Cisco

Exam Questions 100-150

Cisco Certified Support Technician (CCST) Networking

NEW QUESTION 1
An engineer configured a new VLAN named VLAN2 for the Data Center team. When the team tries to ping addresses outside VLAN2 from a computer in VLAN2, they are unable to reach them. What should the engineer configure?

A. Additional VLAN
B. Default route
C. Default gateway
D. Static route

Answer: C

Explanation:
When devices within a VLAN are unable to reach addresses outside their VLAN, it typically indicates that they do not have a configured path to external networks. The engineer should configure a default gateway for VLAN2. The default gateway is the IP address of the router??s interface that is connected to the VLAN, which will route traffic from the VLAN to other networks12.
References :=
•Understanding and Configuring VLAN Routing and Bridging on a Router Using the IRB Feature
•VLAN 2 not able to ping gateway - Cisco Community
==========
•VLANs: Virtual Local Area Networks (VLANs) logically segment network traffic to improve security and performance. Devices within the same VLAN can communicate directly.
•Default Gateway: For devices in VLAN2 to communicate with devices outside their VLAN, they need a default gateway configured. The default gateway is typically a router or Layer 3 switch that routes traffic between different VLANs and subnets.
•Additional VLAN: Not needed in this scenario as the issue is related to routing traffic outside VLAN2, not creating another VLAN.
•Default Route: While a default route on the router may be necessary, the primary issue for devices within VLAN2 is to have a configured default gateway.
•Static Route: This is used on routers to manually specify routes to specific networks but does not address the need for a default gateway on the client devices.
References:
•Cisco VLAN Configuration Guide: Cisco VLAN Configuration
•Understanding and Configuring VLANs: VLANs Guide

NEW QUESTION 2
Which command will display the following output?

Image is command output that states the following.

