



**Cisco**

**500-220 Exam**

**Engineering Cisco Meraki Solutions**

**Thank you for Downloading 500-220 exam PDF Demo**

You can also try our 500-220 practice exam software

**Download Free Demo**

<https://prepbolt.com/500-220.html>

QUESTIONS & ANSWERS  
**DEMO VERSION**  
*(LIMITED CONTENT)*

# Version: 6.0

---

## Question: 1

---

DRAG DROP

Drag and drop the descriptions from the left onto the corresponding MX operation mode on the right.

The MX appliance acts as a layer 2 bridge	<b>Routed mode</b> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
This mode is the default mode of operation	
DHCP services can be configured on the MX appliance	
VLANs cannot be configured	
This mode is generally also the default gateway for devices on the LAN	<b>Passthrough mode</b> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
This mode is not recommended at the network perimeter	
No address translation is provided	
Client traffic to the internet has the source IP rewritten to match the WAN IP of the appliance	

---

**Answer:**

---

Explanation:

**Routed Mode:**

This mode is the default mode of operation

This mode is generally also the default gateway for devices on the LAN

Client traffic to the internet has the source IP rewritten to match the WAN IP of the appliance

DHCP services can be configured on the MX appliance

**Passthrough Mode:**

The MX appliance acts as a layer 2 bridge

VLANs cannot be configured

No address translation is provided

This mode is not recommended at the network perimeter

This question is related to the topic of MX Addressing and VLANs in the Cisco Meraki documentation.

You can find more information about this topic in the [MX Addressing and VLANs](#) article or the [General MX Best Practices](#) page.

---

**Question: 2**

---

When an SSID is configured with Sign-On Splash page enabled, which two settings must be configured for unauthenticated clients to have full network access and not be allow listed? (Choose two.)

- A. Controller disconnection behavior
- B. Captive Portal strength
- C. Simultaneous logins
- D. Firewall & traffic shaping
- E. RADIUS for splash page settings

---

**Answer: AB**

---

Explanation:

To clarify, when an SSID is configured with Sign-On Splash page enabled, the two settings that must be configured for unauthenticated clients to have full network access and not be allow listed are:  
Controller disconnection behavior: This setting determines how the clients are treated when the Meraki cloud controller is unreachable. The options are Restricted or Unrestricted. The former option blocks all traffic from unauthenticated clients until the controller is reachable again. [The latter option allows unauthenticated clients to access the network without signing on until the controller is reachable again1.](#)

Captive Portal strength: This setting determines how often the clients are redirected to the splash page for authentication. The options are Block all access until sign-on is complete or Allow non-HTTP traffic prior to sign-on. The latter option allows unauthenticated clients to access other protocols such as DNS, DHCP, ICMP, etc., but blocks HTTP and HTTPS traffic until they sign on. [This option is recommended for compatibility with devices that do not support web-based authentication1.](#)

Reference: [https://documentation.meraki.com/MR/Access\\_Control](https://documentation.meraki.com/MR/Access_Control)

---

**Question: 3**

---

Refer to the exhibit.

Uplink selection

**Global preferences**

Primary uplink

WAN 1 ▾

Load balancing

- Enabled  
Traffic will be spread across both uplinks in the proportions specified above. Management traffic to the Meraki cloud will use the primary uplink.
- Disabled  
All Internet traffic will use the primary uplink unless overridden by an uplink preference or if the primary uplink fails.

Active-Active AutoVPN

- Enabled  
Create VPN tunnels over all of the available uplinks (primary and secondary).
- Disabled  
Do not create VPN tunnels over the secondary uplink unless the primary uplink fails.

**Flow preferences**

Internet traffic

There are no uplink preferences for Internet traffic configured on this network.

[Add a preference](#)

SD-WAN policies

VPN traffic

**Uplink selection policy**

Use the uplink that's best for VoIP traffic. Prefer WAN 2. Fail over if poor performance for "Conf"

[Add a preference](#)

**Traffic filters**

All VoIP & video conferencing  
WebEx

Actions  
+ ×  
+ ×

Custom performance classes

Name	Maximum latency (ms)	Maximum jitter (ms)	Maximum loss (%)	Actions
Conf	200	50	5	×

[Create a new custom performance class](#)

Assuming this MX has established a full tunnel with its VPN peer, how will the MX route the WebEx traffic?

- A. WebEx traffic will prefer WAN 2 as long as it meets the thresholds in the "Conf" performance class.
- B. WebEx traffic will prefer WAN 1 as it is the primary uplink.
- C. WebEx traffic will prefer WAN 2 as long as it is up.
- D. WebEx traffic will be load-balanced between both active WAN links.

