Exam

N10-009

CompTIA Network+ (V9)

Free demo	80 sample questions
Full exam	594 questions with answers and explanations
Contents	Questions with answers and explanations

Exam domains

Domain	Exam weight	Questions
D1 Networking concepts		16
D2 Network implementation		23
D3 Network operations		9
D4 Network security		17
D5 Network troubleshooting		15

This is a free demo from Dumpsgate: 80 of the exam's 594 questions. **Get the full N10-009 exam** with every question, answer and explanation.

Question 1

Single choice · Domain: D1 Networking concepts › Identify administrative distance values for routing protocols, specifically internal BGP

Which of the following is the administrative distance for internal BGP routes?

A. 20
B. 110
C. 170
D. 200

Answer: D. 200

Explanation

This question tests knowledge of how administrative distance ranks the trustworthiness of routes learned from different routing protocols. Internal BGP routes have an administrative distance of 200 on Cisco platforms.

✗ **A** 20
Incorrect. An administrative distance of 20 is commonly assigned to external BGP (eBGP), not internal BGP (iBGP).
https://www.comptia.org/certifications/network

✗ **B** 110
Incorrect. An administrative distance of 110 is commonly assigned to OSPF routes.
https://www.comptia.org/certifications/network

✗ **C** 170
Incorrect. An administrative distance of 170 is not the standard value for internal BGP routes.
https://www.comptia.org/certifications/network

✓ **D** 200
Correct. Internal BGP (iBGP) routes have an administrative distance of 200 on Cisco routers.
https://www.comptia.org/certifications/network

Question 2

Single choice · Domain: D1 Networking concepts › Identify and apply PTR records for reverse DNS lookups

A network engineer troubleshoots an issue with an SMTP relay server. The engineer suspects the issue is related to a reverse DNS lookup failure. Which of the following should the engineer implement to resolve the issue?

A. DNSSEC
B. MX
C. DoT
D. PTR

Free demo · full exam: 594 questions

Answer: D. PTR

Explanation

This question tests recognition of the DNS record type used to map an IP address back to a hostname. PTR records provide reverse DNS resolution, which can be required for SMTP relay validation.

✗ **A** DNSSEC
Incorrect. DNSSEC authenticates DNS data and helps prevent tampering, but it does not perform reverse DNS lookups.

https://www.comptia.org/content/guides/what-is-dns

✗ **B** MX
Incorrect. An MX record identifies the mail server responsible for receiving mail for a domain; it does not map an IP address to a hostname.

https://www.comptia.org/content/guides/what-is-dns

✗ **C** DoT
Incorrect. DNS over TLS encrypts DNS queries between a client and resolver, but it does not create the reverse DNS record needed to map an IP address to a hostname.

https://www.comptia.org/content/guides/what-is-dns

✓ **D** PTR
Correct. A PTR record supports reverse DNS by mapping an IP address to a hostname. SMTP systems commonly use reverse DNS during relay or sender validation.

https://www.comptia.org/content/guides/what-is-dns

Question 3

Single choice · Domain: D1 Networking concepts › Identify IPv4 address classes and their associated traffic types

Which of the following traffic types uses Class D IP address space?

A. Multicast
B. Anycast
C. Broadcast
D. Unicast

Answer: A. Multicast

Explanation

This question tests recognition that IPv4 Class D addresses are reserved for multicast traffic. Class D occupies the 224.0.0.0 through 239.255.255.255 range.

✓ **A** Multicast
Correct. Class D IPv4 address space is reserved for multicast traffic, which delivers packets to multiple subscribed hosts.

https://www.comptia.org/content/guides/what-is-an-ip-address

Free demo · full exam: 594 questions

✗ **B** Anycast
Incorrect. Anycast uses the same unicast address on multiple nodes and is routed to the nearest or best destination; it is not associated with Class D address space.
https://www.comptia.org/content/guides/what-is-an-ip-address

✗ **C** Broadcast
Incorrect. Broadcast traffic is sent to all hosts within a broadcast domain and commonly uses a subnet's broadcast address, not Class D address space.
https://www.comptia.org/content/guides/what-is-an-ip-address

✗ **D** Unicast
Incorrect. Unicast traffic is sent from one host to one destination and generally uses Class A, B, or C IPv4 address space rather than Class D.
https://www.comptia.org/content/guides/what-is-an-ip-address

Question 4

Single choice · Domain: D1 Networking concepts › Compare private and public cloud deployment models

Which of the following is a key advantage of a private cloud?

A. On-demand scalability
B. Greater control
C. Publicly accessible
D. No up-front costs

Answer: B. Greater control

Explanation

This question tests understanding of cloud deployment models and the primary benefits of a private cloud, especially the organization's greater control over infrastructure, access, and data.

✗ **A** On-demand scalability
Incorrect. On-demand scalability is a general cloud-computing characteristic and is not the key distinguishing advantage of a private cloud.
https://www.comptia.org/content/articles/what-is-cloud-computing

✓ **B** Greater control
Correct. A private cloud is dedicated to one organization, providing greater control over infrastructure, security, access, and configuration than a public cloud.
https://www.comptia.org/content/articles/what-is-cloud-computing

✗ **C** Publicly accessible
Incorrect. Public accessibility is associated with public cloud services, not a key advantage of a private cloud.
https://www.comptia.org/content/articles/what-is-cloud-computing

✗ **D** No up-front costs
Incorrect. Private clouds commonly require significant up-front investment in dedicated hardware, software, and administration.
https://www.comptia.org/content/articles/what-is-cloud-computing

Free demo · full exam: 594 questions

Question 5

Single choice · Domain: D1 Networking concepts › Identify common mail-service ports and distinguish legacy SMTP from encrypted mail submission

An ongoing mail server migration is in progress. The current system does not use encrypted mail protocols, but the new system does. Which of the following port can the administrator close to deny non-encrypted mail protocols without interrupting the migration?

A. 22
B. 23
C. 25
D. 443
E. 587

Answer: C. 25

Explanation

This question tests recognition of standard TCP ports and selection of the port associated with traditional SMTP traffic. Port 25 is commonly used for legacy server-to-server SMTP, while port 587 is used for mail submission and can support encryption during migration.

✗ **A** 22
Incorrect. TCP port 22 is used by SSH for secure remote administration, not standard mail transfer.
https://www.comptia.org/certifications/network

✗ **B** 23
Incorrect. TCP port 23 is used by Telnet, which provides unencrypted remote terminal access; it is not a mail protocol port.
https://www.comptia.org/certifications/network

✓ **C** 25
Correct. TCP port 25 is the traditional SMTP port and is commonly associated with non-encrypted server-to-server mail transfer. Closing it blocks legacy SMTP while allowing the encrypted mail system to continue using its submission service.
https://www.comptia.org/certifications/network

✗ **D** 443
Incorrect. TCP port 443 is used by HTTPS for secure web traffic, not standard SMTP mail transfer.
https://www.comptia.org/certifications/network

✗ **E** 587
Incorrect. TCP port 587 is the standard mail submission port and is commonly used with authentication and STARTTLS, so closing it could interrupt the new mail system during migration.
https://www.comptia.org/certifications/network

Question 6

Single choice · Domain: D1 Networking concepts › Identify dual-stack technology for IPv4 and IPv6 interoperability

A CDN provider needs to implement a solution that delivers services to customers using IPv4, IPv6, or both to ensure interoperability. Which of the following technologies is the most appropriate for this requirement?

A. Quality of service
B. Automatic Private IP Addressing
C. Dual stack
D. Stateless Address Autoconfiguration

Answer: C. Dual stack

Explanation

This question tests recognition of the IPv4/IPv6 coexistence method that allows devices and services to use IPv4, IPv6, or both. Dual stack supports simultaneous operation of both protocols.

✗ **A** Quality of service
Incorrect. Quality of service prioritizes or manages network traffic to meet performance requirements; it does not provide IPv4 and IPv6 interoperability.

https://www.comptia.org/content/guides/what-is-ipv6

✗ **B** Automatic Private IP Addressing
Incorrect. Automatic Private IP Addressing assigns a self-configured IPv4 address when DHCP is unavailable. It does not support operation across both IPv4 and IPv6.

https://www.comptia.org/content/guides/what-is-ipv6

✓ **C** Dual stack
Correct. Dual stack enables systems and services to run IPv4 and IPv6 simultaneously, allowing customers to connect using either protocol or both.

https://www.comptia.org/content/guides/what-is-ipv6

✗ **D** Stateless Address Autoconfiguration
Incorrect. Stateless Address Autoconfiguration is an IPv6 mechanism for automatically generating addresses and learning network information; it does not itself provide simultaneous IPv4 and IPv6 support.

https://www.comptia.org/content/guides/what-is-ipv6

Free demo · full exam: 594 questions

Question 7

Single choice · Domain: D1 Networking concepts › Identify connector types used with coaxial cable

Which of the following types of connectors allows the transmission of network data through a coaxial cable?

A. SC
B. MPO
C. BNC
D. RJ11

Answer: C. BNC

Explanation

This question tests recognition of physical network connectors and their associated cable media. BNC connectors are used to terminate coaxial cable, while SC and MPO are fiber-optic connectors and RJ11 is used for telephone cabling.

✗ **A** SC
Incorrect. SC is a push-pull fiber-optic connector, not a coaxial-cable connector.
https://www.comptia.org/certifications/network

✗ **B** MPO
Incorrect. MPO is a multi-fiber push-on connector used with fiber-optic cabling, not coaxial cable.
https://www.comptia.org/certifications/network

✓ **C** BNC
Correct. BNC, or Bayonet Neill–Concelman, is a bayonet-style connector commonly used with coaxial cable for network and other signal applications.
https://www.comptia.org/certifications/network

✗ **D** RJ11
Incorrect. RJ11 is a modular connector typically used for telephone and low-bandwidth voice wiring, not coaxial cable.
https://www.comptia.org/certifications/network

Dumpsgate

Question 8

Multiple choice · Domain: D1 Networking concepts › Identify the SMB protocol and TCP port used for Windows network-share file transfers

Which of the following are commonly used in Windows-based environments to facilitate file transfers between clients and network shares? Select two.

A. Port 21
B. Port 443
C. Port 445
D. HTTPS
E. SMB

Answer

- C. **Port 445**
- E. **SMB**

Explanation

This question tests recognition of common networking protocols and port numbers, specifically SMB and its standard TCP port used to access Windows file shares.

✗ **A** Port 21
Incorrect. TCP port 21 is used by FTP for control traffic. It is not the standard port for Windows SMB network shares.

https://www.comptia.org/certifications/network

✗ **B** Port 443
Incorrect. TCP port 443 is used for HTTPS and encrypted web traffic, not the standard SMB port for Windows file shares.

https://www.comptia.org/certifications/network

✓ **C** Port 445
Correct. TCP port 445 is commonly used by SMB directly over TCP to provide access to Windows network shares.

https://www.comptia.org/certifications/network

✗ **D** HTTPS
Incorrect. HTTPS provides secure web communication and normally uses TCP port 443; it is not the Windows network-share protocol tested here.

https://www.comptia.org/certifications/network

✓ **E** SMB
Correct. Server Message Block (SMB) is the Windows file and printer-sharing protocol used to access network shares, commonly over TCP port 445.

https://www.comptia.org/certifications/network

Dumpsgate

Question 9

Single choice · Domain: D1 Networking concepts › Classify an IPv4 address using classful address ranges

A network engineer configures a NIC that has an IP address of 192.168.123.232. Which of the following classes is this address an example of?

A. Class A
B. Class B
C. Class C
D. Class D

Answer: C. Class C

Explanation

This question tests recognition of IPv4 address classes based on the first octet. The first octet, 192, falls within the Class C range of 192–223.

✗ **A** Class A
Incorrect. Class A addresses use a first octet from 1 through 126. The address begins with 192.
https://www.comptia.org/certifications/network

✗ **B** Class B
Incorrect. Class B addresses use a first octet from 128 through 191. The address begins with 192.
https://www.comptia.org/certifications/network

✓ **C** Class C
Correct. Class C addresses use a first octet from 192 through 223, so 192.168.123.232 is a Class C address.
https://www.comptia.org/certifications/network

✗ **D** Class D
Incorrect. Class D addresses use a first octet from 224 through 239 and are reserved for multicast. The address begins with 192.
https://www.comptia.org/certifications/network

Question 10

Single choice · Domain: D1 Networking concepts › Identify the OSI model layer associated with HTTP

Which of the following OSI model layers manages the exchange of HTTP information?

A. Session
B. Data link
C. Network
D. Application

Answer: D. Application

Free demo · full exam: 594 questions

Dumpsgate

Question 11

Multiple choice · Domain: D1 Networking concepts › Calculate subnet sizes and select CIDR ranges that provide sufficient host capacity

Company C is acquiring Company A and Company B. Company C needs to merge all three networks into one Class B network. Additionally, the network capacity of each company needs to grow by 20%. Company C also requires segmentation of Company A and Company B to account for unknown security vulnerabilities within each.

Instructions:

Select the correct subnet range to meet Company C's requirements.

Free demo · full exam: 594 questions

A. 168.10.0/22
B. 0.8.0/26
C. 168.10.0/27
D. 0.1.0/21
E. 168.10.0/26
F. 0.0.1/17
G. 0.0.1/18
H. 168.1.0/23
I. 168.1.0/22
J. 0.1.0/22
K. 0.8.0/27

Free demo · full exam: 594 questions

Answer

- E. **168.10.0/26**
- G. **0.0.1/18**
- H. **168.1.0/23**

Explanation

This question tests subnetting calculations, including determining the smallest subnet that supports each company's current devices plus 20% growth. It also tests selecting distinct private address ranges for network segmentation.

✗ **A** 168.10.0/22
Incorrect as the best selection for the listed requirements. A /22 provides far more addresses than Company A or B needs, while it does not provide the approximately 12,000 usable addresses required for Company C.

https://www.comptia.org/content/guides/what-is-subnetting

✗ **B** 0.8.0/26
Incorrect for the complete selection. A /26 can support Company A's 32 devices plus 20% growth, but this address range is not the intended range for Company A in the consolidated addressing plan.

https://www.comptia.org/content/guides/what-is-subnetting

✗ **C** 168.10.0/27
Incorrect. A /27 has only 30 usable host addresses, which cannot support Company A's required capacity of at least 39 hosts after 20% growth.

https://www.comptia.org/content/guides/what-is-subnetting

✗ **D** 0.1.0/21
Incorrect as the best-fit selection. A /21 provides substantially more capacity than Company A or B requires and is not the intended range for the corresponding company in the answer set.

https://www.comptia.org/content/guides/what-is-subnetting

✓ **E** 168.10.0/26
Correct for Company A. Thirty-two devices with 20% growth require at least 39 usable host addresses; a /26 provides 62 usable host addresses and preserves segmentation.

https://www.comptia.org/content/guides/what-is-subnetting

✗ **F** 0.0.1/17
Incorrect as the best-fit selection. A /17 is much larger than required for Company A or Company B and is not the intended range for Company C, for which a /18 is sufficient.

https://www.comptia.org/content/guides/what-is-subnetting

✓ **G** 0.0.1/18
Correct for Company C. Ten thousand devices plus 20% growth require approximately 12,000 usable addresses; a /18 provides 16,382 usable host addresses. The address 10.0.0.1/18 belongs to the 10.0.0.0/18 subnet.

https://www.comptia.org/content/guides/what-is-subnetting

✓ **H** 168.1.0/23
Correct for Company B in the provided answer set. A /23 supplies 510 usable host addresses, exceeding the 120 hosts required after 20% growth, while maintaining a separate subnet for segmentation.

https://www.comptia.org/content/guides/what-is-subnetting

✗ **I** 168.1.0/22
Incorrect as the intended best-fit selection. Although a /22 can accommodate Company B, it is substantially larger than needed for 120 hosts and does not represent the selected subnet in the provided answer set.

https://www.comptia.org/content/guides/what-is-subnetting

Free demo · full exam: 594 questions

✗ **J** 0.1.0/22
Incorrect. A /22 provides only 1,022 usable host addresses, which is insufficient for Company C's required capacity of approximately 12,000 hosts.
https://www.comptia.org/content/guides/what-is-subnetting

✗ **K** 0.8.0/27
Incorrect. A /27 provides only 30 usable host addresses, so it cannot support Company A after 20% growth and is far too small for Company B or Company C.
https://www.comptia.org/content/guides/what-is-subnetting

Question 12

Single choice · Domain: D1 Networking concepts › Identify IPv6 transition mechanisms, specifically NAT64 for IPv6-to-IPv4 connectivity

A company implements a new network utilizing only IPv6 addressing and needs to connect to the internet. Which of the following must be enabled in order for the internal network to contact servers on the internet?

