

CompTIA

Exam Questions N10-009

CompTIA Network+ Exam



NEW QUESTION 1

- (Exam Topic 1)

Which of the following TCP ports is used by the Windows OS for file sharing?

- A. 53
- B. 389
- C. 445
- D. 1433

Answer: C

Explanation:

TCP port 445 is used by the Windows OS for file sharing. It is also known as SMB (Server Message Block) or CIFS (Common Internet File System) and allows users to access files, printers, and other shared resources on a network. References:

<https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smb>

NEW QUESTION 2

- (Exam Topic 1)

A technician is installing a high-density wireless network and wants to use an available frequency that supports the maximum number of channels to reduce interference. Which of the following standard 802.11 frequency ranges should the technician look for while reviewing WAP specifications?

- A. 2.4GHz
- B. 5GHz
- C. 6GHz
- D. 900MHz

Answer: B

Explanation:

* 802.11 a/b/g/n/ac wireless networks operate in two frequency ranges: 2.4 GHz and 5 GHz. The 5 GHz frequency range supports more channels than the 2.4 GHz frequency range, making it a better choice for high-density wireless networks.

References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 3

- (Exam Topic 1)

Branch users are experiencing issues with videoconferencing. Which of the following will the company MOST likely configure to improve performance for these applications?

- A. Link Aggregation Control Protocol
- B. Dynamic routing
- C. Quality of service
- D. Network load balancer
- E. Static IP addresses

Answer: C

Explanation:

To improve performance for videoconferencing, the company should configure Quality of Service (QoS). This technology allows for the prioritization of network traffic, ensuring that videoconferencing traffic is given higher priority and therefore better performance. Link Aggregation Control Protocol (LACP), Dynamic routing, Network load balancer, and Static IP addresses are not directly related to improving performance for videoconferencing.

References:

> Network+ N10-007 Certification Exam Objectives, Objective 2.6: Given a scenario, implement and configure the appropriate wireless security and implement the appropriate QoS concepts.

NEW QUESTION 4

- (Exam Topic 1)

An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex. Which of the following is the MOST likely cause of this issue?

- A. The link is improperly terminated
- B. One of the devices is misconfigured
- C. The cable length is excessive
- D. One of the devices has a hardware issue

Answer: C

Explanation:

In a half-duplex link, devices can only send or receive data at one time, not simultaneously. Late collisions occur when devices transmit data at the same time after waiting for a clear channel. One of the causes of late collisions is excessive cable length, which increases the propagation delay and makes it harder for devices to detect collisions. The link termination, device configuration, and device hardware are not likely to cause late collisions on a half-duplex link.

NEW QUESTION 5

- (Exam Topic 1)

At which of the following OSI model layers would a technician find an IP header?

- A. Layer 1

- B. Layer 2
- C. Layer 3
- D. Layer 4

Answer: C

Explanation:

An IP header can be found at the third layer of the OSI model, also known as the network layer. This layer is responsible for logical addressing, routing, and forwarding of data packets.

References:

➤ CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: Network Models, p. 82

NEW QUESTION 6

- (Exam Topic 1)

An attacker is attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt. Which of the following attack types BEST describes this action?

- A. Pass-the-hash attack
- B. Rainbow table attack
- C. Brute-force attack
- D. Dictionary attack

Answer: D

Explanation:

The attacker attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt is using a dictionary attack.

References: CompTIA Network+ Certification Study Guide, Chapter 6: Network Attacks and Mitigation.

NEW QUESTION 7

- (Exam Topic 1)

Which of the following DNS records works as an alias to another record?

- A. AAAA
- B. CNAME
- C. MX
- D. SOA

Answer: B

Explanation:

The DNS record that works as an alias to another record is called CNAME (Canonical Name). CNAME records are used to create an alias for a domain name that points to another domain name.

References:

➤ CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.3: Given a scenario, implement and configure the appropriate addressing schema.

NEW QUESTION 8

- (Exam Topic 1)

A workstation is configured with the following network details:

IP address	Subnet mask	Default gateway
10.1.2.23	10.1.2.0/27	10.1.2.1

Software on the workstation needs to send a query to the local subnet broadcast address. To which of the following addresses should the software be configured to send the query?