---

**Answer: A**

---

Explanation:

Assuming this MX has established a full tunnel with its VPN peer, the MX will route the WebEx traffic based on the SD-WAN policy configured in the exhibit. The SD-WAN policy has two performance classes: Conf and Default. [The Conf performance class matches the traffic with destination port 9000, which is used by WebEx for VoIP and video RTP3.](#) The Conf performance class has a preferred uplink of WAN 2 and a failover uplink of WAN 1. It also has thresholds for latency, jitter, and loss that determine when to switch from the preferred uplink to the failover uplink. Therefore, the WebEx traffic will prefer WAN 2 as long as it meets the thresholds in the Conf performance class. If WAN 2 exceeds the thresholds or goes down, the WebEx traffic will switch to WAN 1 as the failover uplink.

---

**Question: 4**

For which two reasons can an organization become "Out of License"? (Choose two.)

- A. licenses that are in the wrong network

- B. more hardware devices than device licenses
- C. expired device license
- D. licenses that do not match the serial numbers in the organization
- E. MR licenses that do not match the MR models in the organization

---

**Answer: BC**

---

Explanation:

More hardware devices than device licenses: An organization needs to have enough device licenses to cover all the hardware devices in its network. A device license is consumed by each device that is added to the network. [If the number of devices exceeds the number of licenses, the organization will be out of license and will lose access to some features and support until it purchases more licenses or removes some devices<sup>4</sup>.](#)

Expired device license: A device license has an expiration date that depends on the license term purchased by the organization. If a device license expires, it will no longer be valid and will not count towards the license limit. [The organization will need to renew the expired license or purchase a new one to avoid being out of license<sup>4</sup>.](#)

Reference:

[https://documentation.meraki.com/General\\_Administration/Licensing/Meraki\\_Licensing\\_FAQs](https://documentation.meraki.com/General_Administration/Licensing/Meraki_Licensing_FAQs)

---

### **Question: 5**

---

Refer to the exhibit.

**SD-WAN & traffic shaping**

**Uplink configuration**

WAN 1 4 Gbps [details](#)

WAN 2 4 Gbps [details](#)

Cellular Unlimited [details](#)

**Uplink statistics**

Test connectivity to	Description	Default	Actions
8.8.8.8	Google	<input checked="" type="radio"/>	<input type="checkbox"/>

[Add a destination](#)

**List update interval**

WAN 1

WAN 2

Cellular

**Uplink selection**

**Global preferences**

Primary uplink:

Load balancing:  Enabled  Disabled

**Flow preferences**

Internet traffic: There are no uplink preferences for Internet traffic configured on this network.

[Add a preference](#)

Which two actions are required to optimize load balancing asymmetrically with a 4:1 ratio between links? (Choose two.)

- A. Change the primary uplink to "none".
- B. Add an internet traffic preference that defines the load-balancing ratio as 4:1.
- C. Enable load balancing.
- D. Set the speed of the cellular uplink to zero.
- E. Change the assigned speeds of WAN 1 and WAN 2 so that the ratio is 4:1.

---

**Answer: CE**

---

Explanation:

To clarify, to optimize load balancing asymmetrically with a 4:1 ratio between links, two actions that are required are:

Enable load balancing: This option allows the MX to use both of its uplinks for load balancing. [When load balancing is enabled under Security & SD-WAN > Configure > SD-WAN & Traffic shaping, traffic flows will be distributed between the two uplinks proportional to the WAN 1 and WAN 2 bandwidths specified under Uplink configuration1.](#)

Change the assigned speeds of WAN 1 and WAN 2 so that the ratio is 4:1: The assigned speed of a WAN link is a value that indicates the bandwidth available on that link. [By changing the assigned speeds of WAN 1 and WAN 2 so that they reflect the desired load-balancing ratio, the administrator](#)

[can ensure that the MX uses both links efficiently and proportionally](#)<sup>1</sup>. For example, if WAN 1 has a bandwidth of 100 Mbps and WAN 2 has a bandwidth of 25 Mbps, then setting their assigned speeds to 100 Mbps and 25 Mbps respectively will achieve a 4:1 load-balancing ratio.

## Thank You for trying 500-220 PDF Demo

To try our 500-220 practice exam software visit link below

<https://prepbolt.com/500-220.html>

## Start Your 500-220 Preparation

Use Coupon "SAVE50" for extra 50% discount on the purchase of Practice Test Software. Test your 500-220 preparation with actual exam questions.