   - Name: Route to Legacy
   - Subnet: 10.0. [150 + **n**] .0/24
   - Next hop IP: 10.0. [10 + **n**] .201
   - In VPN: Yes

3. Go back to your switch and go to **Monitor > Switch ports** in order to configure port 24 of your switch to be an access port in VLAN [600 + **n**].

4. We are now ready to configure OSPF routing – start by navigating to **Configure > OSPF routing** and enable OSPF. Once it has been turned on, proceed with the following configurations:
   - Verify that the default backbone has an area ID of 0
   - Edit the Legacy and OSPF interfaces (click on their respective rows in the table) with default Area 0 and Cost 1
   - Verify that the default static route is to be preferred over OSPF routes

Exercise 2.2 – Routing Configuration Verification

A. Verify that switch port 24 is now operational

Hint: Go to your MS switch and look at port 24 specifically – you should see the switch with green/healthy status and not amber (usually an indicator that is has been blocked).

B. Verify that your switch is using 192.168. [100 + **n**] . [**n**] as the Router ID

Hint: You can find the Router ID by going to your switch and looking for it on the L3 Routing tab.

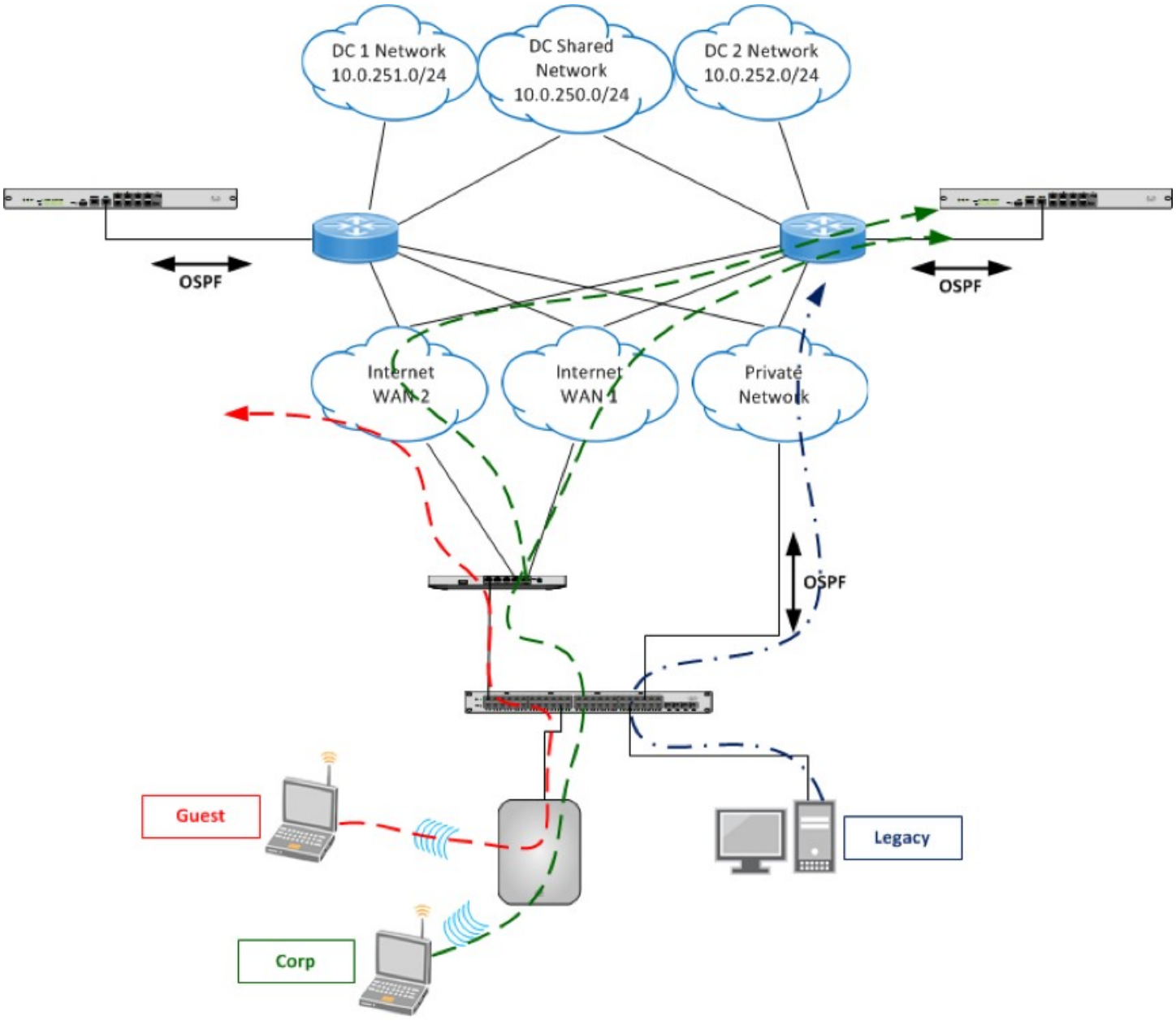
C. Verify that OSPF is functioning and that you can see the data center switch that should be listed as 10.0.250.1