A. MPLS
B. NAT64
C. GRE
D. Static routing

Answer: B. NAT64

Explanation

This question tests the ability to select the IPv6 transition technology that allows IPv6-only internal hosts to communicate with IPv4 internet servers. NAT64 performs translation between IPv6 and IPv4 addressing.

✗ **A** MPLS
Incorrect. MPLS is a provider-based traffic-forwarding technology and does not translate IPv6 traffic into IPv4 traffic for internet connectivity.
https://www.comptia.org/certifications/network

✓ **B** NAT64
Correct. NAT64 translates communication between IPv6-only clients and IPv4 servers, enabling an IPv6-only internal network to reach IPv4 internet resources.
https://www.comptia.org/certifications/network

✗ **C** GRE
Incorrect. GRE encapsulates traffic inside a tunnel but does not inherently translate IPv6 addresses into IPv4 addresses for communication with IPv4 internet servers.
https://www.comptia.org/certifications/network

✗ **D** Static routing
Incorrect. Static routing can provide paths between networks, but it cannot translate IPv6 packets into IPv4 packets. An IPv6-only network requires a translation mechanism such as NAT64 to reach IPv4 servers.
https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 13

Single choice · Domain: D1 Networking concepts › Identify common network protocols and their associated port numbers

Which of the following ports is used to transfer data between mail exchange servers?

A. 21
B. 25
C. 53
D. 69

Answer: B. 25

Explanation

This question tests recognition of SMTP and its standard port for transferring email between mail exchange servers.

✗ **A** 21
Incorrect. Port 21 is used by FTP for control connections, not for transferring email between mail exchange servers.
https://www.comptia.org/certifications/network

✓ **B** 25
Correct. SMTP uses TCP port 25 to transfer email between mail exchange servers.
https://www.comptia.org/certifications/network

✗ **C** 53
Incorrect. Port 53 is used by DNS for name resolution and DNS queries, not for mail transfer.
https://www.comptia.org/certifications/network

✗ **D** 69
Incorrect. Port 69 is used by TFTP, a simple file-transfer protocol, not for transferring email between mail exchange servers.
https://www.comptia.org/certifications/network

Question 14

Single choice · Domain: D1 Networking concepts › Identify wireless network types and topologies

A technician needs to quickly set up a network with five wireless devices. Which of the following network types should the technician configure to accomplish this task?

A. Ad hoc
B. Spine and leaf
C. Point to point
D. Mesh

Answer: A. Ad hoc

Explanation

This question tests the ability to distinguish an ad hoc wireless network, which allows devices to communicate directly without a central access point, from other network topologies.

✓ **A** Ad hoc
Correct. An ad hoc network enables wireless devices to connect directly to one another without requiring a wireless access point, making it suitable for quickly connecting five devices.

https://www.comptia.org/certifications/network

✗ **B** Spine and leaf
Incorrect. Spine-and-leaf is a structured network topology commonly used in data centers, not a quick peer-to-peer wireless network for a small group of devices.

https://www.comptia.org/certifications/network

✗ **C** Point to point
Incorrect. A point-to-point network directly connects two endpoints, so it is not appropriate for connecting five wireless devices as a group.

https://www.comptia.org/certifications/network

✗ **D** Mesh
Incorrect. A mesh network uses multiple interconnected nodes and is designed for resilient coverage and redundancy; it is not the simplest method for quickly connecting five devices directly.

https://www.comptia.org/certifications/network

Question 15

Single choice · Domain: D1 Networking concepts › Identify the purpose of common network protocols, including SNMP

Which of the following protocols is used to send networking status messages between clients and servers?

A. SSH
B. DHCP
C. NTP
D. SNMP

Answer: D. SNMP

Explanation

This question tests recognition of the functions of common networking protocols. SNMP is used for monitoring and exchanging network-management and status information between managed devices and network management systems.

✗ **A** SSH
Incorrect. SSH provides secure remote command-line access and encrypted administration; it is not the

protocol used for exchanging network status information.

https://www.comptia.org/content/guides/what-is-snmp

✗ **B** DHCP
Incorrect. DHCP automatically provides clients with IP configuration information such as addresses, gateways, and DNS servers; it does not provide general network-status monitoring.

https://www.comptia.org/content/guides/what-is-snmp

✗ **C** NTP
Incorrect. NTP synchronizes the clocks of networked systems. It does not exchange network-management status information.

https://www.comptia.org/content/guides/what-is-snmp

✓ **D** SNMP
Correct. SNMP is the Simple Network Management Protocol, used to monitor and exchange status and management information between network-management systems and managed devices.

https://www.comptia.org/content/guides/what-is-snmp

Question 16

Single choice · Domain: D1 Networking concepts › Calculate IPv4 subnet capacity and select an appropriately sized CIDR network

A network administrator prepares a VLAN for a new office while planning for minimal IP address waste. The new office will have approximately 800 workstations. Which of the following network schemes meets the requirements?

A. 10.0.100.0/22
B. 172.16.8.0/23
C. 172.16.15.0/20
D. 192.168.4.0/21

Answer: A. 10.0.100.0/22

Explanation

This question tests IPv4 subnetting, including usable host capacity, CIDR prefix lengths, and selecting the smallest valid subnet that can support approximately 800 workstations with minimal address waste.

✓ **A** 10.0.100.0/22
Correct. A /22 subnet provides 1,024 total addresses and 1,022 usable host addresses, which supports approximately 800 workstations with less waste than the larger alternatives. The address is also a valid /22 network boundary.

https://www.comptia.org/certifications/network

✗ **B** 172.16.8.0/23
Incorrect. A /23 subnet provides only 512 total addresses and 510 usable host addresses, which is insufficient for approximately 800 workstations.

https://www.comptia.org/certifications/network

✗ **C** 172.16.15.0/20
Incorrect. A /20 subnet provides 4,096 total addresses and 4,094 usable host addresses, creating substantially more address waste than necessary. Additionally, 172.16.15.0 is not a valid /20 network

boundary; the corresponding /20 network would begin at 172.16.0.0.

https://www.comptia.org/certifications/network

✗ **D** 192.168.4.0/21
Incorrect. A /21 subnet provides 2,048 total addresses and 2,046 usable host addresses, which is larger than needed and wastes more addresses than a /22. Also, 192.168.4.0 is not a valid /21 network boundary because /21 networks increment by eight in the third octet.

https://www.comptia.org/certifications/network

Question 17

Single choice · Domain: D2 Network implementation › Configure MTU sizes, including jumbo frames, to reduce packet fragmentation

A network administrator needs to reduce network fragmentation between the SAN and the server to decrease backup times. Which of the following MTU sizes should the administrator configure to accomplish this task?

A. 1500
B. 2000
C. 7935
D. 9000

Answer: D. 9000

Explanation

This question tests selecting an appropriate Ethernet MTU for high-throughput SAN traffic. A 9000-byte MTU is a common jumbo-frame setting that reduces the number of frames and fragmentation during transfers when supported end to end.

✗ **A** 1500
Incorrect. A 1500-byte MTU is the standard Ethernet MTU and does not provide the jumbo-frame advantage needed to reduce fragmentation for SAN traffic.

https://www.comptia.org/certifications/network

✗ **B** 2000
Incorrect. Although larger than the standard Ethernet MTU, 2000 bytes is not the commonly used jumbo-frame size for SAN and Ethernet networks and provides less benefit than a 9000-byte MTU.

https://www.comptia.org/certifications/network

✗ **C** 7935
Incorrect. This is not the conventional jumbo-frame MTU value used for SAN traffic. A 9000-byte MTU is the standard practical choice when jumbo frames are supported across the entire path.

https://www.comptia.org/certifications/network

✓ **D** 9000
Correct. A 9000-byte MTU enables jumbo frames, allowing more data per frame and reducing frame overhead and fragmentation during SAN-to-server transfers, which can improve backup times. The setting must be supported consistently by the SAN, servers, switches, and other devices along the path.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 18

Single choice · Domain: D2 Network implementation › Configure DHCP relay using an IP helper address

Users in a new subnet segment are unable to get IP addresses from the DHCP server. A network administrator notices that the DHCP server is located on a remote segment. Which of the following should the administrator do to resolve the issue?

A. Configure the IP helper on the network device
B. Configure the switch to accept EAPoL on the new VLAN segment
C. Configure the existing DHCP lease time
D. Configure the DHCP server to operate on non-standard ports

Answer: A. Configure the IP helper on the network device

Explanation

This question tests the ability to enable DHCP clients on a remote subnet to reach a DHCP server across a routed network. An IP helper or DHCP relay forwards DHCP requests because DHCP discovery messages are broadcasts and normally do not cross routers.

✓ **A** Configure the IP helper on the network device
Correct. An IP helper configured on the Layer 3 network device relays DHCP broadcasts from the new subnet to the remote DHCP server.

https://www.comptia.org/certifications/network

✗ **B** Configure the switch to accept EAPoL on the new VLAN segment
Incorrect. EAPoL is used for 802.1X port-based authentication, not for forwarding DHCP requests between routed subnets.

https://www.comptia.org/certifications/network

✗ **C** Configure the existing DHCP lease time
Incorrect. DHCP lease duration controls how long clients retain assigned addresses; it does not enable DHCP requests to cross a router or reach a remote DHCP server.

https://www.comptia.org/certifications/network

✗ **D** Configure the DHCP server to operate on non-standard ports
Incorrect. Changing DHCP to non-standard ports would not solve the routing of DHCP broadcasts and could prevent normal DHCP communication. A DHCP relay or IP helper is required instead.

https://www.comptia.org/certifications/network

Dumpsgate

Question 19

Single choice · Domain: D2 Network implementation › Compare administrative distances of static routes and dynamic routing protocols

Which of the following has the highest administrative distance?

A. Enhanced Interior Gateway Routing Protocol
B. Border Gateway Protocol
C. Static route
D. Open Shortest Path First

Answer: D. Open Shortest Path First

Explanation

This question tests the ability to identify which routing source is preferred or least preferred by comparing default administrative distance values. Among the listed standard values, OSPF has an administrative distance of 110, higher than EIGRP at 90, eBGP at 20, and static routes at 1.

✗ **A** Enhanced Interior Gateway Routing Protocol
Incorrect. EIGRP has a default administrative distance of 90 for internal routes, which is lower than OSPF's 110.

https://www.comptia.org/certifications/network

✗ **B** Border Gateway Protocol
Incorrect in the standard comparison used here. External BGP has a default administrative distance of 20, which is lower than OSPF's 110.

https://www.comptia.org/certifications/network

✗ **C** Static route
Incorrect. A static route has a default administrative distance of 1, making it more preferred than the listed dynamic routing protocols.

https://www.comptia.org/certifications/network

✓ **D** Open Shortest Path First
Correct. OSPF has a default administrative distance of 110, which is higher than internal EIGRP at 90, external BGP at 20, and static routes at 1.

https://www.comptia.org/certifications/network

Dumpsgate

Question 20

Single choice · Domain: D2 Network implementation › Identify power and connectivity issues affecting wireless access point deployment

Some newly installed wireless access points are not broadcasting. Which of the following is the most likely cause of the issue?

A. PoE power budget exceeded
B. Improper VLAN assignment
C. Limited signal strength/degradation
D. Uplink transceiver incorrectly configured

Answer: A. PoE power budget exceeded

Explanation

This question tests the ability to determine why newly installed access points are not operating or broadcasting, with emphasis on Power over Ethernet capacity and network implementation factors.

✓ **A** PoE power budget exceeded
Correct. If the PoE switch or injector's available power budget is exceeded, newly installed access points may not receive sufficient power and therefore cannot broadcast.

https://www.comptia.org/content/guides/what-is-power-over-ethernet

✗ **B** Improper VLAN assignment
Incorrect. An improper VLAN assignment can prevent clients from reaching network resources or can disrupt management connectivity, but the access point would typically still power on and broadcast its wireless network.

https://www.comptia.org/content/guides/what-is-power-over-ethernet

✗ **C** Limited signal strength/degradation
Incorrect. Weak signal strength or interference affects wireless coverage and client connectivity; it does not normally prevent a powered access point from broadcasting.

https://www.comptia.org/content/guides/what-is-power-over-ethernet

✗ **D** Uplink transceiver incorrectly configured
Incorrect. An uplink transceiver configuration problem can affect upstream connectivity, but it is less likely than an exceeded PoE budget to cause newly installed access points not to broadcast at all.

https://www.comptia.org/content/guides/what-is-power-over-ethernet

Free demo · full exam: 594 questions

Question 21

Single choice · Domain: D2 Network implementation › Configure quality of service (QoS) for VoIP traffic

Following a VoIP deployment, users report issues using the VoIP system. After further review, a network technician reports the following:

• Dropped calls are occurring.
• Local file transfer is successful.
• New firewalls have recently been added.
• Web traffic is functional.
• Users experience audio latency.

Which of the following is the most likely cause of the issues?

A. Conflicting firewall rule
B. Spanning tree issue
C. Incorrect voice VLAN
D. Misconfigured QoS

Answer: D. Misconfigured QoS

Explanation

This question tests the ability to identify how QoS configuration affects real-time voice traffic. VoIP is sensitive to latency, jitter, and packet loss, while successful file transfers and web access indicate that general network connectivity is functioning.

✗ **A** Conflicting firewall rule
Incorrect. A firewall rule could block signaling or media traffic, but the combination of dropped calls and audio latency with otherwise functional network services most strongly indicates inadequate QoS rather than a complete firewall conflict.

https://www.comptia.org/certifications/network

✗ **B** Spanning tree issue
Incorrect. A spanning tree problem would more commonly cause switching loops, broadcast storms, instability, or widespread connectivity disruption, not isolated VoIP latency while local file transfers and web traffic remain functional.

https://www.comptia.org/certifications/network

✗ **C** Incorrect voice VLAN
Incorrect. An incorrect voice VLAN would typically prevent phones from obtaining network access or reaching required voice services. The reported latency and dropped calls are more characteristic of voice traffic competing for bandwidth without suitable prioritization.

https://www.comptia.org/certifications/network

✓ **D** Misconfigured QoS
Correct. VoIP requires traffic prioritization because voice is sensitive to latency, jitter, and packet loss. Misconfigured or absent QoS can allow file transfers and web traffic to compete with voice traffic, resulting in delayed audio and dropped calls.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 22

Single choice · Domain: D2 Network implementation › Configure link aggregation using Link Aggregation Control Protocol to provide redundant, higher-throughput switch connections

A network administrator needs to implement trunk port redundancy. The change should not introduce any loops and should increase throughput. Which of the following technologies should the administrator use?

A. Media Independent Interface with Crossover
B. First Hop Redundancy Protocol
C. Link Aggregation Control Protocol
D. Spanning Tree Protocol

Answer: C. Link Aggregation Control Protocol

Explanation

This question tests the ability to select a switch-link redundancy technology that combines multiple physical links into one logical link. LACP provides increased bandwidth and link resilience while avoiding the loops that unmanaged redundant links could create.

✗ **A** Media Independent Interface with Crossover
Incorrect. MDI crossover describes the wiring or interface relationship between network devices; it does not aggregate links, provide link redundancy, or increase throughput.

https://www.comptia.org/certifications/network

✗ **B** First Hop Redundancy Protocol
Incorrect. FHRP provides redundant default-gateway services at Layer 3, but it does not bundle switch ports or increase the throughput of a trunk connection.

https://www.comptia.org/certifications/network

✓ **C** Link Aggregation Control Protocol
Correct. LACP dynamically negotiates a link aggregation group, combining multiple physical links into one logical trunk. This provides additional throughput and redundancy while presenting a single logical path to spanning-tree protocols, helping prevent switching loops.

https://www.comptia.org/certifications/network

✗ **D** Spanning Tree Protocol
Incorrect. STP prevents Layer 2 loops by blocking redundant paths, but blocked links do not increase active throughput. STP is commonly used with redundant links, whereas LACP is the technology used to aggregate them.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 23

Single choice · Domain: D2 Network implementation › Select and deploy mesh wireless networks to extend Wi-Fi coverage without wired Ethernet connections

New access points need to be added to the network to increase Wi-Fi coverage. However, no Ethernet connections are available. Which of the following will accomplish this task?