- A. 10.1.2.0
- B. 10.1.2.1
- C. 10.1.2.23
- D. 10.1.2.255
- E. 10.1.2.31

Answer: D

Explanation:

The software on the workstation should be configured to send the query to 10.1.2.255, which is the local subnet broadcast address. A broadcast address is a special address that allows a device to send a message to all devices on the same subnet. It is usually derived by setting all the host bits to 1 in the network address. In this case, the network address is 10.1.2.0/27, which has 27 network bits and 5 host bits. By setting all the host bits to 1, we get 10.1.2.31 as the broadcast address in decimal notation, or 10.1.2.255 in dotted decimal notation. References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION 9

- (Exam Topic 1)

A technician is connecting multiple switches to create a large network for a new office. The switches are unmanaged Layer 2 switches with multiple connections between each pair. The network is experiencing an extreme amount of latency. Which of the following is MOST likely occurring?

- A. Ethernet collisions
- B. A DDoS attack

- C. A broadcast storm
- D. Routing loops

Answer: C

Explanation:

A broadcast storm is most likely occurring when connecting multiple unmanaged Layer 2 switches with multiple connections between each pair. A broadcast storm is a situation where broadcast packets flood a network segment and consume all the available bandwidth. It can be caused by loops in the network topology, where broadcast packets are endlessly forwarded by switches without any loop prevention mechanism. Unmanaged switches do not support features such as Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) that can detect and block loops. References: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10556-16.html>

NEW QUESTION 10

- (Exam Topic 1)

A technician is installing multiple UPS units in a major retail store. The technician is required to keep track of all changes to new and old equipment. Which of the following will allow the technician to record these changes?

- A. Asset tags
- B. A smart locker
- C. An access control vestibule
- D. A camera

Answer: A

Explanation:

Asset tags will allow the technician to record changes to new and old equipment when installing multiple UPS units in a major retail store. Asset tags are labels or stickers that are attached to physical assets such as computers, printers, servers, or UPS units. They usually contain information such as asset name, serial number, barcode, QR code, or RFID chip that can be scanned or read by an asset management system or software. Asset tags help track inventory, location, status, maintenance, and ownership of assets. References: <https://www.camcode.com/asset-tags/asset-tagging-guide/>

NEW QUESTION 10

- (Exam Topic 1)

The management team needs to ensure unnecessary modifications to the corporate network are not permitted and version control is maintained. Which of the following documents would BEST support this?

- A. An incident response plan
- B. A business continuity plan
- C. A change management policy
- D. An acceptable use policy

Answer: C

Explanation:

A change management policy is a document that outlines the procedures and guidelines for making changes to a network or system, including how changes are approved, tested, and implemented. By following a change management policy, organizations can ensure that unnecessary modifications to the network are not permitted and version control is maintained. References:

➤ Network+ N10-008 Objectives: 1.6 Given a scenario, implement network configuration and change management best practices.

NEW QUESTION 11

- (Exam Topic 1)

A technician is troubleshooting a wireless connectivity issue in a small office located in a high-rise building. Several APs are mounted in this office. The users report that the network connections frequently disconnect and reconnect throughout the day. Which of the following is the MOST likely cause of this issue?

- A. The AP association time is set too low
- B. EIRP needs to be boosted
- C. Channel overlap is occurring
- D. The RSSI is misreported

Answer: C

Explanation:

Channel overlap is a common cause of wireless connectivity issues, especially in high-density environments where multiple APs are operating on the same or adjacent frequencies. Channel overlap can cause interference, signal degradation, and performance loss for wireless devices. The AP association time, EIRP, and RSSI are not likely to cause frequent disconnects and reconnects for wireless users.

NEW QUESTION 13

- (Exam Topic 1)

A network engineer performs the following tasks to increase server bandwidth: Connects two network cables from the server to a switch stack
Configure LACP on the switchports
Verifies the correct configurations on the switch interfaces Which of the following needs to be configured on the server?

