Exam Code: CCST Networking

Exam Name: Cisco Certified Support Technician (CCST) Networking

QUESTION 1
You want to store files that will be accessible by every user on your network.
Which endpoint device do you need?

A. Access point

B. Server

C. Hub

D. Switch

Correct Answer: B
Section:
Explanation:
To store files that will be accessible by every user on a network, you would need a server. A server is a computer system that provides data to other computers. It can serve data to systems on a local network (LAN) or a wide network (WAN) over the internet. In this context, a file server would be set up to store and manage files, allowing users on the network to access them from their own devices1.
What is a Server?
Understanding Servers and Their Functions
A server is a computer designed to process requests and deliver data to other computers over a local network or the internet. In this case, to store files that will be accessible by every user on the network, a file server is the appropriate endpoint device. It provides a centralized location for storing and managing files, allowing users to access and share files easily.
A . Access point: Provides wireless connectivity to a network.
C . Hub: A basic networking device that connects multiple Ethernet devices together, making them act as a single network segment.
D . Switch: A networking device that connects devices on a computer network by using packet switching to forward data to the destination device.
Thus, the correct answer is B. Server.
File Server Overview (Cisco)
Server Roles in Networking (Cisco)
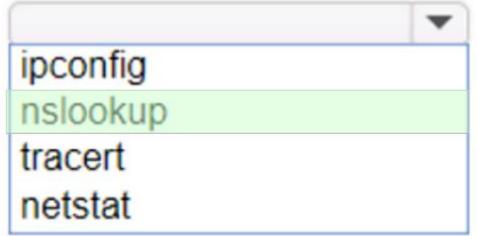
QUESTION 2
HOTSPOT
You want to list the IPv4 addresses associated with the host name www.companypro.net.
Complete the command by selecting the correct option from each drop-down list.

Hot Area:

Answer Area:

Section:
Explanation:
Using nslookup: nslookup Command Guide

QUESTION 3
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

Correct Answer: A, C
Section:
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.
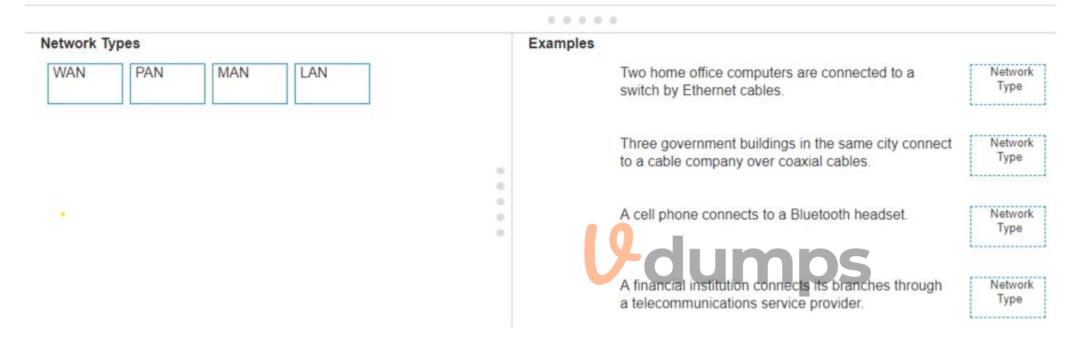
Statement E: 'The description of the top-down fault-finding procedure.' This is more of a troubleshooting methodology than information typically included in an initial support ticket.

Best Practices for Submitting Support Tickets: Support Ticket Guidelines

QUESTION 4
DRAG DROP
Move each network type from the list on the left to the correct example on the right.

Select and Place:

Network Types	Examples	
WAN PAN MAN LAN	Two home office computers are connected to a switch by Ethernet cables.	Network Type
	Three government buildings in the same city connect to a cable company over coaxial cables.	Network Type
	A cell phone connects to a Bluetooth headset.	Network Type
	A financial institution connects its branches through a telecommunications service provider.	Network Type

Correct Answer:

Network Types	Examples	
	Two home office computers are connected to a switch by Ethernet cables.	WAN
	Three government buildings in the same city connect to a cable company over coaxial cables.	MAN
	A cell phone connects to a Bluetooth headset.	PAN
	A financial institution connects its branches through a telecommunications service provider.	LAN

Section:
Explanation:

Network Types Overview: Cisco Networking Basics
Understanding Different Network Types: Network Types Guide

QUESTION 5
HOTSPOT
You plan to use a network firewall to protect computers at a small office.
For each statement about firewalls, select True or False.
Note: You will receive partial credit for each correct selection.