A. Enabling PoE
B. Band steering
C. Mesh deployment
D. Directional antennas

Answer: C. Mesh deployment

Explanation

This question tests wireless network implementation, specifically choosing a mesh deployment when additional access points cannot be connected through Ethernet. Mesh access points use wireless backhaul to extend coverage.

✗ **A** Enabling PoE
Incorrect. Power over Ethernet supplies electrical power over an Ethernet cable, but it does not provide wireless backhaul or solve the absence of Ethernet connections.

https://www.comptia.org/certifications/network

✗ **B** Band steering
Incorrect. Band steering encourages compatible wireless clients to use a particular frequency band; it does not connect new access points without Ethernet or extend coverage by itself.

https://www.comptia.org/certifications/network

✓ **C** Mesh deployment
Correct. A mesh deployment allows access points to communicate through wireless backhaul links, extending Wi-Fi coverage when Ethernet connections are unavailable.

https://www.comptia.org/certifications/network

✗ **D** Directional antennas
Incorrect. Directional antennas focus radio energy in a particular direction and can improve range or point-to-point connectivity, but they do not inherently provide the wireless backhaul and coordinated access-point expansion of a mesh deployment.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 24

Single choice · Domain: D2 Network implementation › Select an interior gateway routing protocol based on configuration overhead and convergence requirements

A school purchases new equipment and needs to configure a routing protocol that minimizes configuration overhead and ensures fast convergence. Which of the following routing protocols is the most suitable choice?

A. IS-IS
B. OSPF
C. RIPv2
D. BGP

Answer: B. OSPF

Explanation

This question tests the ability to choose an appropriate dynamic routing protocol for an internal network by comparing protocol convergence speed, scalability, and administrative overhead.

✗ **A** IS-IS
Incorrect. IS-IS is a link-state interior gateway protocol with fast convergence, but OSPF is generally the more suitable and commonly deployed choice for a school network because it provides fast convergence without the additional operational complexity often associated with IS-IS.

https://www.comptia.org/content/guides/what-is-routing

✓ **B** OSPF
Correct. OSPF is a link-state interior gateway protocol that supports hierarchical design and fast convergence, making it suitable for an internal school network that needs efficient routing with limited configuration overhead.

https://www.comptia.org/content/guides/what-is-routing

✗ **C** RIPv2
Incorrect. RIPv2 is a distance-vector protocol with a 15-hop limit and relatively slow convergence, so it is not the best choice when rapid recovery from topology changes is required.

https://www.comptia.org/content/guides/what-is-routing

✗ **D** BGP
Incorrect. BGP is primarily an exterior gateway protocol used to exchange routes between autonomous systems. It has greater configuration and policy-management overhead than is appropriate for this internal school-network requirement.

https://www.comptia.org/content/guides/what-is-routing

Dumpsgate

Free demo · full exam: 594 questions

Question 25

Single choice · Domain: D2 Network implementation › Identify and troubleshoot VLAN assignments on switch ports supporting IP phones and user devices

A network technician wants to reduce switch port use. The technician connects users' laptops through VoIP phones. However, this change causes users to have issues printing and accessing different network resources. Which of the following is the most likely cause of this issue?

A. Incorrect subnet mask
B. VLAN assignment
C. Address pool exhaustion
D. Duplicate IP addresses

Answer: B. VLAN assignment

Explanation

This question tests the ability to recognize how incorrect voice and data VLAN assignments affect devices connected through an IP phone. A laptop placed in the wrong VLAN may be unable to reach printers and other network resources.

✗ **A** Incorrect subnet mask
An incorrect subnet mask can cause local-versus-remote communication problems, but the change involving laptops connected through VoIP phones most directly points to a switch-port VLAN configuration issue.
https://www.comptia.org/content/articles/what-is-a-vlan

✓ **B** VLAN assignment
Correct. A switch port connected to an IP phone commonly carries separate voice and data VLANs. If the laptop is assigned to the wrong VLAN or the port is not configured correctly, users may be unable to access printers and other network resources.
https://www.comptia.org/content/articles/what-is-a-vlan

✗ **C** Address pool exhaustion
DHCP address pool exhaustion would generally prevent new devices from receiving IP addresses, rather than specifically causing resource-access problems after laptops are connected through VoIP phones.
https://www.comptia.org/content/articles/what-is-a-vlan

✗ **D** Duplicate IP addresses
Duplicate IP addresses can cause intermittent connectivity and address conflicts, but the topology change described is most strongly associated with incorrect voice or data VLAN assignment on the switch port.
https://www.comptia.org/content/articles/what-is-a-vlan

Dumpsgate

Question 26

Multiple choice · Domain: D2 Network implementation › Identify physical and environmental factors that affect wireless coverage and signal strength

A company is implementing a new wireless network in its office building and wants to ensure maximum coverage and signal strength. Which of the following factors should a technician consider to meet these requirements? Select two.

A. Building materials
B. Electrical interference
C. Distance from the server room
D. Type of encryption being used
E. Power over Ethernet
F. Type of client devices

Answer

- A. **Building materials**
- B. **Electrical interference**

Explanation

This question tests selection of site-survey considerations for deploying a wireless network. Building materials can attenuate radio signals, while electrical or radio-frequency interference can reduce signal quality and coverage.

✓ **A** Building materials
Correct. Materials such as concrete, metal, and glass can absorb or reflect wireless signals, reducing coverage and signal strength.

https://www.comptia.org/en-us/certifications/network/

✓ **B** Electrical interference
Correct. Electrical and radio-frequency interference from devices such as microwaves, cordless phones, and other transmitters can degrade wireless performance and reduce effective coverage.

https://www.comptia.org/en-us/certifications/network/

✗ **C** Distance from the server room
Incorrect. An access point's distance from the server room does not directly determine wireless coverage or signal strength; access-point placement and the radio environment are the relevant considerations.

https://www.comptia.org/en-us/certifications/network/

✗ **D** Type of encryption being used
Incorrect. Encryption affects wireless security and processing requirements, not the physical propagation or signal strength of the wireless signal.

https://www.comptia.org/en-us/certifications/network/

✗ **E** Power over Ethernet
Incorrect. Power over Ethernet supplies power and network connectivity to an access point, but the PoE method itself is not a primary factor determining radio coverage or signal strength.

https://www.comptia.org/en-us/certifications/network/

✗ **F** Type of client devices
Incorrect. Client capabilities can affect supported wireless standards and individual client performance, but they are not the primary environmental factors used to ensure maximum access-point coverage and signal strength.

Free demo · full exam: 594 questions

https://www.comptia.org/en-us/certifications/network/

Question 27

Single choice · Domain: D2 Network implementation › Identify and mitigate wireless channel overlap and interference

A user reports issues connecting to the wireless network. A network technician notices the following:

• Several wireless networks are available externally from other businesses

• APs configured in the building are set to use the maximum amount of power

• Signal strength:

First floor lobby: -55 dBm

Break room: -78 dBm

Conference room: -67 dBm

Office area: -61 dBm

Walking path around the building: -80 dBm• Channels in use: 1, 5, 44, 32 Which of the following is causing the user's wireless issues?

A. AP power settings
B. Channel overlap
C. Rogue devices
D. Interference outside the lobby

Answer: B. Channel overlap

Explanation

This question tests the ability to evaluate wireless channel assignments and recognize adjacent-channel interference. Channels 1 and 5 overlap in the 2.4GHz band, which can cause connectivity and performance problems, especially when access points transmit at maximum power. Reference: https://www.comptia.org/en-us/certifications/network/

✗ **A** AP power settings
Incorrect. Excessive transmit power can increase the coverage area and contribute to interference, but the specific configuration showing a direct problem is the overlapping channel assignment.

https://www.comptia.org/en-us/certifications/network/

✓ **B** Channel overlap
Correct. Channels 1 and 5 overlap in the 2.4GHz band, creating adjacent-channel interference. The overlapping channels can cause wireless connectivity and performance issues.

https://www.comptia.org/en-us/certifications/network/

✗ **C** Rogue devices
Incorrect. Wireless networks belonging to other businesses being visible externally does not by itself indicate that unauthorized rogue devices are operating on this network.

https://www.comptia.org/en-us/certifications/network/

✗ **D** Interference outside the lobby
Incorrect. External networks may contribute to RF interference, but the documented channel assignment provides a more specific cause: channels 1 and 5 overlap in the 2.4GHz band.

https://www.comptia.org/en-us/certifications/network/

Question 28

Single choice · Domain: D2 Network implementation › Configure an IEEE 802.1Q trunk between switches to carry VLAN traffic

Computer A cannot reach Computer B in the following network:

Computer A: 172.16.2.10/16

Computer B: 172.16.4.10/16

Switch A:

Gi0/1 access VLAN 1, status up/up

Gi0/9 access VLAN 8, status up/up

Gi0/10 access VLAN 5, status administratively down

Switch B:

Gi0/1 access VLAN 1, status up/up

Gi0/9 access VLAN 8, status up/up

Gi0/10 access VLAN 5, status administratively down

Which of the following will resolve the issue?

A. Set up link aggregation between Switch A and Switch B on Gi0/9 and Gi0/10
B. Configure spanning tree on Switch A and Switch B
C. Establish a trunk connection between Switch A and Switch B
D. Put Computer A and Computer B in the same /24 subnet

Answer: C. Establish a trunk connection between Switch A and Switch B

Explanation

The computers use addresses in the same /16 subnet, but communication still requires a Layer 2 path between their VLANs. A trunk between the switches allows the required VLAN traffic to traverse the inter-switch link.

✗ **A** Set up link aggregation between Switch A and Switch B on Gi0/9 and Gi0/10
Incorrect. Link aggregation combines multiple physical links for redundancy and bandwidth, but these interfaces are configured as access ports, and Gi0/10 is administratively down. Link aggregation alone does not provide the required VLAN trunking.

https://www.comptia.org/certifications/network

✗ **B** Configure spanning tree on Switch A and Switch B
Incorrect. Spanning Tree Protocol prevents Layer 2 loops by managing redundant paths; it does not create an inter-switch connection or carry VLAN traffic between switches.

https://www.comptia.org/certifications/network

✓ **C** Establish a trunk connection between Switch A and Switch B
Correct. A trunk carries VLAN-tagged traffic between switches, providing the Layer 2 path needed for the computers to communicate while preserving their VLAN information.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

✗ **D** Put Computer A and Computer B in the same /24 subnet
Incorrect. The addresses 172.16.2.10/16 and 172.16.4.10/16 are already in the same /16 subnet. Changing them to a /24 would place them in different subnets, increasing the need for routing rather than resolving the Layer 2 connectivity issue.
https://www.comptia.org/certifications/network

Question 29

Single choice · Domain: D2 Network implementation › Select dynamic routing protocols for redundant and internet-connected networks

A network administrator is setting up two new firewalls for redundancy and needs to implement a redundant internet connection. Which of the following routing technologies will the administrator most likely use?

A. EIGRP
B. RIPv2
C. OSPF
D. BGP

Answer: D. BGP

Explanation

This question tests the ability to identify the appropriate routing protocol for a redundant internet connection. BGP is designed for exchanging routing information between autonomous systems and is commonly used for multihoming and redundant connections to internet service providers.

✗ **A** EIGRP
Incorrect. EIGRP is primarily an interior gateway protocol used within an organization and is not the standard choice for exchanging routes between an enterprise and multiple internet service providers.
https://www.comptia.org/certifications/network

✗ **B** RIPv2
Incorrect. RIPv2 is an interior gateway protocol with limited scalability and hop-count limitations, making it unsuitable for redundant internet connections.
https://www.comptia.org/certifications/network

✗ **C** OSPF
Incorrect. OSPF is an interior gateway protocol commonly used within an autonomous system; it is not the standard protocol for connecting an organization redundantly to external internet providers.
https://www.comptia.org/certifications/network

✓ **D** BGP
Correct. BGP is the exterior gateway protocol used to exchange routing information between autonomous systems and is the most likely choice for redundant or multihomed internet connections.
https://www.comptia.org/certifications/network

Question 30

Single choice · Domain: D2 Network implementation › Implement quality of service (QoS) to prioritize network traffic over a link

A network engineer needs to prioritize traffic over a link with the goal of more effectively utilizing the connection. Which of the following should the engineer implement?

A. CDN
B. VPN
C. TTL
D. QoS

Answer: D. QoS

Explanation

This question tests the ability to select QoS mechanisms that classify and prioritize traffic so that bandwidth on a constrained link is used more effectively.

✗ **A** CDN
Incorrect. A content delivery network distributes cached content from geographically closer servers to improve content-delivery performance; it does not prioritize traffic on an existing network link.
https://www.comptia.org/certifications/network

✗ **B** VPN
Incorrect. A virtual private network provides an encrypted or logically isolated connection across another network, but it does not inherently prioritize traffic to improve link utilization.
https://www.comptia.org/certifications/network

✗ **C** TTL
Incorrect. Time to Live limits the number of router hops a packet can traverse to prevent routing loops; it does not manage traffic priority or bandwidth allocation.
https://www.comptia.org/certifications/network

✓ **D** QoS
Correct. Quality of Service classifies and prioritizes network traffic, allowing important traffic to receive preferential treatment over a constrained link and improving effective utilization.
https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 31

Single choice · Domain: D2 Network implementation › Implement Spanning Tree Protocol to provide Layer 2 switch redundancy and prevent switching loops

A network administrator must implement a feature that supports redundancy and scaling on the switches at the distribution layer of the network. Which of the following is the best option?

A. VLAN assignment
B. Spanning tree
C. Port speed
D. Full duplex

Answer: B. Spanning tree

Explanation

This question tests selecting the appropriate Layer 2 technology for redundant distribution-layer switch paths. Spanning Tree Protocol provides redundancy while preventing broadcast storms and switching loops caused by those paths.

✗ **A** VLAN assignment
Incorrect. VLAN assignment logically segments a network but does not provide redundant switch paths or prevent Layer 2 loops.

https://www.comptia.org/content/guides/what-is-networking

✓ **B** Spanning tree
Correct. Spanning Tree Protocol supports redundant Layer 2 paths by placing some paths in a blocking state and activating them if the primary path fails, preventing switching loops while maintaining availability.

https://www.comptia.org/content/guides/what-is-networking

✗ **C** Port speed
Incorrect. Increasing port speed improves link throughput but does not provide switch redundancy or protect against Layer 2 loops.

https://www.comptia.org/content/guides/what-is-networking

✗ **D** Full duplex
Incorrect. Full-duplex operation allows simultaneous transmission and reception on a link, but it does not provide redundant paths or loop prevention between switches.

https://www.comptia.org/content/guides/what-is-networking

Dumpsgate

Question 32

Single choice · Domain: D2 Network implementation › Select an IPv6-capable interior routing protocol

A company is implementing a new internal network in which all devices use IPv6 addresses. Which of the following routing protocols will be best for this setup?

A. EIGRP
B. OSPFv3
C. BGP4
D. iBGP

Answer: B. OSPFv3

Explanation

This question tests the ability to select an appropriate routing protocol for an IPv6-only internal network. OSPFv3 is the OSPF version designed to support IPv6 routing.

✗ **A** EIGRP
Incorrect. EIGRP is primarily associated with IPv4 in this context; although Cisco provides an IPv6-capable EIGRP variant, the standard protocol choice for IPv6 internal routing is OSPFv3.

https://www.comptia.org/certifications/network

✓ **B** OSPFv3
Correct. OSPFv3 was developed to support IPv6 and is an appropriate interior gateway protocol for an IPv6-only internal network.

https://www.comptia.org/certifications/network

✗ **C** BGP4
Incorrect. BGP4 is primarily an exterior gateway protocol used to exchange routes between autonomous systems. It is not the best choice for routing within a new internal IPv6 network.

https://www.comptia.org/certifications/network

✗ **D** iBGP
Incorrect. iBGP is BGP used between routers within the same autonomous system, typically for distributing externally learned routes; it is not the preferred interior routing protocol for this IPv6-only network.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 33

Single choice · Domain: D2 Network implementation › Identify the BGP AS_PATH attribute used for loop avoidance

Which of the following does BGP use for loop avoidance?