- A. Load balancing
- B. Multipathing
- C. NIC teaming
- D. Clustering

Answer: C

Explanation:

NIC teaming is a technique that combines two or more network interface cards (NICs) on a server into a single logical interface that can increase bandwidth, provide redundancy, and balance traffic. NIC teaming can be configured with different modes and algorithms depending on the desired outcome. Link Aggregation Control Protocol (LACP) is a protocol that enables NIC teaming by dynamically bundling multiple links between two devices into one logical link. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming/nic-teaming>

NEW QUESTION 17

- (Exam Topic 1)

Given the following information:

Protocol	Local address	Foreign address	State
TCP	127.0.0.1:57779	Desktop-Open:57780	Established
TCP	127.0.0.1:57780	Desktop-Open:57779	Established

Which of the following command-line tools would generate this output?

- A. netstat
- B. arp
- C. dig
- D. tracert

Answer: D

Explanation:

Tracert is a command-line tool that traces the route of a packet from a source to a destination and displays the number of hops and the round-trip time for each hop. The output shown in the question is an example of a tracert output, which shows five hops with their IP addresses and hostnames (if available) and three latency measurements for each hop in milliseconds. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.lumen.com/help/en-us/network/traceroute/understanding-the-traceroute-output.html>

NEW QUESTION 19

- (Exam Topic 1)

A network administrator is configuring a load balancer for two systems. Which of the following must the administrator configure to ensure connectivity during a failover?

- A. VIP
- B. NAT
- C. APIPA
- D. IPv6 tunneling
- E. Broadcast IP

Answer: A

Explanation:

A virtual IP (VIP) address must be configured to ensure connectivity during a failover. A VIP address is a single IP address that is assigned to a group of servers or network devices. When one device fails, traffic is automatically rerouted to the remaining devices, and the VIP address is reassigned to the backup device, allowing clients to continue to access the service without interruption.

References:

➤ CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 6: Network Servers, p. 300

NEW QUESTION 21

- (Exam Topic 1)

Which of the following can be used to centrally manage credentials for various types of administrative privileges on configured network devices?

- A. SSO
- B. TACACS+
- C. Zero Trust
- D. Separation of duties
- E. Multifactor authentication

Answer: B

Explanation:

TACACS+ (Terminal Access Controller Access Control System Plus) can be used to centrally manage credentials for various types of administrative privileges on configured network devices. This protocol separates authentication, authorization, and accounting (AAA) functions, providing more granular control over access to network resources.

References:

➤ Network+ N10-007 Certification Exam Objectives, Objective 4.2: Given a scenario, implement secure network administration principles.

NEW QUESTION 24

- (Exam Topic 1)

Which of the following is used to track and document various types of known vulnerabilities?

- A. CVE
- B. Penetration testing
- C. Zero-day
- D. SIEM

E. Least privilege

Answer: A

Explanation:

CVE stands for Common Vulnerabilities and Exposures, which is a list of publicly disclosed cybersecurity vulnerabilities that is free to search, use, and incorporate into products and services. CVE provides a standardized identifier and description for each vulnerability, as well as references to related sources of information. CVE helps to track and document various types of known vulnerabilities and facilitates communication and coordination among security professionals. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://cve.mitre.org/cve/>

NEW QUESTION 25

- (Exam Topic 1)

A network administrator is implementing OSPF on all of a company's network devices. Which of the following will MOST likely replace all the company's hubs?

- A. A Layer 3 switch
- B. A proxy server
- C. A NGFW
- D. A WLAN controller

Answer: A

Explanation:

A Layer 3 switch will likely replace all the company's hubs when implementing OSPF on all of its network devices. A Layer 3 switch combines the functionality of a traditional Layer 2 switch with the routing capabilities of a router. By implementing OSPF on a Layer 3 switch, an organization can improve network performance and reduce the risk of network congestion. References: Network+ Certification Study Guide, Chapter 5: Network Security

NEW QUESTION 27

- (Exam Topic 1)

Which of the following transceiver types can support up to 40Gbps?

- A. SFP+
- B. QSFP+
- C. QSFP
- D. SFP

Answer: B

Explanation:

QSFP+ is a transceiver type that can support up to 40Gbps. It stands for Quad Small Form-factor Pluggable Plus and uses four lanes of data to achieve high-speed transmission. It is commonly used for data center and high-performance computing applications. References: https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-6600

NEW QUESTION 30

- (Exam Topic 1)

A technician is installing a cable modem in a SOHO. Which of the following cable types will the technician MOST likely use to connect a modem to the ISP?