Hot Area:

	True	False
A firewall can direct all web traffic to a specific IP address.	○	○
A firewall can block traffic to specific ports on internal computers.	○	○
A firewall can prevent specific apps from running on a computer.	○	○

Answer Area:

	True	False
A firewall can direct all web traffic to a specific IP address.	☑	○
A firewall can block traffic to specific ports on internal computers.	☑	○
A firewall can prevent specific apps from running on a computer.	○	☑

Section:
Explanation:
Understanding Firewalls: Firewall Capabilities
Network Security Best Practices: Network Security Guide

QUESTION 6
DRAG DROP
Move each protocol from the list on the left to the correct TCP/IP model layer on the right.
Note: You will receive partial credit for each correct match.

Select and Place:

Protocols

| TCP | IP | FTP | Ethernet |

TCP Model Layer

Application	Protocol
Transport	Protocol
Internetwork	Protocol
Network	Protocol

Correct Answer:

Protocols

TCP Model Layer

Application	FTP
Transport	TCP
Internetwork	IP
Network	Ethernet

Section:
Explanation:
TCP/IP Model Overview: Cisco TCP/IP Model
Understanding the TCP/IP Model: TCP/IP Layers

QUESTION 7
HOTSPOT
An app on a user's computer is having problems downloading data. The app uses the following URL to download data:
https://www.companypro.net:7100/api
You need to use Wireshark to capture packets sent to and received from that URL.
Which Wireshark filter options would you use to filter the results? Complete the command by selecting the correct option from each drop-down list.
Note: You will receive partial credit for each correct selection.

Hot Area:

tcp	.	port	==	7100
udp		user_agent		companypro.net
				http

Answer Area:

tcp	.	port	==	7100
udp		user_agent		companypro.net
				http

Explanation:
Wireshark Filters: Wireshark Display Filters

QUESTION 8
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

Correct 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.
* 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.
* Cisco VLAN Configuration Guide: Cisco VLAN Configuration
* Understanding and Configuring VLANs: VLANs Guide

QUESTION 9
A host is given the IP address 172.16.100.25 and the subnet mask 255.255.252.0.
What is the CIDR notation for this address?

A. 172.16.100.25 /23

B. 172.16.100.25 /20

C. 172.16.100.25 /21

D. 172.16.100.25 /22

Correct Answer: D
Explanation:
The CIDR (Classless Inter-Domain Routing) notation for the subnet mask 255.255.252.0 is /22. This notation indicates that the first 22 bits of the IP address are used for network identification, and the remaining bits are used for host addresses within the network1.
* Subnet Cheat Sheet -- 24 Subnet Mask, 30, 26, 27, 29, and other IP Address CIDR Network Reference
=========================
* Subnet Mask to CIDR Notation: The given subnet mask is 255.255.252.0. To convert this to CIDR notation:
* Convert the subnet mask to binary: 11111111.11111111.11111100.00000000

* Count the number of consecutive 1s in the binary form: There are 22 ones.
* Therefore, the CIDR notation is /22.
* Understanding Subnetting and CIDR: Cisco CIDR Guide

QUESTION 10
You need to connect a computer's network adapter to a switch using a 1000BASE-T cable.
Which connector should you use?

A. Coax

B. RJ-11

C. OS2 LC

D. RJ-45

Correct Answer: D
Section:
Explanation:
* 1000BASE-T Cable: This refers to Gigabit Ethernet over twisted-pair cables (Cat 5e or higher).
* Connector: RJ-45 connectors are used for Ethernet cables, including those used for 1000BASE-T.
* Coax: Used for cable TV and older Ethernet standards like 10BASE2.
* RJ-11: Used for telephone connections.
* OS2 LC: Used for fiber optic connections.
* Ethernet Standards and Cables: Ethernet Cable Guide

QUESTION 11
A Cisco switch is not accessible from the network. You need to view its running configuration.
Which out-of-band method can you use to access it?

A. SNMP

B. Console

C. SSH

D. Telnet

Correct Answer: B
Section:
Explanation:

When a Cisco switch is not accessible from the network, the recommended out-of-band method to access its running configuration is through the console port. Out-of-band management involves accessing the network device through a dedicated management channel that is not part of the data network. The console port provides direct access to the switch's Command Line Interface (CLI) without using the network, which is essential when the switch cannot be accessed remotely via the network12.
Out-of-band (OOB) network interface configuration guidelines

Out of band management configuration
==========================
If you have any more questions or need further assistance, feel free to ask!

QUESTION 12
A user reports that a company website is not available. The help desk technician issues a tracert command to determine if the server hosting the website is reachable over the network. The output of the command is shown as follows:

```
C:\>tracert 192.168.1.10
Tracing route to 192.168.1.10 over a maximum of 30 hops:
1  0 ms   0 ms   1 ms   192.168.5.1
2  1 ms   0 ms   0 ms   10.0.1.1
3  *      *      *      Request timed out.
4  1 ms   1 ms   0 ms   10.0.0.2
5  1 ms   1 ms   0 ms   192.168.1.10
```

What can you tell from the command output?