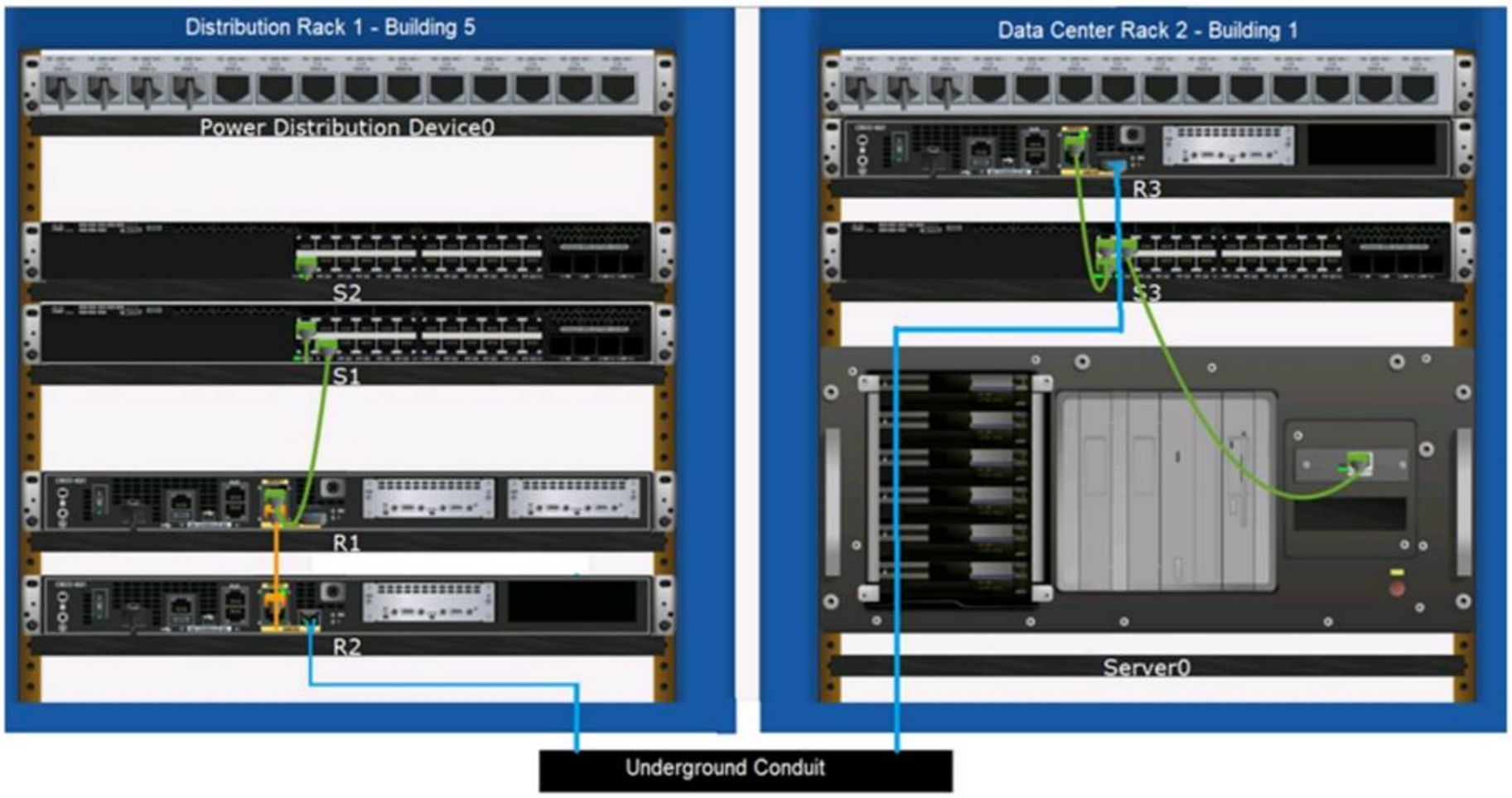
```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
esxi             Gig 0/5           177              S    VMware ES vmnic0
esxi             Gig 0/7           177              S    VMware ES vmnic1
esxi             Gig 0/6           177              S    VMware ES vmnic2
981888fc23a7     Gig 0/47          160            R S    Meraki MR Port 0
3456fecd1d08     Gig 0/1           178              S    MS120-8LP Port 9"
```

A. show mac-address-table
B. show cdp neighbor
C. show inventory
D. show ip interface

Answer: B

Explanation:
The command that will display the output provided, which includes capability codes, local interface details, device IDs, hold times, and platform port ID capabilities, is the show cdp neighbor command. This command is used in Cisco devices to display current information about neighboring devices detected by Cisco Discovery Protocol (CDP), which includes details such as the interface through which the neighbor is connected, the type of device, and the port ID of the device1.
References :=
•Cisco - show cdp neighbors
The provided output is from the Cisco Discovery Protocol (CDP) neighbor table. The show cdp neighbor command displays information about directly connected Cisco devices, including Device ID, Local Interface, Holdtime, Capability, Platform, and Port ID.
•A. show mac-address-table: Displays the MAC address table on the switch.
•C. show inventory: Displays information about the hardware inventory of the device.
•D. show ip interface: Displays IP interface status and configuration. Thus, the correct answer is B. show cdp neighbor.
References :=
•Cisco CDP Neighbor Command
•Understanding CDP