D. Using the Ping tool (from the Tools tab of your switch) start a ping to the data center switch (10.0.250.1) from the Legacy Source interface (10.0. [150 + **n**] .1) – this should be a series of successful pings

E. Proceed by disabling port 24 and waiting 30-60 seconds. Attempt the same ping again as the previous verification – this should also be a successful ping

F. What path is the switch now taking to get to 10.0.250.1?

Hint: The topology diagrams seen below should help you understand the logical data flow of what is taking place when port 24 (the "MPLS" connection) has been disabled.



Important: Once you have finished the previous verification steps, be sure to go back and re-enable port 24 of your switch before proceeding to the next lab exercise.

Lab 3: Distributed Enterprise

Exercise 3.1 – VPN Topology and Redundancy

1. As the organization's network architecture expands, we will also evolve the VPN design to a more scalable model by implementing a hub-and-spoke topology while still leveraging Meraki MX's Auto VPN function. From the **Configure > Site-to-site VPN** page, start by re-configuring your site (lab station) as a spoke.

2. Add both "SF Data Center – DC 1" AND "NY Data Center – DC 2" as hubs but make sure that you prioritize the NY location as the primary hub.

Hint: You can drag and drop to rearrange your hubs, with the one at the top having higher priority and acting as the primary.

---

3. Make sure a full tunnel VPN is established by checking the default route boxes for both data center hubs.

4. Enable VPN for only the Corp and Voice networks/subnets.

Exercise 3.2 – VPN Verification

A. Verify that connectivity is still preserved to the other sites (the MX LAN IP's of the other lab stations)

Hint: Navigate to the Tools tab of your MX security appliance and using the ping tool.)

B. Verify connectivity to all 3 data center subnets:
   - Shared subnet (10.0.250.0/24): **10.0.250.1**
   - Data Center 1 subnet (10.0.251.0/24): **10.0.251.2**
   - Data Center 2 subnet (10.0.252.0/24): **10.0.252.2**

Exercise 3.3 – Configuring SD-WAN (Software-Defined WAN)

1. SD-WAN offers many features that can be enabled out-of-the-box across all Meraki MX devices. Navigate to **Configure > Traffic shaping** and start by configuring different uplink bandwidths. Set WAN 1 to 10 Mb and WAN 2 to 5 Mb.

2. Since we have two uplinks, we will also want to take advantage of those connections by enabling load balancing on our MX appliance – turn on this feature.

3. Our first Flow Preferences to configure is a rule for Internet traffic. Our networking team has mandated that all guest internet traffic should only traverse our ISP connection on WAN 2.

Hint: Any traffic (protocol) with a source IP address of 10.0. [100 + **n**] .0/24 – our guest subnet – outbound to any destination should prefer WAN 2 as the uplink.

4. Proceed by creating a custom performance class named "Acceptable Delay" with a setting of 200 ms maximum latency.

Note: After you have created this custom performance class, save your changes and refresh your Dashboard page before proceeding.

5. Under Flow Preferences, we will now create a few VPN traffic rules. The first rule will define how to treat outbound traffic destined for 8.8.8.8 (Google Public DNS). When prompted, use Custom expressions for your filter that defines the following:

Traffic Filter (Layer 3)		Policy	
Protocol	Any	Preferred uplink	WAN2
Source	Any (Src port: Any)	Failover if	Poor performance
Destination	8.8.8.8/32 (Src port: Any)	Performance class	Acceptable Delay

Hint: After defining the custom expression for your Traffic Filter, click the 'Add expression' button to save and then proceed to define the Policy portion of your flow preference. Also, if you are not seeing the Acceptable Delay performance class, go back to Step 4 to make sure you have created & saved it.