- A. Coaxial
- B. Single-mode fiber
- C. Cat 6e
- D. Multimode fiber

Answer: A

Explanation:

Coaxial cable is a type of cable that consists of a central copper conductor surrounded by an insulating layer and a braided metal shield. Coaxial cable is commonly used to connect a cable modem to an ISP by transmitting data over cable television networks. Coaxial cable can support high bandwidth and long distances with minimal interference or attenuation. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.techopedia.com/definition/4027/coaxial-cable>

NEW QUESTION 34

- (Exam Topic 1)

A new cabling certification is being requested every time a network technician rebuilds one end of a Cat 6 (vendor-certified) cable to create a crossover connection that is used to connect switches. Which of the following would address this issue by allowing the use of the original cable?

- A. CSMA/CD
- B. LACP
- C. PoE+
- D. MDIX

Answer: D

Explanation:

MDIX (medium-dependent interface crossover) is a feature that allows network devices to automatically detect and configure the appropriate cabling type, eliminating the need for crossover cables. By enabling MDIX on the switches, a technician can use the original Cat 6 cable to create a crossover connection. References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 38

- (Exam Topic 1)

According to troubleshooting methodology, which of the following should the technician do NEXT after determining the most likely probable cause of an issue?

- A. Establish a plan of action to resolve the issue and identify potential effects
- B. Verify full system functionality and, if applicable, implement preventive measures
- C. Implement the solution or escalate as necessary
- D. Test the theory to determine the cause

Answer: A

Explanation:

According to troubleshooting methodology, after determining the most likely probable cause of an issue, the next step is to establish a plan of action to resolve the issue and identify potential effects. This step involves defining the steps needed to implement a solution, considering the possible consequences of each step, and obtaining approval from relevant stakeholders if necessary. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.comptia.org/blog/the-comptia-guide-to-it-troubleshooting>

NEW QUESTION 41

- (Exam Topic 1)

A technician is deploying a new switch model and would like to add it to the existing network monitoring software. The technician wants to know what metrics can be gathered from a given switch. Which of the following should the technician utilize for the switch?

- A. MIB
- B. Trap
- C. Syslog
- D. Audit log

Answer: A

Explanation:

To determine what metrics can be gathered from a given switch, a technician should utilize the Management Information Base (MIB). The MIB is a database of network management information that is used to manage and monitor network devices. It contains information about device configuration, status, and performance. References: Network+ Certification Study Guide, Chapter 5: Network Security

NEW QUESTION 42

- (Exam Topic 1)

A technician receives feedback that some users are experiencing high amounts of jitter while using the wireless network. While troubleshooting the network, the technician uses the ping command with the IP address of the default gateway and verifies large variations in latency. The technician thinks the issue may be interference from other networks and non-802.11 devices. Which of the following tools should the technician use to troubleshoot the issue?

- A. NetFlow analyzer
- B. Bandwidth analyzer
- C. Protocol analyzer
- D. Spectrum analyzer

Answer: D

Explanation:

A spectrum analyzer is a tool that measures the frequency and amplitude of signals in a wireless network. It can be used to troubleshoot issues related to interference from other networks and non-802.11 devices, such as microwave ovens or cordless phones, by identifying the sources and levels of interference in the wireless spectrum. A spectrum analyzer can also help to optimize the channel selection and placement of wireless access points. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.flukenetworks.com/blog/cabling-chronicles/what-spectrum-analyzer-and-how-do-you-use-it>

NEW QUESTION 43

- (Exam Topic 1)

Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

- A. Scope options
- B. Reservation
- C. Dynamic assignment
- D. Exclusion
- E. Static assignment

Answer: B

Explanation:

A reservation should be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP. A reservation is a feature of DHCP that allows an administrator to assign a fixed IP address to a device based on its MAC address. This way, the device will always receive the same IP address from the DHCP server, even if it is powered off or disconnected from the network for a long time. References: <https://docs.microsoft.com/en-us/windows-server/troubleshoot/configure-dhcp-reservations>

NEW QUESTION 44

- (Exam Topic 1)

A network administrator is designing a new datacenter in a different region that will need to communicate to the old datacenter with a secure connection. Which of the following access methods would provide the BEST security for this new datacenter?