NEW QUESTION 3
DRAG DROP
Examine the connections shown in the following image. Move the cable types on the right to the appropriate connection description on the left. You may use each cable type more than once or not at all.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Based on the image description provided, here are the cable types matched with the appropriate connection descriptions:
Connects Switch S1 to Router R1 Gi0/0/1 interface Cable Type: = Straight-through UTP Cable
Connects Router R2 Gi0/0/0 to Router R3 Gi0/0/0 via underground conduit Cable Type: = Fiber Optic Cable
Connects Router R1 Gi0/0/0 to Router R2 Gi0/0/1 Cable Type: = Crossover UTP Cable Connects Switch S3 to Server0 network interface card Cable Type: = Straight-through UTP Cable
The choices are based on standard networking practices where:
? Straight-through UTP cables are typically used to connect a switch to a router or a network interface card.
? Fiber optic cables are ideal for long-distance, high-speed data transmission, such as connections through an underground conduit.
? Crossover UTP cables are used to connect similar devices, such as router-to- router connections.
These matches are consistent with the color-coded cables in the image: green for switch connections, yellow for router-to-router connections within the same rack, and blue for inter-rack connections. The use of these cables follows the Ethernet cabling standards.
? Connects Switch S1 to Router R1 Gi0/0/1 interface:
? Connects Router R2 Gi0/0/0 to Router R3 Gi0/0/0 via underground conduit:
? Connects Router R1 Gi0/0/0 to Router R2 Gi0/0/1:
? Connects Switch S3 to Server0 network interface card:
? Straight-through UTP Cable: Used to connect different devices (e.g., switch to router, switch to server).
? Crossover UTP Cable: Used to connect similar devices directly (e.g., router to
router, switch to switch).
? Fiber Optic Cable: Used for long-distance and high-speed connections, often between buildings or data centers.
References:
? Network Cable Types and Uses: Cisco Network Cables
? Understanding Ethernet Cabling: Ethernet Cable Guide

NEW QUESTION 4
For each statement about bandwidth and throughput, select True or False.
Note: You will receive partial credit for each correct selection.

For each statement about bandwidth and throughput, select **True** or **False**.

Note: You will receive partial credit for each correct selection.

Answer Area

	True	False
Low bandwidth can increase network latency.	○	○
High levels of network latency decrease network bandwidth.	○	○
You can increase throughput by decreasing network latency.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Statement 1: Low bandwidth can increase network latency.
? Statement 2: High levels of network latency decrease network bandwidth.
? Statement 3: You can increase throughput by decreasing network latency.
? Bandwidth vs. Latency: Bandwidth refers to the maximum rate at which data can be transferred over a network path. Latency is the time it takes for a data packet to travel from the source to the destination.
References:
? Network Performance Metrics: Cisco Network Performance
? Understanding Bandwidth and Latency: Bandwidth vs. Latency

NEW QUESTION 5
What is the purpose of assigning an IP address to the management VLAN interface on a Layer 2 switch?

A. To enable the switch to act as a default gateway for the attached devices
B. To enable the switch to resolve URLs for the attached the devices
C. To enable the switch to provide DHCP services to other switches in the network
D. To enable access to the CLI on the switch through Telnet or SSH

Answer: D

Explanation:
The primary purpose of assigning an IP address to the management VLAN interface on a Layer 2 switch is to facilitate remote management of the switch. By configuring an IP address on the management VLAN, network administrators can access the switch??s Command Line Interface (CLI) remotely using protocols such as Telnet or Secure Shell (SSH). This allows for convenient configuration changes, monitoring, and troubleshooting without needing physical access to the switch1.
References :=
•Understanding the Management VLAN
•Cisco - VLAN Configuration Guide
•Remote Management of Switches
Assigning an IP address to the management VLAN interface (often the VLAN 1 interface by default) on a Layer 2 switch allows network administrators to remotely manage the switch using protocols such as Telnet or SSH. This IP address does not affect the switch's ability to route traffic between VLANs but provides a means to access and configure the switch through its Command Line Interface (CLI).
•A: The switch does not act as a default gateway; this is typically a function of a Layer 3 device like a router.
•B: The switch does not resolve URLs; this is typically a function of DNS servers.
•C: The switch can relay DHCP requests but does not typically provide DHCP services itself; this is usually done by a dedicated DHCP server or router.
Thus, the correct answer is D. To enable access to the CLI on the switch through Telnet or SSH.
References :=
•Cisco VLAN Management Overview
•Cisco Catalyst Switch Management