6. Similarly, a second preference should enforce that any traffic from the "Corp" subnet (10.0. [10 + **n**] .0/24) should load balance on uplinks that meet "Acceptable Delay":

Traffic Filter (Layer 3)		Policy	
Protocol	Any	Preferred uplink	Load balance
Source	10.0. [10 + **n**].0/24 (Src port: Any)	On uplinks that meet performance class	Acceptable Delay
Destination	Any (Src port: Any)		

Hint: If you are not able to select the Load Balance option, make sure you have enabled Load Balancing under the Global Preferences section.

7. Finally, a third preference should enforce that any traffic from the "Voice" (10.0. [30 + **n**] .0/24) subnet should use the best uplink for VoIP:

Traffic Filter (Layer 3)		Policy	
Protocol	Any	Preferred uplink	Best for VoIP
Source	10.0. [30 + **n**].0/24 (Src port: Any)		
Destination	Any (Src port: Any)		

Exercise 3.4 – SD-WAN Configuration Verification

A. On your MS switch, select any one of the L3 interfaces as the source and start a ping to 8.8.8.8 – this should be a consistent series with fairly low latency

B. In a new browser tab, open the **Monitor > VPN status** page of your MX appliance and scroll down to the Uplink Decision section/table to verify that these packets destined for 8.8.8.8 is in fact, using WAN 2

C. In the same section/table, look for the "Uplink decision" column and click one of the links (should be either WAN 1 or WAN 2) and observe the average latency and MOS score between your branch and the Data Center.

Lab 4: Physical Security

Exercise 4.1 – Initial Camera Setup

1. Start by identifying your camera on the **Monitor > Cameras** page and click on the camera's MAC address to see a live feed of the camera – by default this will be the "Video" tab. Look for the pencil icon which will allow you to change/edit the name of the camera and change it to "MV [**n**]" where **n** is your station number.

2. Switch to the "Network" tab and verify that the camera has an IP address from the proper subnet (VLAN 50), it is in good health status, and the firmware & configuration are up to date. On this tab will also be the Ping tool – use it to ensure the device is active and responding.

3. Move to the "Settings" tab and allow the low-latency stream to load. Feel free to adjust the various fields under the feed such as the optical zoom, focus, and aperture until you are satisfied.

4. Take note that there are three additional sub-tabs under settings: Zoom and Focus, Quality and Retention, and Night Mode. Our deployment requires a higher video quality recording, so be sure to use the Enhanced (765 kbps at 15fps) quality option.

Exercise 4.2 – Configuring a Video Wall

1. Even though we only have 1 camera for this site (lab station) we still want to become familiar with setting up a video wall. Navigate to **Monitor > Video Walls** to start building a custom layout.

2. Rename this layout tab (the default title is "New layout") and call it "My Wall".

3. Select your camera stream that appears down below and drag-and-drop the frame so it fills the entire window.

Note: Remember to click "Save layouts" near the upper-right corner of the Dashboard window when you are finished to save this video wall.

Lab 5: Enterprise Mobility Management

Exercise 5.1 – Device Enrollment

Important: If you do not have an iOS/Apple mobile device such as an iPhone or iPad, or if your iOS/Apple device is already enrolled in a different EMM/MDM solution, you may skip **Exercise 5.1** and proceed directly to **Exercise 5.2**.

1. To begin the enrollment process of your iOS/Apple mobile device, start by navigating to **MDM > Add devices** and click on the iOS selection (top-left option).

2. Follow the instructions on the screen to enroll your device in Systems Manager. The recommended method is to enter the 10-digit Network ID once you've navigated to m.meraki.com from your mobile device's browser.

Hint: As you progress through the enrollment process, be sure to click "Trust" and to accept all certificates or permission requests that pop up on your mobile device.

3. To verify that the enrollment was successful, go to **Monitor > Clients** (of Systems Manager) to look for your mobile device. Your device should also have automatically downloaded/installed the Systems Manager mobile app.

Exercise 5.2 – Configuring a Device Profile

1. To create a device profile within Systems Manager, navigate to **MDM > Settings** and click on the "Create a profile" button or the "+" icon near the upper-right corner.

2. Select the radio button for a "New Meraki managed profile" as that will give us access to the most number of configurable Systems Manager settings.