A. Autonomous system path
B. Peer autonomous system
C. Autonomous system length
D. Public autonomous system

Answer: A. Autonomous system path

Explanation

This question tests knowledge of BGP route-selection and loop-prevention behavior. BGP examines the autonomous system path and rejects routes that already contain its own autonomous system number.

✓ **A** Autonomous system path
Correct. BGP uses the AS_PATH attribute for loop avoidance; a BGP router will not accept a route if its own autonomous system number is already present in the path.

https://www.comptia.org/certifications/network

✗ **B** Peer autonomous system
Incorrect. The peer autonomous system identifies the neighboring BGP system but is not the route attribute used to detect an existing loop.

https://www.comptia.org/certifications/network

✗ **C** Autonomous system length
Incorrect. AS_PATH length can influence BGP route selection, but length alone does not provide loop avoidance. BGP checks the autonomous system numbers listed in the path.

https://www.comptia.org/certifications/network

✗ **D** Public autonomous system
Incorrect. A public autonomous system number is an identifier used in Internet routing, not the BGP mechanism for detecting routing loops.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 34

Single choice · Domain: D2 Network implementation › Distinguish full-tunnel VPN configurations from other VPN deployment models

Which of the following VPN configurations forces a remote user to access internet resources through the corporate network?

A. Clientless
B. Site-to-site
C. SSE
D. Full-tunnel

Answer: D. Full-tunnel

Explanation

This question tests the ability to identify the VPN configuration that routes a remote user's internet-bound traffic through the corporate network. A full-tunnel VPN sends all client traffic through the VPN connection, rather than only traffic destined for corporate resources.

✗ **A** Clientless
Incorrect. A clientless VPN generally provides browser-based access to selected internal applications and does not inherently force all internet traffic through the corporate network.
https://www.comptia.org/content/guides/what-is-a-vpn

✗ **B** Site-to-site
Incorrect. A site-to-site VPN connects entire networks or locations; it does not describe the remote-user configuration that forces all internet traffic through the corporate network.
https://www.comptia.org/content/guides/what-is-a-vpn

✗ **C** SSE
Incorrect. Security service edge is a cloud-delivered security architecture, not the VPN tunnel-routing mode that specifically forces a remote user's internet traffic through the corporate network.
https://www.comptia.org/content/guides/what-is-a-vpn

✓ **D** Full-tunnel
Correct. A full-tunnel VPN routes all traffic from the remote user, including internet-bound traffic, through the corporate VPN gateway and network.
https://www.comptia.org/content/guides/what-is-a-vpn

Free demo · full exam: 594 questions

Question 35

Single choice · Domain: D2 Network implementation › Identify the appropriate location for an intermediate distribution frame (IDF) when extending a network

A network administrator is extending a network beyond the primary equipment location. Which of the following is where the administrator should install additional network switches?

A. MDF
B. VPC
C. VXLAN
D. IDF

Answer: D. IDF

Explanation

This question tests the ability to distinguish physical network distribution locations and select the proper location for additional access switches beyond the primary equipment room.

✗ **A** MDF
Incorrect. The main distribution frame (MDF) is the primary equipment location, typically housing core network equipment and the main connection point. Additional switches serving remote areas are normally installed in an IDF.

https://www.comptia.org/certifications/network

✗ **B** VPC
Incorrect. A virtual private cloud (VPC) is a logical cloud-networking construct, not a physical location for installing network switches.

https://www.comptia.org/certifications/network

✗ **C** VXLAN
Incorrect. VXLAN is a network virtualization and overlay technology used to extend Layer 2 networks across Layer 3 infrastructure; it is not a physical equipment location.

https://www.comptia.org/certifications/network

✓ **D** IDF
Correct. An intermediate distribution frame (IDF) is a secondary telecommunications or equipment room used beyond the MDF to house additional network switches and serve a remote area of the network.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 36

Single choice · Domain: D2 Network implementation › Configure Spanning Tree Protocol on switches to prevent Layer 2 switching loops

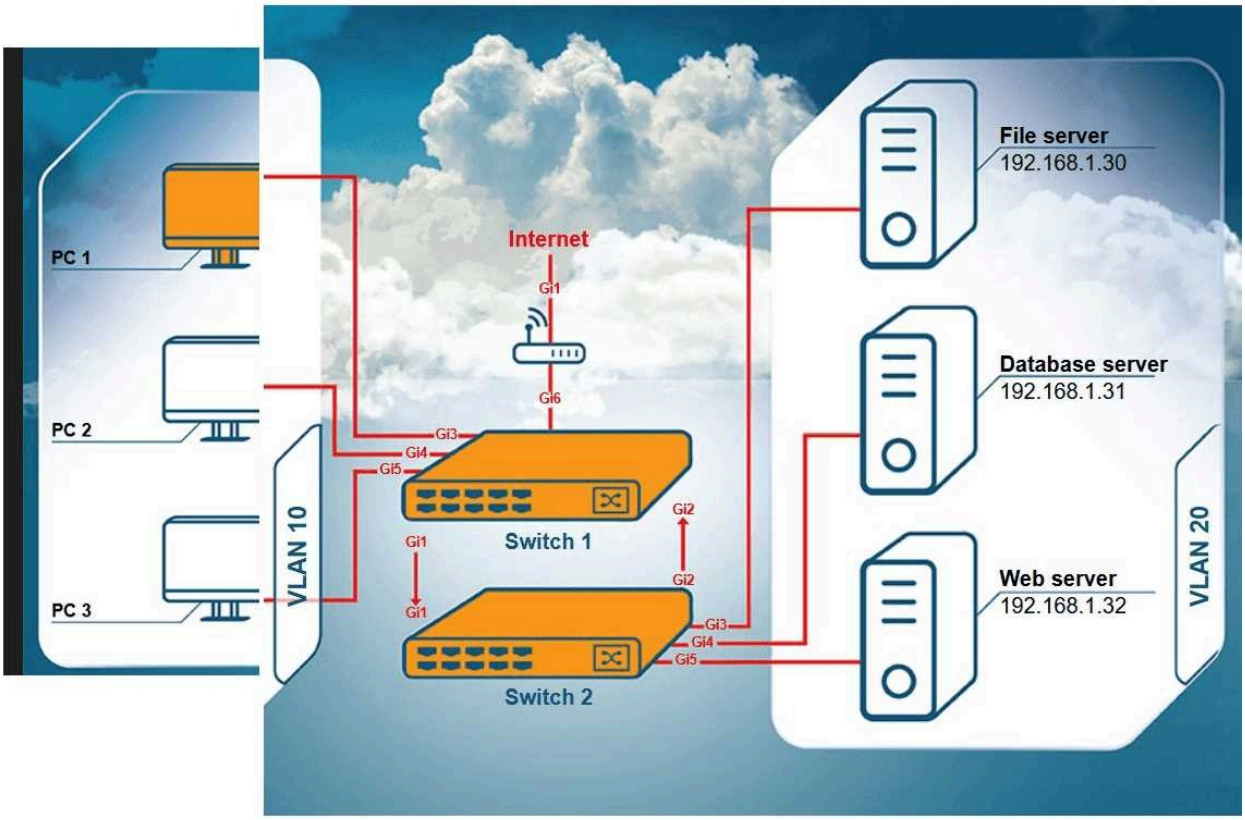
SIMULATION

A network technician receives a ticket from an employee who is working on PC 1 but is unable to connect to the database server. The technician pings the database server from PC 1, but the request times out. After reviewing the utilization of Switch 1 and Switch 2, the technician finds high CPU utilization and sees that the MAC table is continuously changing.

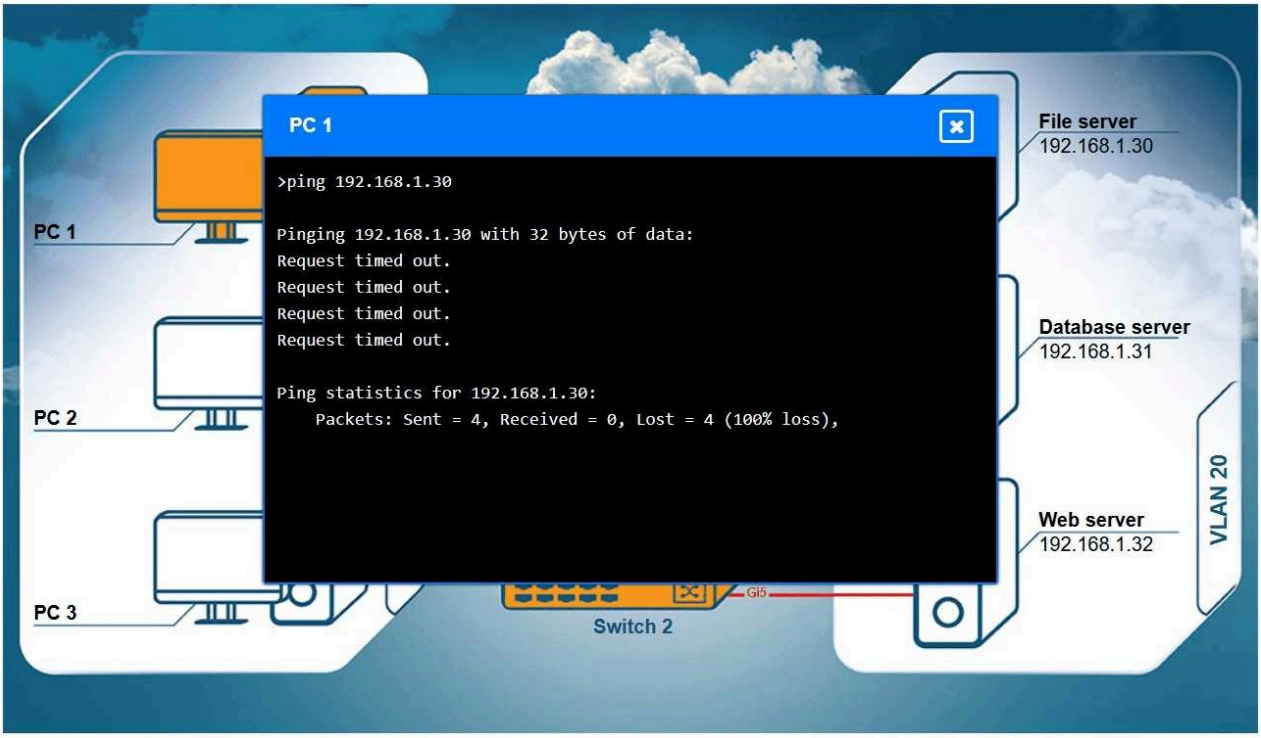
INSTRUCTIONS

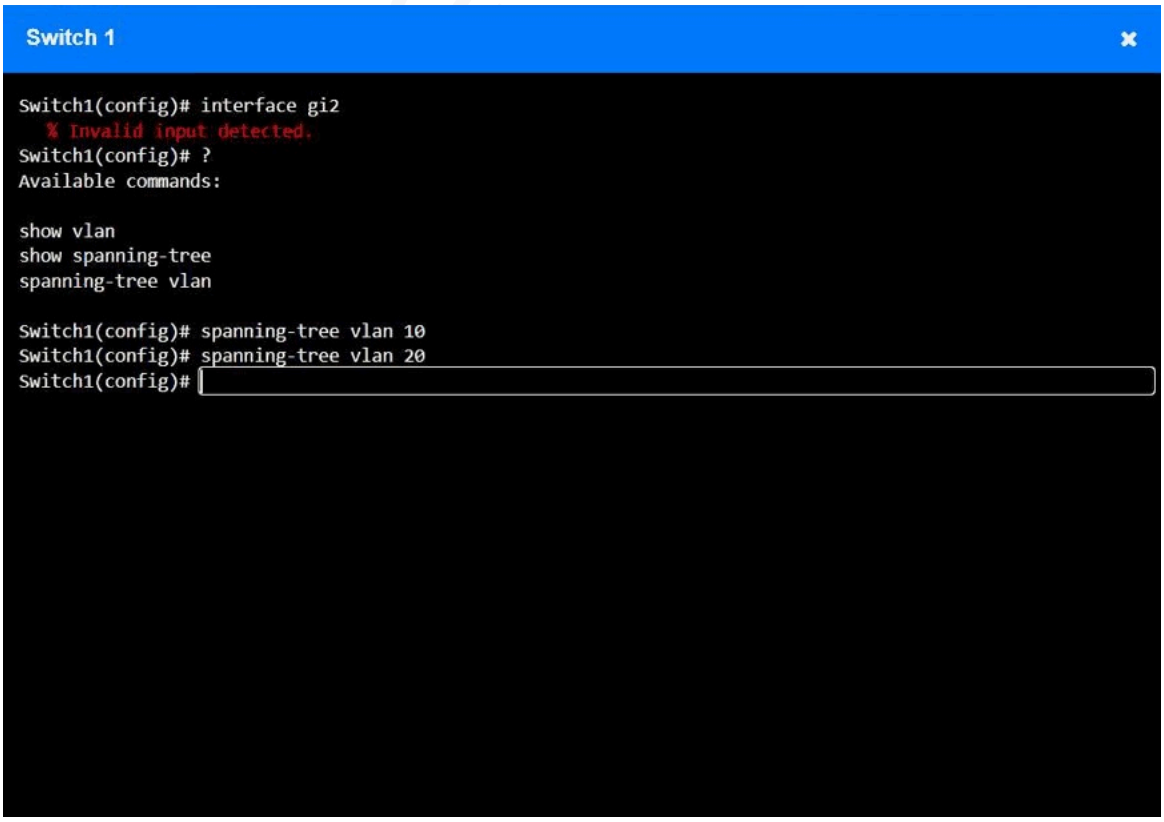
Configure Switch 1 and Switch 2 to remediate the employee's issue. Then, validate connectivity between PC 1 and the database server.

Switch 1 and Switch 2 are already in configuration mode. Type help to view a list of available commands.



Free demo · full exam: 594 questions


PC 1
>ping 192.168.1.30
Pinging 192.168.1.30 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.30:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC 1
PC 2
PC 3
File server
192.168.1.30
Database server
192.168.1.31
Web server
192.168.1.32
VLAN 20
Gi5
Switch 2


Switch 1
Switch1(config)# interface gi2
% Invalid input detected.
Switch1(config)# ?
Available commands:
show vlan
show spanning-tree
spanning-tree vlan
Switch1(config)# spanning-tree vlan 10
Switch1(config)# spanning-tree vlan 20
Switch1(config)#

A. On Switch 1 and Switch 2, enable spanning tree for VLAN 10 and VLAN 20, then verify connectivity by pinging 192.168.1.31 from PC 1

Answer: A. On Switch 1 and Switch 2, enable spanning tree for VLAN 10 and VLAN 20, then verify connectivity by pinging 192.168.1.31 from PC 1

Explanation

The continuously changing MAC address table and high switch CPU utilization indicate a Layer 2 switching loop or broadcast storm. Enabling spanning tree for VLANs 10 and 20 on both switches allows redundant paths to be blocked and restores stable connectivity between PC 1 and the database server.

✓ **A** On Switch 1 and Switch 2, enable spanning tree for VLAN 10 and VLAN 20, then verify connectivity by pinging 192.168.1.31 from PC 1
Correct. The changing MAC table and high CPU utilization are symptoms of a Layer 2 loop. Enabling Spanning Tree Protocol for both VLANs allows the switches to detect and block a redundant path, stopping the loop and allowing traffic to reach the database server.

https://www.comptia.org/certifications/network

Question 37

Single choice · Domain: D2 Network implementation › Configure IPv4 DHCP scopes and reservations to provide addresses within the correct subnet

Ten new laptops are added to an existing network, and they can only communicate with one another.

An administrator reviews documentation and sees the following:

Subnet: 10.8.100.1/24

Scope: 10.8.100.50 – 10.8.100.150

Reservation: 10.8.100.151 – 10.8.100.175

A technician scans the network and receives the following results:

IP addresses used: 10.8.100.45 – 10.8.100.175

Which of the following should be done to ensure connectivity on all laptops?

A. Increase the scope to 10.8.100.35 – 10.8.100.150
B. Increase the scope to 10.8.100.40 – 10.8.100.150
C. Increase the scope to 10.8.100.40 – 10.8.100.175
D. Increase the scope to 10.8.100.50 – 10.8.100.175

Answer: C. Increase the scope to 10.8.100.40 – 10.8.100.175

Explanation

This question tests the ability to align a DHCP scope with the IP addresses required by hosts on a /24 network. The scope must include the observed client address range while remaining within the 10.8.100.0/24 subnet.