NEW QUESTION 6
DRAG DROP
Move each cloud computing service model from the list on the left to the correct example on the right
Note: You will receive partial credit for each correct answer.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Three virtual machines are connected by a virtual network in the cloud.
? Users access a web-based graphics design application in the cloud for a monthly fee.
? A company develops applications using cloud-based resources and tools.
? IaaS (Infrastructure as a Service): Provides virtualized hardware resources that customers can use to build their own computing environments.
? PaaS (Platform as a Service): Offers a platform with tools and services to develop,
test, and deploy applications.
? SaaS (Software as a Service): Delivers fully functional applications over the internet that users can access and use without managing the underlying infrastructure.
References:
? Cloud Service Models: Understanding IaaS, PaaS, SaaS
? NIST Definition of Cloud Computing: NIST Cloud Computing

NEW QUESTION 7
Which wireless security option uses a pre-shared key to authenticate clients?

A. WPA2-Personal
B. 802.1x
C. 802.1q
D. WPA2-Enterprise

Answer: A

Explanation:
WPA2-Personal, also known as WPA2-PSK (Pre-Shared Key), is the wireless security
option that uses a pre-shared key to authenticate clients. This method is designed for home and small office networks and doesn??t require an authentication server. Instead, every user on the network uses the same key or passphrase to connect1.
References :=
•What is a Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)?
•Exploring WPA-PSK and WiFi Security
==========
•WPA2-Personal: This wireless security option uses a pre-shared key (PSK) for authentication. Each client that connects to the network must use this key to gain access. It is designed for home and small office networks where simplicity and ease of use are important.
•WPA2-Enterprise: Unlike WPA2-Personal, WPA2-Enterprise uses 802.1x authentication with an authentication server (such as RADIUS) and does not rely on a pre-shared key.
•802.1x: This is a network access control protocol for LANs, particularly wireless LANs. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
•802.1q: This is a networking standard that supports VLAN tagging on Ethernet networks and is not related to wireless security.
References:
•Cisco Documentation on WPA2 Security: Cisco WPA2
•Understanding Wireless Security: Wireless Security Guide

NEW QUESTION 8
Which two pieces of information should you include when you initially create a support ticket? (Choose 2.)

A. A detailed description of the fault
B. Details about the computers connected to the network
C. A description of the conditions when the fault occurs
D. The actions taken to resolve the fault
E. The description of the top-down fault-finding procedure

Answer: AC

Explanation:
? Statement A: "A detailed description of the fault." This is essential for support staff to understand the nature of the problem and begin troubleshooting effectively.
? Statement C: "A description of the conditions when the fault occurs." This helps in reproducing the issue and identifying patterns that might indicate the cause of the fault.
? Statement B: "Details about the computers connected to the network." While useful, this is not as immediately critical as understanding the fault itself and the

conditions under which it occurs.
? Statement D: "The actions taken to resolve the fault." This is important but typically follows the initial report.
? Statement E: "The description of the top-down fault-finding procedure." This is more of a troubleshooting methodology than information typically included in an initial support ticket.
References:
? Best Practices for Submitting Support Tickets: Support Ticket Guidelines

NEW QUESTION 9
Which device protects the network by permitting or denying traffic based on IP address, port number, or application?

A. Firewall
B. Access point
C. VPN gateway
D. Intrusion detection system

Answer: A

Explanation:
? Firewall: A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It permits or denies traffic based on IP addresses, port numbers, or applications.
? Access Point: This is a device that allows wireless devices to connect to a wired network using Wi-Fi. It does not perform traffic filtering based on IP, port, or application.
? VPN Gateway: This device allows for secure connections between networks over the internet, but it is not primarily used for traffic filtering based on IP, port, or application.
? Intrusion Detection System (IDS): This device monitors network traffic for suspicious activity and policy violations, but it does not actively permit or deny traffic.
References:
? Understanding Firewalls: Firewall Basics

NEW QUESTION 10
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

100-150 Practice Exam Features:

* 100-150 Questions and Answers Updated Frequently

* 100-150 Practice Questions Verified by Expert Senior Certified Staff

* 100-150 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 100-150 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year