3. Name this profile "Corporate Devices" and then continue by defining the scope of the profile with the following settings:

- Apply to devices: with ANY of the following tags
- Device tags: create a tag named “corp”

Hint: When attempting to create the device tag, click on the field and type “corp” and look for “add option” to confirm/create this custom tag.

4. Now that we have defined (using tags) the scope that the profile will be pushed out to, we must define the various settings and restrictions. “Add settings” near the left side of the page will open up the full list of SM configurable options. Proceed to add the following:
   - Restrictions: remove the ability to use the camera on the device
   - Passcode: allow simple value, require alphanumeric values, and a minimum length of 6 characters
   - WiFi: use Sentry as the configuration type, your lab station’s wireless network, and have devices auto join your “Corporate” SSID

Note: Make sure to save all settings for this profile before navigating away.

Exercise 5.3 – Pushing and Removing a Device Profile

Important: If you previously skipped **Exercise 5.1** (device enrollment) then you will also skip **Exercise 5.3** (pushing/removing device profile) – simply proceed to Section B.

1. In order to implement the configurations on the device profiles, we will first select the desired devices by tagging them. From the **Monitor > Clients** page of Systems Manager, tag your device with the “corp” tag to push out the file.

2. If successful, your mobile device should be prompt you to configure a passcode with the complexity and length as previously defined. You should also be able to confirm that the other restrictions are also in effect by attempting to use the camera on your device (shortcuts to the camera app might have disappeared altogether).

3. Once you have confirmed the profile has been pushed, you may remove the SM profile from your device.

Additional Reading: Follow the instructions as outlined in the following knowledge base document to complete the un-enrollment process and fully remove the SM profile:
https://documentation.meraki.com/SM/Profiles_and_Settings/Removing_Profiles_and_Apps_from_Managed_Devices

*** End of Section A – Full Stack Configuration ***

(Please proceed to Section B – Troubleshooting)

Section B – Troubleshooting

In this section of the lab, your main objective will be to perform root cause analysis and troubleshooting of issues. The exercises in this portion are based on some of the most commonly reported and occurring problems that the Meraki Support Team frequently encounter. By successfully resolving these complications directly within Dashboard, you will be well equipped with the knowledge to quickly tackle them in real-world deployments.

Notifying Instructor for Lab Setup

Important: You must notify your CMNO instructor before proceeding to any of the exercises within Section B (troubleshooting) of the lab.

Once you have completed all of the labs and exercises of Section A, please notify your CMNO instructor that you are now ready for Section B (troubleshooting). This section of the lab requires some setup by the instructor that will take roughly 2-5 minutes per station to prepare.

> **Hi [*insert name of instructor*] – I have completed Section A of the lab and I'm ready to move onto Section B. I am lab station number [*insert station number*].**

Please let the instructor know within the Spark chatroom (preferably via a unicast/direct message) that you are ready to move on and what lab station number you are. Here is a sample message:

Once the instructor has finished setting up your lab station, they will notify you that it is okay to continue onto Section B. If they do not respond immediately, give them a few minutes as they may be tending to another lab station or helping to resolve an earlier inquiry.

Exercise 1 – Offline Device and Network Troubleshooting

Scenario: A new device (Meraki MR access point) needs to be brought onto the existing network infrastructure. The AP has been unboxed and plugged into the assigned Ethernet port in the wall, which is patched to a Meraki MS switch that is capable of delivering PoE. Most of the wireless settings have also already been properly configured, but several minutes have gone by and the AP is reported as unreachable or offline within Dashboard.

Objective: Your task is to troubleshoot the network infrastructure and apply the proper fixes needed in order to bring the AP online. There are multiple factors and root causes to this offline and inaccessible device. You should consider the following points when troubleshooting within Dashboard:

Hint: You are operating under the assumption that all physical (layer 1) connections are reliable and properly connected/designed. There are no bad cables or hardware issues to troubleshoot.

- What or where is the power source of the device? Is it functioning properly?
- What or where is the device plugged into? Is it configured to perform properly?
- Are there any misconfigurations along the path that the device is taking to get outbound (reach the internet)?

This exercise is completed once the MR access point is back online (green status in Dashboard) with an IP address and reachable (can be pinged with the “Ping AP” tool).

Exercise 2 – Bad IP Assignment

Scenario: Now that the access point is back online, the next step is to re-configure and assign the device onto the corporate VLAN since the address it received from the network (likely) is not in the proper subnet. The access point will need to continue pulling/receiving an IP address via DHCP – do not assign a static IP address to the device.