✗ **A** Increase the scope to 10.8.100.35 – 10.8.100.150
Incorrect. This range includes addresses below the observed starting address but does not extend through the reservation range ending at 10.8.100.175.

https://www.comptia.org/certifications/network

✗ **B** Increase the scope to 10.8.100.40 – 10.8.100.150
Incorrect. The scope still ends at 10.8.100.150 and therefore does not cover the addresses through 10.8.100.175 used by hosts in the network.

https://www.comptia.org/certifications/network

✓ **C** Increase the scope to 10.8.100.40 – 10.8.100.175
Correct. This scope encompasses the observed address range from 10.8.100.45 through 10.8.100.175 and remains within the 10.8.100.0/24 subnet, allowing the laptops to receive addresses from the appropriate DHCP range.

https://www.comptia.org/certifications/network

✗ **D** Increase the scope to 10.8.100.50 – 10.8.100.175
Incorrect. This range covers the reservation addresses but does not include the used addresses beginning at 10.8.100.45, so it does not cover all observed hosts.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 38

Single choice · Domain: D2 Network implementation › Configure link aggregation to provide redundant, higher-bandwidth switch connections

A network administrator needs to configure the core switches where multiple connections between data centers are used. Given the following requirements:

• Fault tolerance and redundancy
• Vendor interoperability
• Increased bandwidth
• Cost effectiveness
• Simplified management

Which of the following should the administrator configure?

A. Spanning tree
B. Interface speeds to 10GB
C. Link aggregation
D. Jumbo frames

Answer: C. Link aggregation

Explanation

This question tests the ability to select link aggregation for combining multiple physical links into one logical connection. Link aggregation provides redundancy, increased bandwidth, simplified management, and vendor interoperability when using standards-based protocols such as LACP.

✗ **A** Spanning tree
Incorrect. Spanning Tree Protocol prevents Layer 2 switching loops by blocking redundant paths, but it does not combine multiple links to increase bandwidth.

https://www.comptia.org/certifications/network

✗ **B** Interface speeds to 10GB
Incorrect. Increasing individual interface speed can improve throughput, but it does not provide the required link-level redundancy, aggregation, or simplified management for multiple connections.

https://www.comptia.org/certifications/network

✓ **C** Link aggregation
Correct. Link aggregation combines multiple physical connections into a logical link, providing fault tolerance, increased aggregate bandwidth, simplified management, and interoperability when standards-based LACP is used.

https://www.comptia.org/certifications/network

✗ **D** Jumbo frames
Incorrect. Jumbo frames increase the maximum Ethernet frame size and can reduce protocol overhead for supported traffic, but they do not provide connection redundancy, link aggregation, or increased aggregate bandwidth across multiple connections.

https://www.comptia.org/certifications/network

Question 39

Single choice · Domain: D2 Network implementation › Configure quality of service (QoS) to prioritize voice traffic

A network administrator is responding to a request to configure a new IP phone. Which of the following should the network administrator do to allow data and voice traffic to be properly prioritized?

A. Configure full duplex.
B. Modify QoS.
C. Enable 802.1Q tagging.
D. Change the native VLAN.

Answer: B. Modify QoS.

Explanation

This question tests the ability to apply QoS so latency-sensitive IP voice traffic receives appropriate priority over ordinary data traffic. QoS is the feature that manages traffic prioritization; duplex and VLAN settings do not by themselves prioritize packets.

✗ **A** Configure full duplex.
Incorrect. Full duplex allows simultaneous transmission and reception and helps prevent collisions, but it does not classify or prioritize voice traffic.
https://www.comptia.org/certifications/network

✓ **B** Modify QoS.
Correct. Quality of service (QoS) classifies and prioritizes traffic, allowing voice packets to receive preferential treatment over data traffic and reducing the effects of delay, jitter, and congestion.
https://www.comptia.org/certifications/network

✗ **C** Enable 802.1Q tagging.
Incorrect. IEEE 802.1Q tagging identifies VLAN membership and can support voice and data VLAN separation, but tagging alone does not prioritize traffic. QoS must be configured for prioritization.
https://www.comptia.org/certifications/network

✗ **D** Change the native VLAN.
Incorrect. The native VLAN identifies untagged traffic on an 802.1Q trunk; changing it does not establish priority for voice traffic and may create connectivity or security problems if done unnecessarily.
https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 40

Single choice · Domain: D3 Network operations › Select redundant power infrastructure to maintain network-device availability during an outage

Which of the following provides two switches with the most uptime if a power outage occurs?

A. Plugging both switches into the same PDU
B. Plugging each switch into a different circuit
C. Plugging each switch into a different PDU
D. Plugging each switch into a different UPS

Answer: D. Plugging each switch into a different UPS

Explanation

This question tests high-availability planning for network devices by comparing shared and independent power-distribution and backup options. An independent UPS provides battery backup and avoids a shared power failure, maximizing expected uptime.

✗ **A** Plugging both switches into the same PDU
Incorrect. A shared PDU creates a single point of failure; if the PDU or its upstream power source fails, both switches can lose power.

https://www.comptia.org/certifications/network

✗ **B** Plugging each switch into a different circuit
Incorrect. Separate circuits can improve power-path redundancy, but they do not inherently provide battery backup during a utility outage.

https://www.comptia.org/certifications/network

✗ **C** Plugging each switch into a different PDU
Incorrect. Separate PDUs reduce dependence on one PDU, but ordinary PDUs do not provide backup power during an outage.

https://www.comptia.org/certifications/network

✓ **D** Plugging each switch into a different UPS
Correct. Separate UPS units provide each switch with independent battery-backed power, avoiding a shared UPS failure and providing the best uptime during a power outage.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 41

Single choice · Domain: D3 Network operations › Identify required disaster recovery plan components, including regular data backups

A company is implementing a disaster recovery plan in case of a network security incident. Which of the following steps must be included in the disaster recovery plan?

A. Schedule network vulnerability scans
B. Install antivirus software on all devices
C. Back up all data regularly
D. Deploy an IDS on all networks

Answer: C. Back up all data regularly

Explanation

This question tests recognition of a fundamental disaster recovery activity: maintaining recoverable copies of data so services and information can be restored after a security incident.

✗ **A** Schedule network vulnerability scans
Incorrect. Vulnerability scans are important for identifying security weaknesses, but they are a preventive security activity rather than a core disaster recovery step for restoring data after an incident.
https://www.comptia.org/content/guides/what-is-disaster-recovery

✗ **B** Install antivirus software on all devices
Incorrect. Antivirus software helps prevent or detect malware, but it does not provide the recoverable data and restoration capability required by a disaster recovery plan.
https://www.comptia.org/content/guides/what-is-disaster-recovery

✓ **C** Back up all data regularly
Correct. Regular backups provide recoverable copies of data that can be restored after a network security incident, making them an essential disaster recovery measure.
https://www.comptia.org/content/guides/what-is-disaster-recovery

✗ **D** Deploy an IDS on all networks
Incorrect. An intrusion detection system can identify suspicious activity, but detection is a security monitoring function and does not by itself enable recovery of systems or data after an incident.
https://www.comptia.org/content/guides/what-is-disaster-recovery

Free demo · full exam: 594 questions

Question 42

Single choice · Domain: D3 Network operations › Identify the purpose of a central repository for storing network infrastructure configurations

Which of the following describes a company that houses all of its critical network infrastructure configurations in one location?

A. Central repository
B. Version control
C. Conflict mitigation
D. Branching

Answer: A. Central repository

Explanation

This question tests knowledge of configuration-management practices used to maintain critical network infrastructure information. A central repository stores configurations in one controlled location for consistent access and management.

✓ **A** Central repository
Correct. A central repository is a single location used to store and manage critical network infrastructure configurations.

https://www.comptia.org/certifications/network

✗ **B** Version control
Incorrect. Version control tracks and manages changes to configuration files over time; it does not specifically describe the single location where configurations are housed.

https://www.comptia.org/certifications/network

✗ **C** Conflict mitigation
Incorrect. Conflict mitigation consists of practices used to prevent or resolve competing configuration changes, not the storage location for configurations.

https://www.comptia.org/certifications/network

✗ **D** Branching
Incorrect. Branching creates separate development or configuration paths so changes can be worked on independently; it does not describe housing all configurations in one location.

https://www.comptia.org/certifications/network

Dumpsgate

Question 43

Single choice · Domain: D3 Network operations › Select an out-of-band management method to preserve remote administrative access when in-band SSH management is unavailable

Which of the following should a network technician do to maintain remote administrative redundancy if a switch becomes unresponsive through SSH?

A. Deploy a jump host
B. Use an out-of-band management solution
C. Enable an administrative GUI
D. Connect a physical console cable

Answer: B. Use an out-of-band management solution

Explanation

This question tests remote-management redundancy and the distinction between in-band access such as SSH and an independent out-of-band management path.

✗ **A** Deploy a jump host
Incorrect. A jump host can centralize or broker administrative connections, but it still depends on the switch's reachable management service and does not provide an independent path when SSH on the switch is unresponsive.

https://www.comptia.org/certifications/network

✓ **B** Use an out-of-band management solution
Correct. Out-of-band management uses a separate management path from the production network and can preserve remote administrative access when the switch's in-band SSH service is unavailable.

https://www.comptia.org/certifications/network

✗ **C** Enable an administrative GUI
Incorrect. An administrative GUI is another management interface on the switch and generally remains dependent on the same device availability and in-band network path; it does not provide management redundancy by itself.

https://www.comptia.org/certifications/network

✗ **D** Connect a physical console cable
Incorrect. A physical console connection can provide local recovery access, but it is not remote administrative redundancy. An out-of-band management solution is the appropriate remote alternative.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 44

Single choice · Domain: D3 Network operations › Apply hardware lifecycle management practices for end-of-life network devices

Which of the following is a best practice when a hardware device reaches its end of life?

A. Purchasing an extended warranty and support
B. Decommissioning and replacing the device
C. Selling or donating the device
D. Using the device for testing and training

Answer: B. Decommissioning and replacing the device

Explanation

This question tests the ability to identify the appropriate operational response when network hardware reaches end of life. End-of-life equipment should be formally decommissioned and replaced to maintain supportability, security, and reliability.

✗ **A** Purchasing an extended warranty and support
Incorrect. Extended warranties or support may not be available for end-of-life hardware and do not address the risks of unsupported equipment.

https://www.comptia.org/content/articles/what-is-end-of-life-eol

✓ **B** Decommissioning and replacing the device
Correct. Decommissioning end-of-life hardware and replacing it with supported equipment is the best practice because the device may no longer receive security updates, vendor support, or replacement parts.

https://www.comptia.org/content/articles/what-is-end-of-life-eol

✗ **C** Selling or donating the device
Incorrect. Selling or donating end-of-life equipment can transfer unsupported hardware to another party and may create data-security concerns unless the device is properly sanitized and disposal requirements are met.

https://www.comptia.org/content/articles/what-is-end-of-life-eol

✗ **D** Using the device for testing and training
Incorrect. Reusing end-of-life hardware for testing or training may be acceptable in limited circumstances, but it is not the best general lifecycle practice because the equipment remains unsupported and may not represent current production technology.

https://www.comptia.org/content/articles/what-is-end-of-life-eol

Free demo · full exam: 594 questions

Question 45

Single choice · Domain: D3 Network operations › Update IP address management records when assigning or configuring network interfaces

A network engineer deploys ten new virtual servers and configures the NICs. Which of the following should the engineer update?

A. Asset inventory
B. Warranty support
C. Rack diagrams
D. IP address management

Answer: D. IP address management

Explanation

Configuring NICs on newly deployed virtual servers requires documenting their assigned IP addresses and related network details in the IP address management system. This tests network documentation and operational record-keeping practices covered by CompTIA Network+. Reference: https://www.comptia.org/certifications/network

✗ **A** Asset inventory
Incorrect. An asset inventory may eventually be updated to record the new virtual servers, but the configuration of their NICs specifically requires documenting address assignments in IP address management.

https://www.comptia.org/certifications/network

✗ **B** Warranty support
Incorrect. Virtual server NIC configuration does not require updating warranty or support information. Warranty records concern vendor coverage rather than network addressing.

https://www.comptia.org/certifications/network

✗ **C** Rack diagrams
Incorrect. Virtual servers and their virtual NICs do not represent new physical equipment that needs to be added to a rack diagram.

https://www.comptia.org/certifications/network

✓ **D** IP address management
Correct. Configuring the NICs on new virtual servers involves assigning or recording IP addresses, so the IP address management system must be updated to maintain accurate address-allocation records and prevent conflicts.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 46

Single choice · Domain: D3 Network operations › Identify infrastructure as code (IaC) as a method for consistent and automated infrastructure provisioning and management

A company is migrating a data center from on premises to the cloud. Which of the following tools will help maintain consistency, reliability, and efficiency of provisioning and management?

A. IaC
B. CDN
C. SASE
D. ZTA

Answer: A. IaC

Explanation

This question tests the ability to select an operational tool that improves consistency, reliability, and efficiency when provisioning and managing cloud infrastructure.

✓ **A** IaC
Correct. Infrastructure as code uses machine-readable definitions to automate and standardize infrastructure provisioning and management, which supports consistent, reliable, and efficient cloud migrations.
https://www.comptia.org/content/articles/what-is-infrastructure-as-code-iac

✗ **B** CDN
Incorrect. A content delivery network distributes cached content geographically to improve content delivery performance; it is not primarily a tool for consistently provisioning and managing infrastructure.
https://www.comptia.org/content/articles/what-is-infrastructure-as-code-iac

✗ **C** SASE
Incorrect. Secure Access Service Edge combines networking and security capabilities delivered from the cloud, but it does not specifically automate infrastructure provisioning and management.
https://www.comptia.org/content/articles/what-is-infrastructure-as-code-iac

✗ **D** ZTA
Incorrect. Zero Trust Architecture is a security model based on continuous verification and least-privilege access; it is not a provisioning and configuration-management tool.
https://www.comptia.org/content/articles/what-is-infrastructure-as-code-iac

Free demo · full exam: 594 questions

Question 47

Single choice · Domain: D3 Network operations › Identify and distinguish SNMP traps from SNMP management objects and identifiers

A network administrator wants an automatic alert to be sent when a switch's link status changes, administered through SNMP. Which of the following SNMP technologies will allow for this alert?

A. Trap
B. Object identifier
C. String
D. MIB

Answer: A. Trap

Explanation

This question tests recognition of SNMP trap messages as unsolicited notifications sent by a managed device when an event, such as a switch link-status change, occurs. This aligns with Network+ knowledge of network monitoring and management technologies.

✓ **A** Trap
Correct. An SNMP trap is an unsolicited alert sent by an SNMP-managed device to a monitoring system when an event occurs, such as a link going up or down.

https://www.comptia.org/certifications/network

✗ **B** Object identifier
Incorrect. An object identifier (OID) uniquely identifies a managed object or metric in the SNMP hierarchy; it does not itself send alerts.

https://www.comptia.org/certifications/network

✗ **C** String
Incorrect. An SNMP community string is used for authentication or access control in applicable SNMP versions, not for generating event alerts.

https://www.comptia.org/certifications/network

✗ **D** MIB
Incorrect. A Management Information Base (MIB) defines the collection of managed objects that SNMP can monitor; it is not the notification mechanism.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 48

Single choice · Domain: D3 Network operations › Select a SIEM platform to correlate security events and generate alerts

A network engineer needs to correlate findings and receive alerts if there are brute force attacks, DDoS attacks, or port scanning happening within their network. Which of the following network monitoring technologies should the engineer implement?

A. Packet capture
B. SNMPv3
C. SIEM
D. Syslog collector

Answer: C. SIEM

Explanation

The question tests the ability to identify the monitoring technology that aggregates and correlates events from multiple sources to detect brute-force attacks, DDoS activity, and port scans and issue alerts.