A. The router at hop 3 is not forwarding packets to the IP address 192.168.1.10.
B. The server address 192.168.1.10 is being blocked by a firewall on the router at hop 3.
C. The server with the address 192.168.1.10 is reachable over the network.
D. Requests to the web server at 192.168.1.10 are being delayed and time out.

Correct Answer: C
Section:
Explanation:
The tracert command output shows the path taken to reach the destination IP address, 192.168.1.10. The command output indicates:
* Hops 1 and 2 are successfully reached.
* Hop 3 times out, meaning the router at hop 3 did not respond to the tracert request. However, this does not necessarily indicate a problem with forwarding packets, as some routers may be configured to block or not respond to ICMP requests.
* Hops 4 and 5 are successfully reached, with hop 5 being the destination IP 192.168.1.10, indicating that the server is reachable.
Thus, the correct answer is C. The server with the address 192.168.1.10 is reachable over the network.
* Cisco Traceroute Command
* Understanding Traceroute
The tracert command output indicates that the server with the address 192.168.1.10 is reachable over the network. The asterisk (*) at hop 3 suggests that the probe sent to that hop did not return a response, which could be due to a variety of reasons such as a firewall blocking ICMP packets or the router at that hop being configured not to respond to ICMP requests. However, since the subsequent hops (4 and 5) are showing response times, it means that the packets are indeed getting through and the server is reachable12.
* How to Use Traceroute Command to Read Its Results
* How to Use the Tracert Command in Windows

QUESTION 13
Which wireless security option uses a pre-shared key to authenticate clients?

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

D. WPA2-Enterprise

Correct Answer: A
Section:
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.
* 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.
* Cisco Documentation on WPA2 Security: Cisco WPA2
* Understanding Wireless Security: Wireless Security Guide

QUESTION 14
What is the most compressed valid format of the IPv6 address 2001 :0db8:0000:0016:0000:001b: 2000:0056?

A. 2001:db8: : 16: : 1b:2:56
B. 2001:db8: : 16: : 1b: 2000: 56
C. 2001:db8: 16: :1b:2:56
D. 2001:db8: 0:16: :1b: 2000:56

Correct Answer: D
Section:
Explanation:
IPv6 addresses can be compressed by removing leading zeros and replacing consecutive groups of zeros with a double colon (::). Here's how to compress the address 2001:0db8:0000:0016:0000:001b:2000:0056:
Remove leading zeros from each segment:
2001:db8:0000:0016:0000:001b:2000:0056 becomes 2001:db8:0:16:0:1b:2000:56
Replace the longest sequence of consecutive zeros with a double colon (::). In this case, the two consecutive zeros between the 16 and 1b:
2001:db8:0:16::1b:2000:56
Thus, the most compressed valid format of the IPv6 address is 2001:db8:0:16::1b:2000:56.
Cisco Learning Network
IPv6 Addressing (Cisco)

QUESTION 15
HOTSPOT
For each statement about bandwidth and throughput, select True or False.
Note: You will receive partial credit for each correct selection.

Hot Area:

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.	○	○

Answer Area:

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.	⦿	○

Section:
Explanation:
Network Performance Metrics: Cisco Network Performance
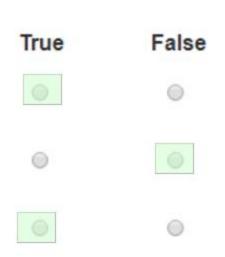Understanding Bandwidth and Latency: Bandwidth vs. Latency

QUESTION 16
DRAG DROP
Move each protocol from the list on the left to its correct example on the right.

Select and Place:

Move each protocol from the list on the left to its correct example on the right.

⬤ ⬤ ⬤ ⬤ ⬤

Protocols			Examples	
DHCP	DNS	ICMP	Perform a query to translate companypro.net to an IP address.	Protocol
			Assign the reserved IP address 10.10.10.200 to a web server at your company.	Protocol
			Perform a ping to ensure that a server is responding to network connections.	Protocol

Correct Answer:

Move each protocol from the list on the left to its correct example on the right.

Protocols			Examples	
			Perform a query to translate companypro.net to an IP address.	DNS
			Assign the reserved IP address 10.10.10.200 to a web server at your company.	DHCP
			Perform a ping to ensure that a server is responding to network connections.	ICMP

Section:
Explanation:
DNS Basics: What is DNS?
DHCP Overview: What is DHCP?
ICMP and Ping: Understanding ICMP

QUESTION 17
Which standard contains the specifications for Wi-Fi networks?