Objective: Your task will be to troubleshoot the network within the Dashboard to fix any misconfigurations that is contributing to the bad IP assignment. This exercise is completed once the AP has successfully pulled an IP address from the corporate VLAN (10).

Hint 1: Not mandatory, but by reconfiguring your VPN as split-tunnel (uncheck the boxes for Default Route for both NY & SF hubs) it could help facilitate the IP addressing for the access points into the proper VLAN.

Hint 2: Once you've made the necessary corrections, the recommended method of forcing the AP to pull a new IP address is by cycling the port – there are multiple ways to perform that action, including (but not limited to) disabling the port and re-enabling it.

Exercise 3 – No Connectivity Over Site-to-site VPN

Scenario: Great job so far! With the access point online and in the correct VLAN, we will need to ensure that all subsequent devices/clients that connect to the configured SSIDs are able to reach a database server at the main data center. That server is located in the San Francisco DC and has a static address of **10.0.251.2**.

Objective: Your task is to resolve any issues that would prevent a successful ping from the MR access point to that database server. This exercise is completed once you are able to establish a consistent and reliable ping test.

Hint 1: You should be leveraging the Ping tool from the MR access point for this exercise.

Hint 2: Some participants may be able to immediately ping the database server while others may not. This exercise is a built-in check to verify that you have properly configured the proper routes and site-to-site VPN topology from Section A. If you ARE able to ping it, you may move on the next exercise. If you are NOT able to ping it, then you have to perform troubleshooting until you are able to reach it – or else you will not receive full credit during the grading of your lab station.

Exercise 4 – Unreachable Device (Inaccessible MV Stream)

Scenario: Within the organization there's a separate networking and building infrastructure team. While the entire deployment has standardized on Meraki equipment, the separate teams are not on the same page. The MV cameras have been connected/patched to the right ports, but the physical security team is reporting them as unreachable within their Dashboard and can't see the live video stream.

Objective: Your task is to determine the root cause to the offline camera. This exercise is completed once the MV camera is back online within Dashboard and you can properly see a camera video stream.

Hint: If your MV camera already appears online and you are able to see a live camera feed, then it means that you did NOT properly configure your network to provide your MV camera with the proper IP addressing. Your MV should have an address along the lines of 10.0. [50 + n] .0 which is from VLAN 50. If it has an address similar to 192.168.1.0 then you must return to Section A to resolve that before proceeding.

There are multiple factors and root causes to this offline security camera. You should consider the following points when troubleshooting within Dashboard:

- The Dashboard uses a service called Cloud Proxy Stream to supply the camera feed to operators. Is there anything that is obstructing that service from communicating properly?
- Which VLAN/subnet is the MV camera configured for on the network? Is the traffic across that VLAN/subnet unobstructed across the entire outbound path for the device?

This exercise is completed once the MV security camera is back and reachable (can be pinged with the “Ping camera” tool) and you are able to see a live camera feed playing back in Dashboard.

*** End of Section B – Troubleshooting ***

(Please read the next section – Concluding the Lab)

Concluding the Lab

The following sections include important instructions regarding next steps and concluding the CMNO certification training course. This final portion of the lab guide will also include key information about follow-up communications and what to expect.

Lab Grading / Evaluation

As previously stated by the CMNO instructor, the biggest determining factor of your CMNO certification is the evaluation of your lab performance. Below are the answers to some commonly asked questions:

When are the lab stations graded?
The CMNO instructor will be grading all CMNO participant lab stations at the end of the day (typically after 4PM or approximately 7 hours from the start of the day) – please check with your instructor for specifics. If time permits, instructors may begin grading lab stations should participants finish early.

How are the lab stations graded or scored?
The CMNO instructor has an administrative view with full access to all CMNO lab stations. They will be checking each individual station for A.) **completion** and B.) **accuracy** of configurations across various lab exercises from Section A as well as Section B. Each exercise that passes the assessment will be added to the points needed by the participant to meet the required 80% threshold for a passing grade.

I've finished both Section A and Section B of the lab early, or due to other reasons have to leave the CMNO training early – what do I do?
If you've completed the lab to the best of your ability and would like to submit it for grading, please notify your instructor within the Spark chatroom. If you find yourself in the situation where you must exit the training, notify your instructor immediately and it will be handled on a case-by-case basis.