✗ **A** Packet capture
Incorrect. Packet capture records and analyzes network traffic, but it does not inherently correlate events across multiple sources or provide centralized security alerting for these attack patterns.
https://www.comptia.org/content/articles/what-is-siem

✗ **B** SNMPv3
Incorrect. SNMPv3 provides secure monitoring and management of network devices, but it is not a security-event correlation platform for identifying brute-force attacks, DDoS attacks, and port scans.
https://www.comptia.org/content/articles/what-is-siem

✓ **C** SIEM
Correct. A security information and event management system aggregates logs and security events from different sources, correlates related findings, and generates alerts for suspicious activity such as brute-force attacks, DDoS attacks, and port scanning.
https://www.comptia.org/content/articles/what-is-siem

✗ **D** Syslog collector
Incorrect. A syslog collector centralizes log messages, but by itself it generally does not perform the advanced cross-source correlation and security alerting provided by a SIEM.
https://www.comptia.org/content/articles/what-is-siem

Question 49

Single choice · Domain: D4 Network security › Identify the network resource most directly impacted by a denial-of-service attack

Which of the following is most likely affected when executing a successful DoS attack?

A. Bandwidth
B. NAT pool
C. ACL
D. Storage availability

Answer: A. Bandwidth

Explanation

This question tests recognition that a successful DoS attack overwhelms or exhausts a service or network resource, most commonly consuming available bandwidth and preventing legitimate users from accessing resources.

✓ **A** Bandwidth
Correct. A DoS attack commonly floods a target with traffic or requests, consuming available bandwidth and preventing legitimate traffic from reaching the service.
https://www.comptia.org/content/articles/what-is-a-denial-of-service-attack

✗ **B** NAT pool
Incorrect. A NAT pool can be exhausted by certain attacks, but it is not the resource most generally affected by a successful DoS attack.
https://www.comptia.org/content/articles/what-is-a-denial-of-service-attack

✗ **C** ACL
Incorrect. An access control list determines whether traffic is permitted or denied; a DoS attack does not typically modify or directly affect the ACL.
https://www.comptia.org/content/articles/what-is-a-denial-of-service-attack

✗ **D** Storage availability
Incorrect. Storage availability can be affected by resource-exhaustion attacks, but bandwidth is the most likely general network resource affected by a DoS attack.
https://www.comptia.org/content/articles/what-is-a-denial-of-service-attack

Dumpsgate

Question 50

Single choice · Domain: D4 Network security › Deploy a screened subnet or DMZ to isolate an external-facing web server

An administrator must increase the security posture of an organization. The goal is to restrict the external-facing web server from communicating with the internal organization. Which of the following is the most cost-effective deployment?

A. An IPS between the internet and the web server
B. An ACL to only allow traffic from the web server
C. A screened subnet for the web server
D. A WAF directly on the web server

Answer: C. A screened subnet for the web server

Explanation

This question tests the ability to place a public-facing server in a screened subnet, commonly called a DMZ, so it can be accessed externally without permitting direct communication with the internal network.

✗ **A** An IPS between the internet and the web server
Incorrect. An IPS can detect and block malicious traffic, but it does not by itself provide network segmentation that prevents the web server from communicating with the internal organization.
https://www.comptia.org/certifications/network/network

✗ **B** An ACL to only allow traffic from the web server
Incorrect. An ACL can filter traffic based on rules, but this option does not establish a dedicated security boundary around the external-facing server and may not prevent all unintended communication with internal systems.
https://www.comptia.org/certifications/network/network

✓ **C** A screened subnet for the web server
Correct. A screened subnet, or DMZ, places the public-facing web server on a separate network segment between external and internal security controls. This restricts direct communication between the web server and the internal organization while providing a cost-effective segmentation design.
https://www.comptia.org/content/articles/what-is-a-dmz

✗ **D** A WAF directly on the web server
Incorrect. A WAF protects web applications from application-layer attacks, such as malicious HTTP requests, but it does not isolate the web server from the internal network.
https://www.comptia.org/certifications/network/network

Free demo · full exam: 594 questions

Question 51

Single choice · Domain: D4 Network security › Identify single sign-on (SSO) as an authentication method for accessing multiple services with one set of credentials

Which of the following allows an individual to access multiple websites using one set of credentials?

A. SAML
B. One-time password
C. OpenID Connect
D. SSO

Answer: D. SSO

Explanation

This question tests recognition of authentication and identity-management technologies. SSO allows a user to authenticate once and access multiple websites or services without entering separate credentials for each one.

✗ **A** SAML
Incorrect. SAML is an XML-based federation protocol commonly used to implement SSO, but it is the underlying exchange standard rather than the general capability described in the question.

https://www.comptia.org/content/articles/what-is-single-sign-on-sso

✗ **B** One-time password
Incorrect. A one-time password is a temporary authentication code used to verify identity; it does not provide access to multiple websites through one authentication session.

https://www.comptia.org/content/articles/what-is-single-sign-on-sso

✗ **C** OpenID Connect
Incorrect. OpenID Connect is an identity layer built on OAuth 2.0 that can support federated authentication and SSO, but the capability directly described is single sign-on itself.

https://www.comptia.org/content/articles/what-is-single-sign-on-sso

✓ **D** SSO
Correct. Single sign-on allows an individual to authenticate once and then access multiple websites or applications using the same credentials or authentication session.

https://www.comptia.org/content/articles/what-is-single-sign-on-sso

Dumpsgate

Question 52

Single choice · Domain: D4 Network security › Identify on-path attacks that intercept or modify communications between a client and a legitimate service

An executive is unable to log in to their bank account from a hotel lobby. When the executive uses a VPN connection, the web page looks different, and they are able to log in. Which of the following is this scenario an example of?

A. ARP spoofing
B. ARP poisoning
C. Evil twin
D. On-path attack

Answer: D. On-path attack

Explanation

The scenario describes an attacker positioned between the executive and the bank, altering the web content and potentially capturing or interfering with credentials. Using a VPN encrypts the traffic through the local network, preventing the on-path interception from affecting the session.

✗ **A** ARP spoofing
Incorrect. ARP spoofing is a technique in which forged ARP messages associate the attacker's MAC address with another host's IP address; it can enable an on-path attack but is not the broader attack described.

https://www.comptia.org/content/articles/what-is-a-man-in-the-middle-attack

✗ **B** ARP poisoning
Incorrect. ARP poisoning corrupts a device's ARP cache to redirect local-network traffic. The scenario does not specifically identify ARP manipulation, although ARP poisoning can be used to conduct an on-path attack.

https://www.comptia.org/content/articles/what-is-a-man-in-the-middle-attack

✗ **C** Evil twin
Incorrect. An evil twin is a fraudulent wireless access point that imitates a legitimate network. The key evidence here is that traffic is being intercepted or modified and that a VPN prevents the behavior, which identifies an on-path attack rather than specifically proving an evil-twin access point.

https://www.comptia.org/content/articles/what-is-a-man-in-the-middle-attack

✓ **D** On-path attack
Correct. An on-path attack places the attacker between the client and the legitimate bank service, allowing traffic or web content to be intercepted and altered. The VPN encrypts the connection and prevents the local attacker from reading or modifying the protected session.

https://www.comptia.org/content/articles/what-is-a-man-in-the-middle-attack

Free demo · full exam: 594 questions

Question 53

Single choice · Domain: D4 Network security › Select a content-filtering control to block access to specified websites

A cloud administrator must ensure that all access to social media websites is prohibited. Which of the following should the administrator use to prevent users from accessing those websites?

A. NAC
B. Screened subnet
C. VPN
D. Content filter

Answer: D. Content filter

Explanation

This question tests the ability to identify the security control that restricts access to websites based on categories, domains, URLs, or content. A content filter is specifically designed to prohibit access to social media websites.

✗ **A** NAC
Incorrect. Network access control (NAC) enforces access policies for devices and users connecting to a network, but it is not primarily used to block specific website categories.
https://www.comptia.org/content/articles/what-is-network-access-control

✗ **B** Screened subnet
Incorrect. A screened subnet, commonly implemented as a DMZ, isolates publicly accessible services from the internal network; it does not directly filter users' access to social media websites.
https://www.comptia.org/content/articles/what-is-a-firewall

✗ **C** VPN
Incorrect. A virtual private network (VPN) provides an encrypted connection across an untrusted network, but it is not the control used to prohibit access to selected website categories.
https://www.comptia.org/content/articles/what-is-a-vpn

✓ **D** Content filter
Correct. A content filter can block access to websites based on URLs, domains, categories, or content classifications, including social media.
https://www.comptia.org/content/articles/what-is-content-filtering

Free demo · full exam: 594 questions

Question 54

Single choice · Domain: D4 Network security › Identify and distinguish role-based access control from other access-control and authentication mechanisms

Which of the following is the best example of implementing role-based access control?

A. Granting data center access only to server and network administrators
B. Providing the entire IT department access to an application development server
C. Requiring all employees to use multifactor authentication when accessing the network
D. Allowing the human resources director to determine who can access human resources files

Answer: A. Granting data center access only to server and network administrators

Explanation

This question tests recognition of RBAC, in which permissions are assigned according to a user's organizational role. It also contrasts RBAC with broad access, multifactor authentication, and discretionary access control.

✓ **A** Granting data center access only to server and network administrators
Correct. This is role-based access control because access is granted according to defined job roles, such as server administrator or network administrator.

https://www.comptia.org/content/articles/what-is-role-based-access-control-rbac

✗ **B** Providing the entire IT department access to an application development server
Incorrect. Granting access to an entire department is broad group-based access and may provide more access than each individual requires; it is not the best example of permissions tied to specific job roles.

https://www.comptia.org/content/articles/what-is-role-based-access-control-rbac

✗ **C** Requiring all employees to use multifactor authentication when accessing the network
Incorrect. Multifactor authentication verifies identity using multiple authentication factors; it does not assign permissions based on a user's job role.

https://www.comptia.org/content/articles/what-is-multifactor-authentication-mfa

✗ **D** Allowing the human resources director to determine who can access human resources files
Incorrect. This describes discretionary access control, where an owner or authorized individual determines access, rather than permissions being assigned through predefined organizational roles.

https://www.comptia.org/content/articles/what-is-role-based-access-control-rbac

Free demo · full exam: 594 questions

Question 55

Single choice · Domain: D4 Network security › Select MAC filtering to restrict wireless network access by device hardware address

A network administrator needs to limit devices that can connect to a small wireless network. The network consists of less than ten unique laptops, and no network changes are anticipated. Which of the following is the simplest way to accomplish this task?

A. ACLs
B. MAC filtering
C. NAC
D. Trusted zones

Answer: B. MAC filtering

Explanation

This question tests the ability to choose a simple wireless access-control method for a small, static set of known devices. MAC filtering permits or denies connections based on each device's MAC address and is appropriate when few devices are involved and no frequent changes are expected.

✗ **A** ACLs
Incorrect. Access control lists can control traffic or access based on addresses, ports, protocols, or other criteria, but they are more general and are not the simplest choice for limiting a small, fixed set of wireless devices.

https://www.comptia.org/certifications/network

✓ **B** MAC filtering
Correct. MAC filtering allows or denies wireless devices based on their hardware MAC addresses. Because the network has fewer than ten known laptops and the device list is not expected to change, this is the simplest solution.

https://www.comptia.org/certifications/network

✗ **C** NAC
Incorrect. Network access control can enforce more comprehensive policies such as authentication, device posture, and authorization, but it is more complex than necessary for a small wireless network with a fixed set of laptops.

https://www.comptia.org/certifications/network

✗ **D** Trusted zones
Incorrect. Trusted zones are segmentation or security-policy concepts, not the simplest mechanism for permitting a fixed list of wireless devices. MAC filtering directly addresses this requirement.

https://www.comptia.org/certifications/network

Dumpsgate

Question 56

Single choice · Domain: D4 Network security › Evaluate SIEM solutions for compatibility with an organization's network-device log sources

An IT department is considering implementing a SIEM solution to improve network security. The department wants to ensure that the SIEM system is able to ingest and analyze logs from all of the company's core devices. Which of the following is the most important consideration when selecting a SIEM solution?

A. Easy to manage
B. Cost
C. Compatibility
D. Features

Answer: C. Compatibility

Explanation

This question tests the ability to select a SIEM based on whether it can ingest and analyze logs from all required core devices. Compatibility with existing log sources is essential for complete security monitoring and correlation.

✗ **A** Easy to manage
Ease of management is valuable for reducing administrative effort, but it does not ensure that the SIEM can ingest and analyze logs from the company's core devices.
https://www.comptia.org/content/articles/what-is-siem

✗ **B** Cost
Cost is an important procurement factor, but a less expensive SIEM that cannot process the required device logs would not meet the department's security-monitoring objective.
https://www.comptia.org/content/articles/what-is-siem

✓ **C** Compatibility
Correct. Compatibility determines whether the SIEM supports the log formats, collection methods, and device types used by the company, allowing it to ingest and analyze logs from all core devices.
https://www.comptia.org/content/articles/what-is-siem

✗ **D** Features
A broad feature set is useful, but features are not the most important consideration if the SIEM cannot collect and analyze logs from the organization's core devices.
https://www.comptia.org/content/articles/what-is-siem

Dumpsgate

Question 57

Single choice · Domain: D4 Network security › Differentiate between intrusion detection systems (IDS) and intrusion prevention systems (IPS) based on deployment and traffic-handling behavior

Which of the following is an advantage of using an IDS over an IPS?

A. An IDS requires less processing power to analyze traffic.
B. An IDS is less disruptive during the initial deployment of the technology.
C. An IDS is easier to restrict access.
D. An IDS is more accurate due to fewer false positives.

Answer: B. An IDS is less disruptive during the initial deployment of the technology.

Explanation

This question tests the ability to identify the operational advantage of passive IDS monitoring compared with inline IPS enforcement. An IDS can observe and alert without immediately blocking traffic, making initial deployment less disruptive.

✗ **A** An IDS requires less processing power to analyze traffic.
Incorrect. IDS and IPS technologies both analyze network traffic, so using an IDS does not inherently require less processing power.

https://www.comptia.org/content/articles/what-is-an-intrusion-detection-system

✓ **B** An IDS is less disruptive during the initial deployment of the technology.
Correct. An IDS is generally deployed out of band to monitor and alert without blocking traffic, reducing the risk of disrupting legitimate communications during initial deployment.

https://www.comptia.org/content/articles/what-is-an-intrusion-detection-system

✗ **C** An IDS is easier to restrict access.
Incorrect. Restricting or blocking access is primarily an IPS function because an IPS is deployed inline and can automatically prevent detected malicious traffic.

https://www.comptia.org/content/articles/what-is-an-intrusion-prevention-system-ips

✗ **D** An IDS is more accurate due to fewer false positives.
Incorrect. IDS technology can also generate false positives, and passive monitoring does not inherently make an IDS more accurate than an IPS.

https://www.comptia.org/content/articles/what-is-an-intrusion-detection-system

Question 58

Single choice · Domain: D4 Network security › Identify and implement network access control using 802.1X for secure BYOD access

A network engineer wants to implement an 802.1X architecture in which BYOD devices must access a trusted wireless network securely. Which of the following should the engineer implement?

A. ACL
B. MAC filtering
C. Port security
D. NAC

Answer: D. NAC

Explanation

This question tests selecting a network access control solution that authenticates and authorizes BYOD devices before permitting access to a trusted wireless network. 802.1X is commonly implemented as part of NAC architecture.

✗ **A** ACL
Incorrect. An access control list filters traffic based on criteria such as addresses, ports, or protocols, but it does not provide the 802.1X-based device and user admission control required for secure BYOD access.
https://www.comptia.org/certifications/network/network

✗ **B** MAC filtering
Incorrect. MAC filtering permits or denies devices based on their MAC addresses, which can be spoofed and does not provide the authentication and authorization capabilities of an 802.1X NAC implementation.
https://www.comptia.org/certifications/network/network

✗ **C** Port security
Incorrect. Port security restricts which MAC addresses can use a switch port and is primarily a Layer 2 switch-control feature; it is not the appropriate architecture for securely authenticating BYOD devices to a trusted wireless network through 802.1X.
https://www.comptia.org/certifications/network/network

✓ **D** NAC
Correct. Network access control (NAC) uses mechanisms such as 802.1X to authenticate and authorize users or devices before granting network access, making it appropriate for securely admitting BYOD devices to a trusted wireless network.
https://www.comptia.org/certifications/network/network

Free demo · full exam: 594 questions

Question 59

Single choice · Domain: D4 Network security › Select 802.1X port-based network access control for authenticated device access

A network administrator needs to ensure all network ports use a security method that only permits authenticated devices. The solution must meet the following requirements:

• Reduced chance of spoofing

• Centrally managed solution

• Auditable logs

Which of the following technologies provides this functionality?