A. GSM
B. LTE
C. IEEE 802.11
D. IEEE 802.3
E. EIA/TIA 568A

Correct Answer: C
Section:
Explanation:
The IEEE 802.11 standard contains the specifications for Wi-Fi networks. It is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in various frequencies, including but not limited to 2.4 GHz, 5 GHz, and 6 GHz1. This standard is maintained by the Institute of Electrical and Electronics Engineers (IEEE) and is commonly referred to as Wi-Fi. The standard has evolved over time to include several amendments that improve speed, range, and reliability of wireless networks.
* The Most Common Wi-Fi Standards and Types, Explained
* 802.11 Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a
* Wi-Fi Standards Explained - GeeksforGeeks
========================

QUESTION 18
A user initiates a trouble ticket stating that an external web page is not loading. You determine that other resources both internal and external are still reachable.
Which command can you use to help locate where the issue is in the network path to the external web page?

A. ping -t
B. tracert
C. ipconfig/all
D. nslookup

Correct Answer: B
Section:

Explanation:

The tracert command is used to determine the route taken by packets across an IP network. When a user reports that an external web page is not loading, while other resources are accessible, it suggests there might be an issue at a certain point in the network path to the specific web page. The tracert command helps to diagnose where the breakdown occurs by displaying a list of routers that the packets pass through on their way to the destination. It can identify the network segment where the packets stop progressing, which is valuable for pinpointing where the connectivity issue lies. Reference := Cisco CCST Networking Certification FAQs -- CISCONET Training Solutions, Command Prompt (CMD): 10 network-related commands you should know, Network Troubleshooting Commands Guide: Windows, Mac & Linux - Comparitech, How to Use the Traceroute and Ping Commands to Troubleshoot Network, Network Troubleshooting Techniques: Ping, Traceroute, PathPing.

* tracert Command: This command is used to determine the path packets take to reach a destination. It lists all the hops (routers) along the way and can help identify where the delay or failure occurs.
* ping -t: This command sends continuous ping requests and is useful for determining if a host is reachable but does not provide path information.
* ipconfig /all: This command displays all current TCP/IP network configuration values and can be used to verify network settings but not to trace a network path.
* nslookup: This command queries the DNS to obtain domain name or IP address mapping, useful for DNS issues but not for tracing network paths.
* Microsoft tracert Command: tracert Command Guide
* Troubleshooting Network Issues with tracert: Network Troubleshooting Guide
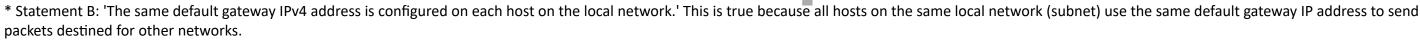
QUESTION 19
Which two statements are true about the IPv4 address of the default gateway configured on a host? (Choose 2.)
Note: You will receive partial credit for each correct selection.

A. The IPv4 address of the default gateway must be the first host address in the subnet.

B. The same default gateway IPv4 address is configured on each host on the local network.

C. The default gateway is the Loopback0 interface IPv4 address of the router connected to the same local network as the host.

D. The default gateway is the IPv4 address of the router interface connected to the same local network as the host.

E. Hosts learn the default gateway IPv4 address through router advertisement messages.

Correct Answer: B, D
Section:
Explanation:
* Statement B: 'The same default gateway IPv4 address is configured on each host on the local network.' This is true because all hosts on the same local network (subnet) use the same default gateway IP address to send packets destined for other networks.
* Statement D: 'The default gateway is the IPv4 address of the router interface connected to the same local network as the host.' This is true because the default gateway is the IP address of the router's interface that is directly connected to the local network.
* Statement A: 'The IPv4 address of the default gateway must be the first host address in the subnet.' This is not necessarily true. The default gateway can be any address within the subnet range.
* Statement C: 'The default gateway is the Loopback0 interface IPv4 address of the router connected to the same local network as the host.' This is not true; the default gateway is the IP address of the router's physical or logical interface connected to the local network.
* Statement E: 'Hosts learn the default gateway IPv4 address through router advertisement messages.' This is generally true for IPv6 with Router Advertisement (RA) messages, but not typically how IPv4 hosts learn the default gateway address.
* Cisco Default Gateway Configuration: Cisco Default Gateway

QUESTION 20
Which address is included in the 192.168.200.0/24 network?

A. 192.168.199.13

B. 192.168.200.13

C. 192.168.201.13

D. 192.168.1.13

Correct Answer: B
Section:
Explanation:

* 192.168.200.0/24 Network: This subnet includes all addresses from 192.168.200.0 to 192.168.200.255. The /24 indicates a subnet mask of 255.255.255.0, which allows for 256 addresses.
* 192.168.199.13: This address is in the 192.168.199.0/24 subnet, not the 192.168.200.0/24 subnet.
* 192.168.200.13: This address is within the 192.168.200.0/24 subnet.
* 192.168.201.13: This address is in the 192.168.201.0/24 subnet, not the 192.168.200.0/24 subnet.
* 192.168.1.13: This address is in the 192.168.1.0/24 subnet, not the 192.168.200.0/24 subnet.
* Subnetting Guide: Subnetting Basics