I didn't have enough time to complete both Section A and/or Section B – does that mean I've failed the CMNO certification?
No, not necessarily. We encourage you to attempt as many of the exercises as possible throughout the entire lab block of time during the day. During evaluation, the 80% passing threshold mark is looking at the entire lab as a whole (Section A + B combined).

Will the instructor tell me if I've passed or failed the certification before the end of the day?

No. Most CMNO instructors do not get around to fully grading each participant's lab stations until the end of the day. You may ask your instructor if they could grade your station early, but the standard procedure is that the grading and results will be communicated by the CMNO programs team within 7 business days after your training course has concluded.

Exiting the Lab

Whether you have finished early or if you've reached the end of the day according to the schedule, the process of exiting the lab is fairly simple and straight forward. You do not need to perform any actions other than to sign-out of your Dashboard session – this can be accomplished from the menu near the top-right of your browser window. Alternatively, you can also just close all web browser windows that have an active Dashboard.

Note: There is no need to delete or erase any configurations to your lab station within Dashboard. The CMNO team will perform a full lab reset at a later point in time in order to prepare the gear for a new group of participants.

You may also at this point sign out of the Cisco Spark chatroom. If you are using the web browser-based client, simply close the browser window. On the desktop client, you may choose to use the "Leave Team" function to close completely out of the training chatroom.

Post-training Communications and Resources

Within 7 business days after concluding the CMNO certification training, CMNO instructors will submit their pass/fail evaluations. Using these results, a system-generated e-mail will notify each participant of their certification status.

Note: On rare occasions the system-generated e-mail for CMNO certification status may get auto-rejected or filtered as spam by certain organizations. Please follow-up with the CMNO program team using the contact information below.

If you need to communicate with the CMNO program team with any follow-up questions or inquiries, they can be reached at cmno@meraki.com.

Frequently Asked Questions

It's been more than 7 business days since my CMNO session ended, but I have not received any follow-up e-mails or other forms of communication.
Course results are distributed automatically through e-mail and are occasionally diverted or filtered by an organization's mail servers – please double check your SPAM/junk folders. If after 7 business days you still have not received any communications from the CMNO program team, please reach out to cmno@meraki.com.

Will I receive a certificate when I pass the CMNO course?
Yes, all participants who successfully pass the CMNO course will receive an electronic certificate with a unique certification number. Please note that it may take up to 2 weeks for us to process your certificate.

Where can I obtain a copy of the CMNO training material?
A copy of the today's training material can be downloaded from the following links:

- Presentation: http://cs.co/cmno-presentation
- Lab Guide: http://cs.co/cmno-lab-guide

How can I provide positive/negative feedback about the CMNO certification training?
We appreciate your interest in helping us improve the course and value all constructive feedback! We've included a link to a feedback survey within the e-mail that includes your CMNO certification results.

Can the CMNO certification be associated with my CSCO training account?
No. As of this time the CMNO certification is not integrated with any of the Cisco training paths or accounts.

Can I post or use my CMNO certification in various business outlets or settings? (i.e. LinkedIn, e-mail signature)
Yes! If you successfully complete the course and receive the certification, you will receive an official e-mail signature included with your digital certificate.

I did not pass CMNO – when is the earliest that I can retake the certification course?
If you were not able to pass the CMNO course, you will be eligible to take the course again in 30 days. As the course is in high demand, we ask that customers who have failed the course wait 30 days to allow others the opportunity for a first attempt of the certification.

I had to leave early due to circumstances that were outside of my control – can I be fast-tracked and re-enrolled into a future CMNO session?
The CMNO program team takes into account that unforeseen circumstances are a part of our day-to-day. If something comes up and you need to leave the session early, please A.) notify your instructor and B.) reach out to cmno@meraki.com. The program team will make every attempt to accommodate you in an upcoming session.

Are there other Meraki-specific training resources available and where can I find them?

- Meraki Documentation: https://documentation.meraki.com
  Our official documentation portal not only contains the written articles on setting up and configuring your Meraki equipment but also contains a variety of other 'How-to' and 'Best Practices' papers that spans all technologies.
- Meraki Community: https://community.meraki.com
  A great source for technical discussion and advice with participants ranging from end-users to integrators to Meraki staff members as contributors. Registration and sign-in is simple with your Cisco.com CCO ID – sign in and join the conversation.