A. MAC filtering
B. Port security
C. ACLs
D. 802.1X

Answer: D. 802.1X

Explanation

This question tests the ability to identify a centrally managed, auditable network access control method that authenticates devices before granting network access and reduces the effectiveness of spoofing attempts.

✗ **A** MAC filtering
Incorrect. MAC filtering permits or denies devices based on MAC addresses, but MAC addresses can be spoofed and the method does not provide the strong centralized authentication and auditing required.
https://www.comptia.org/certifications/network/network-plus

✗ **B** Port security
Incorrect. Switch port security can restrict the number or identity of MAC addresses on a port, but it is primarily a switch-level control and does not provide 802.1X-style centralized user or device authentication and auditing.
https://www.comptia.org/certifications/network/network-plus

✗ **C** ACLs
Incorrect. Access control lists filter traffic according to criteria such as source and destination addresses or ports; they do not authenticate devices before allowing network access.
https://www.comptia.org/certifications/network/network-plus

✓ **D** 802.1X
Correct. 802.1X provides port-based network access control, requiring a device to authenticate before the switch or wireless access point grants network access. Authentication can be centrally managed through an authentication server, and authentication events can be logged for auditing, while stronger identity validation reduces reliance on spoofable MAC addresses.
https://www.comptia.org/certifications/network/network-plus

Free demo · full exam: 594 questions

Question 60

Single choice · Domain: D4 Network security › Identify DNS poisoning as an attack that inserts fraudulent DNS records into a resolver's cache

Which of the following best describes a characteristic of a DNS poisoning attack?

A. DNS address records are edited and changed on a DNS server.
B. An attacker sets up a malicious DNS server in place of a legitimate server.
C. DNS client requests are intercepted and false responses are returned.
D. False DNS records are injected into cache on a DNS server.

Answer: D. False DNS records are injected into cache on a DNS server.

Explanation

This question tests recognition of DNS poisoning, in which an attacker causes a DNS resolver or server cache to store false name-to-address mappings. Those fraudulent records can redirect clients to malicious destinations.

✗ **A** DNS address records are edited and changed on a DNS server.
Incorrect. Directly editing legitimate DNS records is an administrative or server-compromise action, not the defining characteristic of DNS cache poisoning.

https://www.comptia.org/content/articles/what-is-dns

✗ **B** An attacker sets up a malicious DNS server in place of a legitimate server.
Incorrect. This describes replacing or impersonating a legitimate DNS server, rather than injecting fraudulent records into an existing DNS cache.

https://www.comptia.org/content/articles/what-is-dns

✗ **C** DNS client requests are intercepted and false responses are returned.
Incorrect. Intercepting requests and returning false replies is more specifically DNS spoofing or response forgery. DNS poisoning is characterized by false information being stored in a DNS cache so subsequent clients receive the malicious mapping.

https://www.comptia.org/content/articles/what-is-dns

✓ **D** False DNS records are injected into cache on a DNS server.
Correct. DNS poisoning, also called DNS cache poisoning, involves placing fraudulent DNS records in a resolver's cache. Clients are then directed to an incorrect or malicious IP address.

https://www.comptia.org/content/articles/what-is-dns

Free demo · full exam: 594 questions

Question 61

Single choice · Domain: D4 Network security › Identify the security property provided by cryptographic hashing

Which of the following does a hash provide?

A. Non-repudiation
B. Integrity
C. Confidentiality
D. Availability

Answer: B. Integrity

Explanation

This question tests recognition that hashing produces a fixed-length digest used to detect whether data has been altered. Hashing supports integrity, while confidentiality requires encryption and non-repudiation generally requires authenticated digital signatures.

✗ **A** Non-repudiation
Incorrect. A hash by itself does not prove who created or sent the data, so it does not provide non-repudiation. Digital signatures are typically used for that purpose.
https://www.comptia.org/content/articles/what-is-a-hash

✓ **B** Integrity
Correct. Comparing a calculated hash with a known trusted hash can reveal whether data has been modified, providing an integrity check.
https://www.comptia.org/content/articles/what-is-a-hash

✗ **C** Confidentiality
Incorrect. Hashing is not encryption and does not hide the original data. Confidentiality is provided by encryption and access controls.
https://www.comptia.org/content/articles/what-is-a-hash

✗ **D** Availability
Incorrect. Hashing does not ensure that systems or data remain accessible; availability is supported by measures such as redundancy, backups, and fault tolerance.
https://www.comptia.org/content/articles/what-is-a-hash

Free demo · full exam: 594 questions

Question 62

Single choice · Domain: D4 Network security › Identify denial-of-service attacks as threats to network and service availability

Which of the following impacts the availability of a web-based customer portal?

A. MAC flooding
B. ARP spoofing
C. DoS
D. Rogue devices

Answer: C. DoS

Explanation

This question tests recognition of which attack directly targets availability. A denial-of-service attack overwhelms or disrupts a service, preventing legitimate users from accessing the web-based customer portal.

✗ **A** MAC flooding
Incorrect. MAC flooding primarily targets a switch's MAC address table and may enable traffic interception; although it can disrupt switching, it is not the direct availability threat described here.
https://www.comptia.org/content/articles/what-is-a-denial-of-service-attack

✗ **B** ARP spoofing
Incorrect. ARP spoofing primarily redirects or intercepts local network traffic, affecting confidentiality or integrity rather than directly targeting the portal's availability.
https://www.comptia.org/content/articles/what-is-a-denial-of-service-attack

✓ **C** DoS
Correct. A denial-of-service attack attempts to make a service unavailable by overwhelming or disrupting it, which directly impacts access to a web-based customer portal.
https://www.comptia.org/content/articles/what-is-a-denial-of-service-attack

✗ **D** Rogue devices
Incorrect. Rogue devices are unauthorized systems connected to a network and represent an access-control or security risk; they do not inherently target the portal's availability.
https://www.comptia.org/content/articles/what-is-a-denial-of-service-attack

Dumpsgate

Question 63

Single choice · Domain: D4 Network security › Identify the appropriate use case for a site-to-site VPN

Which of the following is the best use case of a site-to-site VPN?

A. Securing access across an untrusted network
B. Encrypting data at rest
C. Filtering traffic between two internal subnets
D. Hosting public-facing applications that contain company resources

Answer: A. Securing access across an untrusted network

Explanation

This question tests the ability to distinguish a site-to-site VPN from other security and network-control technologies. A site-to-site VPN creates an encrypted connection between separate networks across an untrusted network such as the public internet.

✓ **A** Securing access across an untrusted network
Correct. A site-to-site VPN securely connects two networks over an untrusted intermediary network by encrypting traffic between VPN gateways.
https://www.comptia.org/certifications/network/network-plus

✗ **B** Encrypting data at rest
Incorrect. Data-at-rest encryption protects stored data on devices or media; it is not the primary purpose of a site-to-site VPN, which protects data in transit between networks.
https://www.comptia.org/certifications/network/network-plus

✗ **C** Filtering traffic between two internal subnets
Incorrect. Traffic filtering between internal subnets is typically performed by firewalls, access control lists, or other segmentation controls. A site-to-site VPN is intended to securely connect separate networks across an untrusted network.
https://www.comptia.org/certifications/network/network-plus

✗ **D** Hosting public-facing applications that contain company resources
Incorrect. Public-facing applications are commonly placed in a DMZ or other segmented network, whereas a site-to-site VPN provides a secure connection between networks.
https://www.comptia.org/certifications/network/network-plus

Free demo · full exam: 594 questions

Question 64

Single choice · Domain: D4 Network security › Identify SASE as a modern secure remote-access alternative to traditional VPNs

Which of the following would most likely be used as a replacement for a traditional VPN for remote users?

A. SD-WAN
B. SASE
C. Site-to-site VPN
D. Reverse proxy

Answer: B. SASE

Explanation

This question tests the ability to recognize SASE, which combines networking and security services delivered from the cloud and commonly provides secure, identity-aware access for remote users without relying on a traditional VPN.

✗ **A** SD-WAN
Incorrect. SD-WAN primarily optimizes and manages wide-area network connectivity between sites and cloud resources; it is not primarily a replacement for traditional remote-user VPN access.
https://www.comptia.org/content/articles/what-is-sase

✓ **B** SASE
Correct. Secure Access Service Edge (SASE) delivers converged cloud-based networking and security capabilities, including secure remote access that can replace or reduce dependence on traditional VPNs.
https://www.comptia.org/content/articles/what-is-sase

✗ **C** Site-to-site VPN
Incorrect. A site-to-site VPN connects entire networks or locations, rather than serving as the modern cloud-based remote-user access model described by the question.
https://www.comptia.org/content/articles/what-is-sase

✗ **D** Reverse proxy
Incorrect. A reverse proxy publishes or brokers access to specific applications and services, but it is not the broad secure networking and access architecture most associated with replacing traditional VPNs for remote users.
https://www.comptia.org/content/articles/what-is-sase

Free demo · full exam: 594 questions

Question 65

Single choice · Domain: D4 Network security › Identify the role of single sign-on (SSO) in federated identity and access management

Which of the following enables an organization to leverage an identity provider to manage access across SaaS applications?

A. PKI
B. SSO
C. TACACS+
D. RADIUS

Answer: B. SSO

Explanation

This question tests whether the candidate can identify SSO as the mechanism that allows an organization to use an identity provider to manage authentication and access across multiple SaaS applications.

✗ **A** PKI
Incorrect. Public key infrastructure (PKI) manages digital certificates, keys, and trust relationships; it is not the access mechanism described for centrally managing user access across SaaS applications.
https://www.comptia.org/certifications/network

✓ **B** SSO
Correct. Single sign-on (SSO) allows users to authenticate through a centralized identity provider and access multiple SaaS applications without separately signing in to each application.
https://www.comptia.org/certifications/network

✗ **C** TACACS+
Incorrect. TACACS+ is an AAA protocol commonly used to centralize authentication, authorization, and accounting for network device administration, not to provide federated access across SaaS applications.
https://www.comptia.org/certifications/network

✗ **D** RADIUS
Incorrect. RADIUS is an AAA protocol commonly used for network access such as VPNs and wireless authentication; it is not the capability described for accessing multiple SaaS applications through an identity provider.
https://www.comptia.org/certifications/network

Question 66

Single choice · Domain: D5 Network troubleshooting › Analyze how network technologies can introduce latency and contribute to packet loss or timeouts

Which of the following technologies most likely increases the potential for packet loss due to timeout?

A. Load balancer
B. IDS
C. CDN
D. QoS

Answer: B. IDS

Explanation

This question tests the ability to identify which network technology can add processing delay that may cause traffic to exceed timeout thresholds. It focuses on the relationship between network performance, latency, and packet loss.

✗ **A** Load balancer
Incorrect. A load balancer generally distributes traffic among multiple servers to improve availability and performance; it is not the technology most associated with inspection-related delays that can cause timeouts.

https://www.comptia.org/certifications/network

✓ **B** IDS
Correct. An intrusion detection system analyzes network traffic, and the additional inspection and processing can introduce latency. Excessive delay can cause packets or sessions to exceed timeout thresholds, increasing the potential for apparent packet loss.

https://www.comptia.org/certifications/network

✗ **C** CDN
Incorrect. A content delivery network places cached content closer to users, which normally reduces latency and the likelihood of timeouts rather than increasing it.

https://www.comptia.org/certifications/network

✗ **D** QoS
Incorrect. Quality of service prioritizes traffic and manages congestion. Although a QoS policy can intentionally drop lower-priority traffic, it is not primarily associated with packet loss caused by inspection-related timeout delays.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 67

Single choice · Domain: D5 Network troubleshooting › Use MAC addresses to identify and isolate a wireless client in a packet capture

A device is experiencing disconnection from the wireless network. A network support engineer needs to find the root cause of the issue. Which of the following should the engineer use to isolate the device in a packet capture?

A. ESSID
B. MAC
C. PSK
D. BSSID

Answer: B. MAC

Explanation

This question tests the ability to select the identifier that uniquely represents the affected device when examining captured wireless traffic. A client MAC address can be used as a filter to isolate that device's frames.

✗ **A** ESSID
Incorrect. The ESSID or SSID identifies the wireless network name, not a specific client device, so it cannot reliably isolate the affected device in a packet capture.

https://www.comptia.org/content/guides/what-is-a-wireless-network

✓ **B** MAC
Correct. A device's MAC address is its link-layer identifier and can be used to filter packet-capture traffic for that specific wireless client.

https://www.comptia.org/content/guides/what-is-a-mac-address

✗ **C** PSK
Incorrect. A pre-shared key is a wireless authentication credential, not an identifier present in packet captures for isolating a particular device.

https://www.comptia.org/content/guides/what-is-wi-fi-security

✗ **D** BSSID
Incorrect. The BSSID identifies the specific wireless access point or basic service set, so it can isolate an access point's traffic but not the individual client experiencing the disconnection.

https://www.comptia.org/content/guides/what-is-a-wireless-network

Dumpsgate

Question 68

Single choice · Domain: D5 Network troubleshooting › Establish a theory of probable cause by eliminating known issues

Which of the following steps in the troubleshooting methodology is used to strategically eliminate known issues before determining the main source of the reported issue?

A. Establishing a theory of probable cause
B. Establishing a plan of action to resolve the problem
C. Testing the theory to determine the cause
D. Identifying the problem

Answer: A. Establishing a theory of probable cause

Explanation

This question tests the troubleshooting methodology step in which known causes and common issues are considered and eliminated to narrow the investigation before testing the likely cause.

✓ **A** Establishing a theory of probable cause
Correct. Establishing a theory of probable cause involves systematically considering and eliminating known or likely issues to identify the most probable source of the reported problem.

https://www.comptia.org/certifications/network

✗ **B** Establishing a plan of action to resolve the problem
Incorrect. A plan of action is developed after the cause has been identified and is used to implement the appropriate resolution, not to eliminate possible causes.

https://www.comptia.org/certifications/network

✗ **C** Testing the theory to determine the cause
Incorrect. Testing the theory occurs after a probable cause has been established and confirms whether that theory explains the issue.

https://www.comptia.org/certifications/network

✗ **D** Identifying the problem
Incorrect. Identifying the problem involves gathering information, identifying symptoms, and determining the scope of the issue; it does not specifically describe strategically eliminating known causes.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 69

Single choice · Domain: D5 Network troubleshooting › Troubleshoot a missing fiber link caused by reversed transmit and receive connections

A network administrator installs a node that requires a media converter to connect Ethernet to fiber but sees no link light on the node. The administrator notices the following:

• Both terminating points are properly seated.

• Both the fiber and Ethernet cables have been successfully tested.

• The media converter is turned on.

• The switch port is configured as half duplex and enabled.

Which of the following is the reason the link light is not on?

A. The TX/RX connection is transposed.
B. The switch port is misconfigured.
C. One of the cables has a short.
D. The switch port interface has errors.

Answer: A. The TX/RX connection is transposed.

Explanation

This question tests identifying a physical-layer fiber connectivity problem after cables, terminations, power, and port enablement have been verified. Fiber links require the transmitter of one endpoint to connect to the receiver of the other endpoint.

✓ **A** The TX/RX connection is transposed.
Correct. Reversing the fiber transmit and receive strands connects TX to TX and RX to RX, preventing the endpoints from establishing a link and leaving the link light off.

https://www.comptia.org/certifications/network

✗ **B** The switch port is misconfigured.
Incorrect. The port is enabled and configured for half duplex. A duplex mismatch can affect performance, but it normally does not explain a completely absent physical link light.

https://www.comptia.org/certifications/network

✗ **C** One of the cables has a short.
Incorrect. Both cables were successfully tested, making a cable short unlikely. The described symptom is specifically consistent with reversed fiber TX/RX strands.

https://www.comptia.org/certifications/network

✗ **D** The switch port interface has errors.
Incorrect. Interface errors generally indicate problems after a link has been established and would not normally prevent the physical link light from turning on.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 70

Single choice · Domain: D5 Network troubleshooting › Isolate a client-specific connectivity problem by checking the endpoint firewall configuration

A network technician is investigating an issue in which a specific user is unable to access a server.

Other users in the company, however, can access the server. After checking the switch and router logs, the technician is unable to identify any issues. Which of the following troubleshooting steps should the technician take next?

A. Inspect the client's firewall configuration
B. Update the network equipment's firmware
C. Check the server's DNS configuration
D. Check the server's event logs

Answer: A. Inspect the client's firewall configuration

Explanation

Because other users can access the server and network-device logs show no issue, the fault is likely isolated to the affected client. The next step is to inspect the client firewall for rules blocking the server connection.

✓ **A** Inspect the client's firewall configuration
Correct. A single-user access problem with other users able to reach the same server points to an endpoint-specific issue. The client firewall may be blocking the required traffic or application.

https://www.comptia.org/certifications/network

✗ **B** Update the network equipment's firmware
Incorrect. Updating switch or router firmware is not the next logical step when only one user is affected and network-device logs do not identify a problem.

https://www.comptia.org/certifications/network

✗ **C** Check the server's DNS configuration
Incorrect. A server-wide DNS problem would generally affect multiple users, not just one client. The evidence points first to the affected endpoint.

https://www.comptia.org/certifications/network

✗ **D** Check the server's event logs
Incorrect. Server event logs could be useful later, but the server is accessible to other users, making a client-side firewall or configuration issue more likely as the next troubleshooting step.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 71

Single choice · Domain: D5 Network troubleshooting › Identify fiber-optic polarity and connectivity faults

A network administrator upgrades the network infrastructure from copper wiring to fiber connections to increase throughput between network closets. After the upgrade, most of the new connections come online, but one connection remains offline. During troubleshooting with a visual fault locator, the administrator verifies that the final connection was terminated properly. Which of the following is the most likely issue with the fiber connection?

A. Transposed TX/RX
B. Incorrect SFP
C. Incompatible cable
D. CRC errors

Answer: A. Transposed TX/RX

Explanation

This question tests troubleshooting a fiber link that remains offline after proper termination. Reversed transmit and receive fibers prevent the optical transceivers from establishing a link even though the cable passes a visual inspection.

✓ **A** Transposed TX/RX
Correct. In a duplex fiber connection, the transmit fiber from one device must connect to the receive fiber on the other device. Transposing TX and RX prevents link establishment, while a visual fault locator can still confirm continuity and proper termination.
https://www.comptia.org/certifications/network

✗ **B** Incorrect SFP
Incorrect. An incompatible or incorrect SFP can cause a link failure, but the scenario emphasizes a properly terminated fiber connection and points to a polarity problem as the most likely issue.
https://www.comptia.org/certifications/network

✗ **C** Incompatible cable
Incorrect. An incompatible fiber type or specification could cause performance or connectivity problems, but it is less likely than reversed TX/RX when the connection is otherwise properly terminated and remains offline.
https://www.comptia.org/certifications/network

✗ **D** CRC errors
Incorrect. CRC errors indicate corrupted frames after a link is operating; they do not normally explain why a fiber connection cannot come online at all.
https://www.comptia.org/certifications/network

Dumpsgate

Question 72

Single choice · Domain: D5 Network troubleshooting › Use ARP to identify a device associated with a duplicate IP address

A network administrator receives a message that a duplicate IP address is on the network. Which of the following commands should the administrator use to locate the node?

A. arp
B. ping
C. ipconfig
D. nslookup

Answer: A. arp

Explanation

This question tests the ability to use network troubleshooting commands to map an IP address to a MAC address and locate the node causing an IP conflict.

✓ **A** arp
Correct. The arp command displays and can modify the local ARP cache, allowing the administrator to identify the MAC address associated with the duplicate IP address and then locate the corresponding node.

https://www.comptia.org/certifications/network

✗ **B** ping
Incorrect. The ping command tests reachability and measures response time, but it does not directly identify the MAC address or physical node using a duplicate IP address.

https://www.comptia.org/certifications/network

✗ **C** ipconfig
Incorrect. The ipconfig command displays and manages local TCP/IP configuration; it does not map a duplicate IP address to the node's MAC address.

https://www.comptia.org/certifications/network

✗ **D** nslookup
Incorrect. The nslookup command queries DNS records and is used for name-resolution troubleshooting, not for locating a device associated with a duplicate IP address.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 73

Single choice · Domain: D5 Network troubleshooting › Use ARP to inspect local IP-to-MAC address resolution when troubleshooting host-specific or intermittent connectivity

A user reports intermittent issues when sending documents to a printer. However, IT support and other users in the office can reach the printer successfully. Which of the following commands should IT support use first to troubleshoot the issue?

A. arp
B. tracert
C. nmap
D. ipconfig

Answer: A. arp

Explanation

The issue affects one user while other devices can reach the printer, suggesting a problem localized to that user's system. The arp command can display the local ARP cache and help identify stale or incorrect IP-to-MAC mappings that may cause intermittent communication.

✓ **A** arp
Correct. The arp command displays the local ARP cache, allowing IT support to check whether the printer's IP address maps to the correct MAC address. A stale or incorrect entry can cause intermittent, host-specific connectivity problems.

https://www.comptia.org/certifications/network

✗ **B** tracert
Incorrect. tracert identifies the Layer 3 path and routing hops to a destination. It is not the best first command for a problem affecting only one user's local communication with a printer.

https://www.comptia.org/certifications/network

✗ **C** nmap
Incorrect. nmap is primarily used for host discovery and port or service scanning. It is unnecessary as the first step when troubleshooting one user's intermittent access to a known printer.

https://www.comptia.org/certifications/network

✗ **D** ipconfig
Incorrect. ipconfig displays or refreshes the host's IP configuration and is useful for general connectivity troubleshooting, but the host-specific intermittent behavior makes checking ARP resolution the more appropriate first step.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 74

Single choice · Domain: D5 Network troubleshooting › Use Nmap to identify operating systems, running services, and available network ports

A systems administrator is looking for operating system information, running services, and network ports that are available on a server. Which of the following software tools should the administrator use to accomplish this task?

A. Nmap
B. Traceroute
C. Netstat
D. Ping

Answer: A. Nmap

Explanation

This question tests the ability to select an appropriate network discovery and scanning tool. Nmap can perform host discovery, operating system detection, service identification, and port scanning, which directly matches the administrator's requirements.

✓ **A** Nmap
Correct. Nmap is a network scanning and discovery tool that can identify operating systems, detect running services, and enumerate open or available network ports.

https://www.comptia.org/certifications/network

✗ **B** Traceroute
Incorrect. Traceroute identifies the path and intermediate hops between a source and destination, but it does not provide comprehensive operating system, service, or port information.

https://www.comptia.org/certifications/network

✗ **C** Netstat
Incorrect. Netstat displays network connections, listening ports, and related local protocol statistics on the system where it is run, but it is not a remote operating system and service discovery scanner like Nmap.

https://www.comptia.org/certifications/network

✗ **D** Ping
Incorrect. Ping tests reachability and measures round-trip response using ICMP; it does not identify operating systems, running services, or available ports.

https://www.comptia.org/certifications/network

Dumpsgate

Question 75

Single choice · Domain: D5 Network troubleshooting › Use wireless analysis tools to identify a specific access point by its BSSID

A network administrator needs to locate a specific AP using a spectrum analyzer to complete an

802.11ax device migration. Which of the following should display on the analyzer to locate the AP?

A. SSID

B. RSSI

C. Channel number

D. BSSID

Answer: D. BSSID

Explanation

This question tests the ability to interpret wireless analyzer data when locating a particular access point during an 802.11ax migration. The BSSID uniquely identifies the AP's wireless interface, whereas the SSID, RSSI, and channel provide network name, signal strength, and radio information.

✗ **A** SSID
Incorrect. The SSID identifies the wireless network name and may be shared by multiple access points, so it does not uniquely identify the specific AP.

https://www.comptia.org/certifications/network

✗ **B** RSSI
Incorrect. RSSI indicates received signal strength; it can help estimate proximity but does not uniquely identify an access point.

https://www.comptia.org/certifications/network

✗ **C** Channel number
Incorrect. The channel number identifies the radio frequency channel in use, but multiple APs can operate on the same channel.

https://www.comptia.org/certifications/network

✓ **D** BSSID
Correct. The BSSID is the unique MAC address identifying a specific wireless access point or its radio interface, making it the appropriate analyzer value for locating that AP.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 76

Single choice · Domain: D5 Network troubleshooting › Apply the CompTIA troubleshooting methodology in the correct sequence

In the troubleshooting methodology, which of the following actions comes after verifying that the initial problem has been resolved?

A. If necessary, escalating the issue
B. Attempting to replicate the problem
C. Documenting findings
D. Implementing the plan

Answer: C. Documenting findings

Explanation

This question tests knowledge of the ordered troubleshooting process, specifically the action that follows verifying full functionality and confirming that the initial problem has been resolved.

✗ **A** If necessary, escalating the issue
Incorrect. Escalation occurs when the issue cannot be resolved at the current support level, not as the standard step immediately after verifying resolution.

https://www.comptia.org/content/docs/default-source/exam-objectives/comptia-network-n10-009-exam-objectives-(1-0

✗ **B** Attempting to replicate the problem
Incorrect. Replicating the problem occurs early in the methodology while identifying and investigating the issue, before implementing and verifying a solution.

https://www.comptia.org/content/docs/default-source/exam-objectives/comptia-network-n10-009-exam-objectives-(1-0

✓ **C** Documenting findings
Correct. After verifying full functionality and confirming that the initial problem has been resolved, the troubleshooting methodology calls for documenting findings, actions, and outcomes.

https://www.comptia.org/content/docs/default-source/exam-objectives/comptia-network-n10-009-exam-objectives-(1-0

✗ **D** Implementing the plan
Incorrect. Implementing the plan occurs before verifying that the solution resolved the initial problem.

https://www.comptia.org/content/docs/default-source/exam-objectives/comptia-network-n10-009-exam-objectives-(1-0

Question 77

Single choice · Domain: D5 Network troubleshooting › Identify the most likely cause of wireless performance degradation from network utilization and topology information

A company upgrades its wireless infrastructure with a 1Gbps backbone, new APs, and new tablets for all employees. However, the IT department notes that speeds are not improved from the previous tablets. Given the following network information, which of the following is the most likely cause of the performance issues?

A. AP 4 has no devices connected.
B. Too many devices are causing congestion.
C. APs do not have the correct VLAN assignment.
D. Switch bandwidth is creating a bottleneck.

Answer: B. Too many devices are causing congestion.

Explanation

This question tests the ability to distinguish wireless congestion from configuration and switching problems when upgraded infrastructure does not improve client throughput.

✗ **A** AP 4 has no devices connected.
Incorrect. An access point with no associated devices would not create congestion or explain reduced performance for clients connected to other access points.
https://www.comptia.org/content/guides/what-is-network-congestion

✓ **B** Too many devices are causing congestion.
Correct. A high number of clients sharing wireless access points and radio resources can cause contention and congestion, so adding a faster backbone does not necessarily improve each tablet's wireless throughput.
https://www.comptia.org/content/guides/what-is-network-congestion

✗ **C** APs do not have the correct VLAN assignment.
Incorrect. An incorrect VLAN assignment would generally cause connectivity, reachability, or access problems rather than preserve throughput at the previous level for otherwise connected clients.
https://www.comptia.org/content/guides/what-is-network-congestion

✗ **D** Switch bandwidth is creating a bottleneck.
Incorrect. The stated 1Gbps backbone reduces the likelihood that the switch uplink is the limiting factor, while the shared wireless medium and client density are more likely to cause the unchanged performance.
https://www.comptia.org/content/guides/what-is-network-congestion

Free demo · full exam: 594 questions

Question 78

Single choice · Domain: D5 Network troubleshooting › Use a tone generator and probe to identify and trace an unknown network cable or switch-port connection

A user reports issues accessing a file server on a LAN with the IP address 192.168.50.140 at a large facility with incomplete infrastructure documentation. The following are the results of the ping command: ping -c 10 192.168.50.140 Packets: Sent = 10, Received = 5, Lost = 5 (50% loss) Round-trip times: Minimum = 3ms, Maximum = 144ms, Average = 42ms Which of the following should a technician do next to continue troubleshooting the issue at the switch with minimal impact?

A. Perform toning and probe.
B. Replace the cable.
C. Visually locate the fault.
D. Restart the switch.

Answer: A. Perform toning and probe.

Explanation

The question tests selecting a minimally disruptive physical-layer troubleshooting method when documentation is incomplete. Intermittent packet loss and variable latency justify tracing the connected cable before replacing equipment or restarting the switch.

✓ **A** Perform toning and probe.
Correct. A tone generator and probe can identify and trace the cable connected to the file server or switch port without interrupting switch operation, making it appropriate for incomplete documentation and minimal impact.

https://www.comptia.org/certifications/network

✗ **B** Replace the cable.
Incorrect. Replacing the cable before identifying or confirming the fault is premature and may disrupt service. Toning and probing is a less intrusive next step for locating the correct cable and connection.

https://www.comptia.org/certifications/network

✗ **C** Visually locate the fault.
Incorrect. A visual inspection may identify obvious physical damage, but it cannot reliably trace an undocumented cable or detect an intermittent fault inside the cabling. A tone generator and probe provide a more targeted next step.

https://www.comptia.org/certifications/network

✗ **D** Restart the switch.
Incorrect. Restarting the switch would affect multiple users and services and is not justified before isolating the fault. It also does not identify the source of the packet loss.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 79

Single choice · Domain: D5 Network troubleshooting › Identify 2.4GHz wireless channel overlap as a source of connectivity and performance problems

A few employees report issues with sessions disconnecting frequently, buffering repeatedly, and performing poorly. Given the following information:

• Employees are in a multitenant office building.

• The Wi-Fi uses 2.4GHz.

• Wireless signals from users range between -50 to -65dBm.

• WPA2 is used.

Which of the following is the most likely cause of the issues?

A. Channel overlap
B. Insufficient wireless coverage
C. AP antenna type
D. Outdated encryption usage

Answer: A. Channel overlap

Explanation

This question tests troubleshooting wireless performance by correlating a multitenant environment and the 2.4GHz band with likely radio-frequency interference. The reported signal levels indicate adequate coverage, so channel overlap is more likely than weak signal, antenna selection, or encryption issues.

✓ **A** Channel overlap
Correct. The 2.4GHz band has relatively few nonoverlapping channels, and nearby wireless networks in a multitenant building can interfere with one another, causing disconnects, buffering, and poor performance.

https://www.comptia.org/certifications/network

✗ **B** Insufficient wireless coverage
Incorrect. Signal levels from -50 to -65 dBm generally indicate usable to strong coverage, so insufficient signal strength is not the most likely cause.

https://www.comptia.org/certifications/network

✗ **C** AP antenna type
Incorrect. No information indicates that the access point antenna type is unsuitable. The shared 2.4GHz environment and multitenant building more directly point to radio-frequency channel overlap.

https://www.comptia.org/certifications/network

✗ **D** Outdated encryption usage
Incorrect. WPA2 is still a valid wireless security protocol and would not normally cause repeated buffering or session disconnects. The symptoms are more consistent with wireless interference.

https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions

Question 80

Single choice · Domain: D5 Network troubleshooting › Use packet captures to analyze network traffic and isolate performance problems

A user reports network performance issues when accessing a specific server. Which of the following should be used to identify the cause of the issue in real time?

A. Port mirroring
B. Syslog reports
C. Baseline metrics
D. Packet capture

Answer: D. Packet capture

Explanation

This question tests the ability to select a real-time troubleshooting tool for examining traffic between a user and a specific server. Packet capture provides detailed visibility into packets, protocols, retransmissions, errors, and latency that can reveal the cause of the performance issue.

✗ **A** Port mirroring
Incorrect. Port mirroring copies traffic from one switch port or VLAN to another monitoring port, but it is primarily a method for making traffic available to an analyzer rather than the analysis itself.
https://www.comptia.org/certifications/network

✗ **B** Syslog reports
Incorrect. Syslog reports provide event and system messages, generally after devices generate them; they do not provide the detailed real-time packet-level visibility needed to identify the cause of a specific server performance problem.
https://www.comptia.org/certifications/network

✗ **C** Baseline metrics
Incorrect. Baseline metrics establish normal performance for comparison and can indicate that a deviation exists, but they do not directly show the packet-level cause of the current issue in real time.
https://www.comptia.org/certifications/network

✓ **D** Packet capture
Correct. A packet capture records and displays network traffic so a technician can inspect communications in real time or shortly afterward for retransmissions, errors, delays, protocol problems, and other causes of degraded access to the server.
https://www.comptia.org/certifications/network

Free demo · full exam: 594 questions