- A. Virtual network computing
- B. Secure Socket Shell

- C. In-band connection
- D. Site-to-site VPN

Answer: D

Explanation:

Site-to-site VPN provides the best security for connecting a new datacenter to an old one because it creates a secure tunnel between the two locations, protecting data in transit. References: CompTIA Network+ Certification Study Guide, Chapter 5: Network Security.

NEW QUESTION 49

- (Exam Topic 1)

A network technician is reviewing the interface counters on a router interface. The technician is attempting to confirm a cabling issue. Given the following information:

Metric	Value
Last cleared	7 minutes, 34 seconds
# of packets output	6915
# of packets input	270
CRCs	183
Giants	0
Runts	0
Multicasts	14

Which of the following metrics confirms there is a cabling issue?

- A. Last cleared
- B. Number of packets output
- C. CRCs
- D. Giants
- E. Multicasts

Answer: C

Explanation:

CRC stands for Cyclic Redundancy Check, and it is a type of error-detecting code used to detect accidental changes to raw data. If the CRC count is increasing on a particular interface, it indicates that there might be an issue with the cabling, which is causing data corruption. References:

> Network+ N10-008 Objectives: 2.1 Given a scenario, troubleshoot common physical connectivity issues.

NEW QUESTION 53

- (Exam Topic 1)

The network administrator is informed that a user's email password is frequently hacked by brute-force programs. Which of the following policies should the network administrator implement to BEST mitigate this issue? (Choose two.)

- A. Captive portal
- B. Two-factor authentication
- C. Complex passwords
- D. Geofencing
- E. Role-based access
- F. Explicit deny

Answer: BC

Explanation:

Two-factor authentication (2FA) is a method of verifying a user's identity by requiring two pieces of evidence, such as something the user knows (e.g., a password) and something the user has (e.g., a token or a smartphone). 2FA adds an extra layer of security that makes it harder for hackers to access a user's account by brute-force programs. Complex passwords are passwords that are long, random, and use a combination of uppercase and lowercase letters, numbers, and symbols. Complex passwords are more resistant to brute-force attacks than simple or common passwords. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.csoonline.com/article/3225913/what-is-two-factor-authentication-2fa-how-to-enable-it-and-why-yo> <https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/>

NEW QUESTION 55

- (Exam Topic 1)

Which of the following provides redundancy on a file server to ensure the server is still connected to a LAN even in the event of a port failure on a switch?

- A. NIC teaming
- B. Load balancer
- C. RAID array
- D. PDUs

Answer: A

Explanation:

NIC teaming, also known as network interface card teaming or link aggregation, allows multiple network interface cards to be grouped together to provide redundancy and increased throughput. In the event of a port failure on a switch, NIC teaming ensures that the file server remains connected to the LAN by automatically switching to another network interface card.

References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 58

- (Exam Topic 1)

SIMULATION

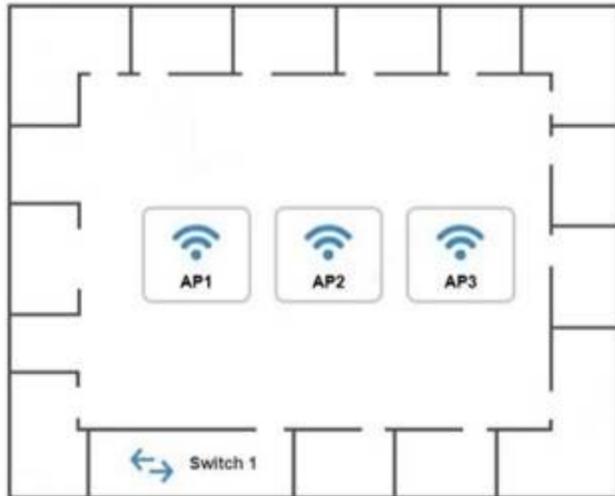
You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

The SSIDs need to be configured as CorpNet with a key of S3cr3t! The wireless signals should not interfere with each other

The subnet the Access Points and switch are on should only support 30 devices maximum The Access Points should be configured to only support TKIP clients at a maximum speed INSTRUCTIONS

Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



192.168.1.2
 Speed: Auto
 Duplex: Auto

AP1 Configuration

Basic Configuration

Access Point Name:

IP Address:

Gateway:

SSID:

SSID Broadcast: Yes No

Wireless

Mode:

Channel:

Wired

Speed: Auto 100 1000

Duplex: Auto Half Full

Security Configuration

Security Settings: None WEP WPA WPA2 WPA2 - Enterprise

Key or Passphrase:

Reset to Default
Save
Close

AP2 Configuration

https://ap2.setup.do

Basic Configuration

Access Point Name: AP2

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast: Yes No

Wireless

Mode:
 B
 G

Channel:
 1
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11

Wired

Speed: Auto 100 1000

Duplex: Auto Half Full

Security Configuration

Security Settings: None WEP WPA WPA2 WPA2 - Enterprise

Key or Passphrase:

Reset to Default Save Close

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name: AP3

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast: Yes No

Wireless

Mode:
 B
 G

Channel:
 1
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11

Wired

Speed: Auto 100 1000

Duplex: Auto Half Full

Security Configuration

Security Settings: None WEP WPA WPA2 WPA2 - Enterprise

Key or Passphrase:

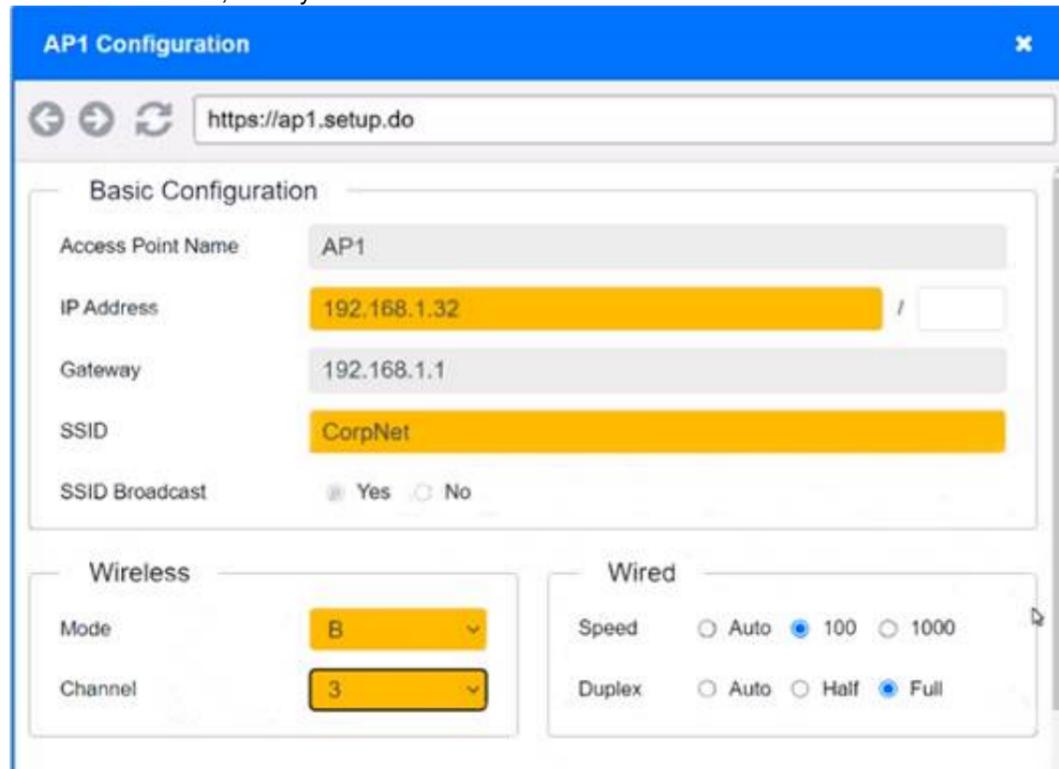
Reset to Default Save Close

- A. Mastered
- B. Not Mastered

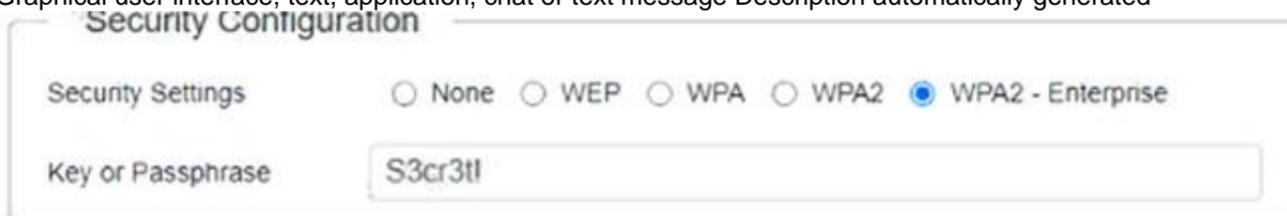
Answer: A

Explanation:

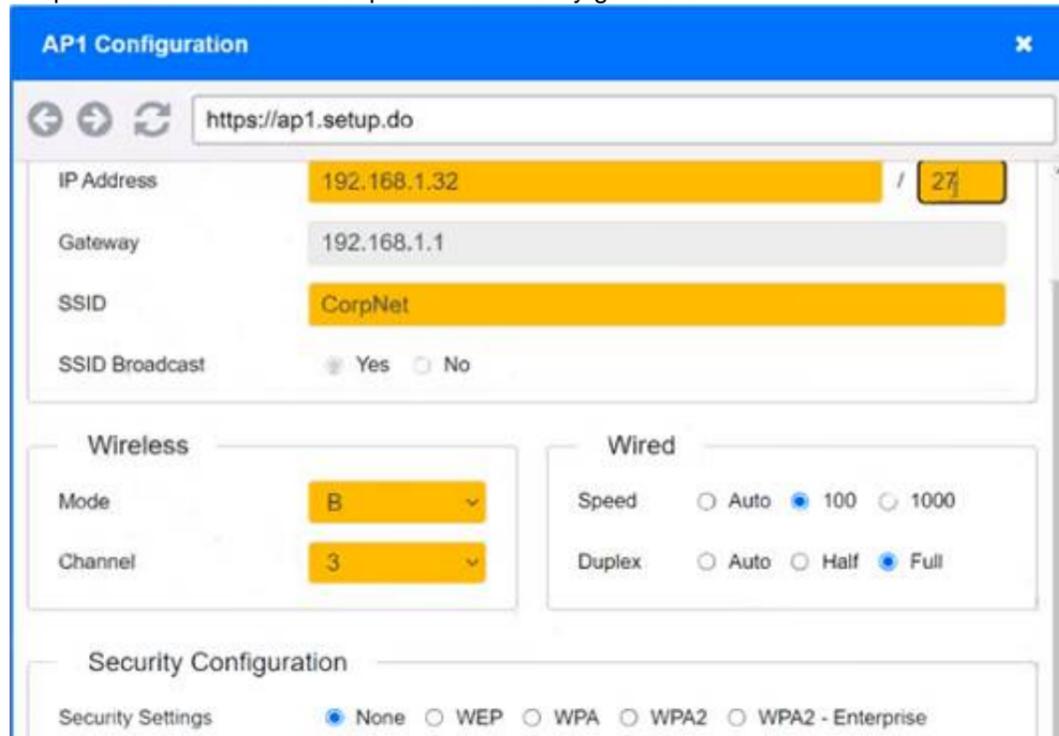
On the first exhibit, the layout should be as follows



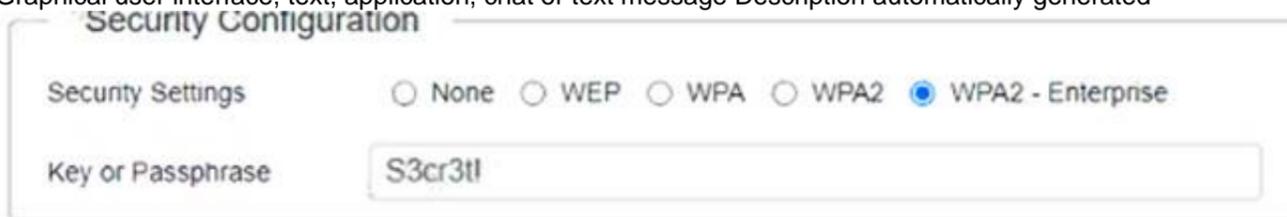
Graphical user interface, text, application, chat or text message Description automatically generated



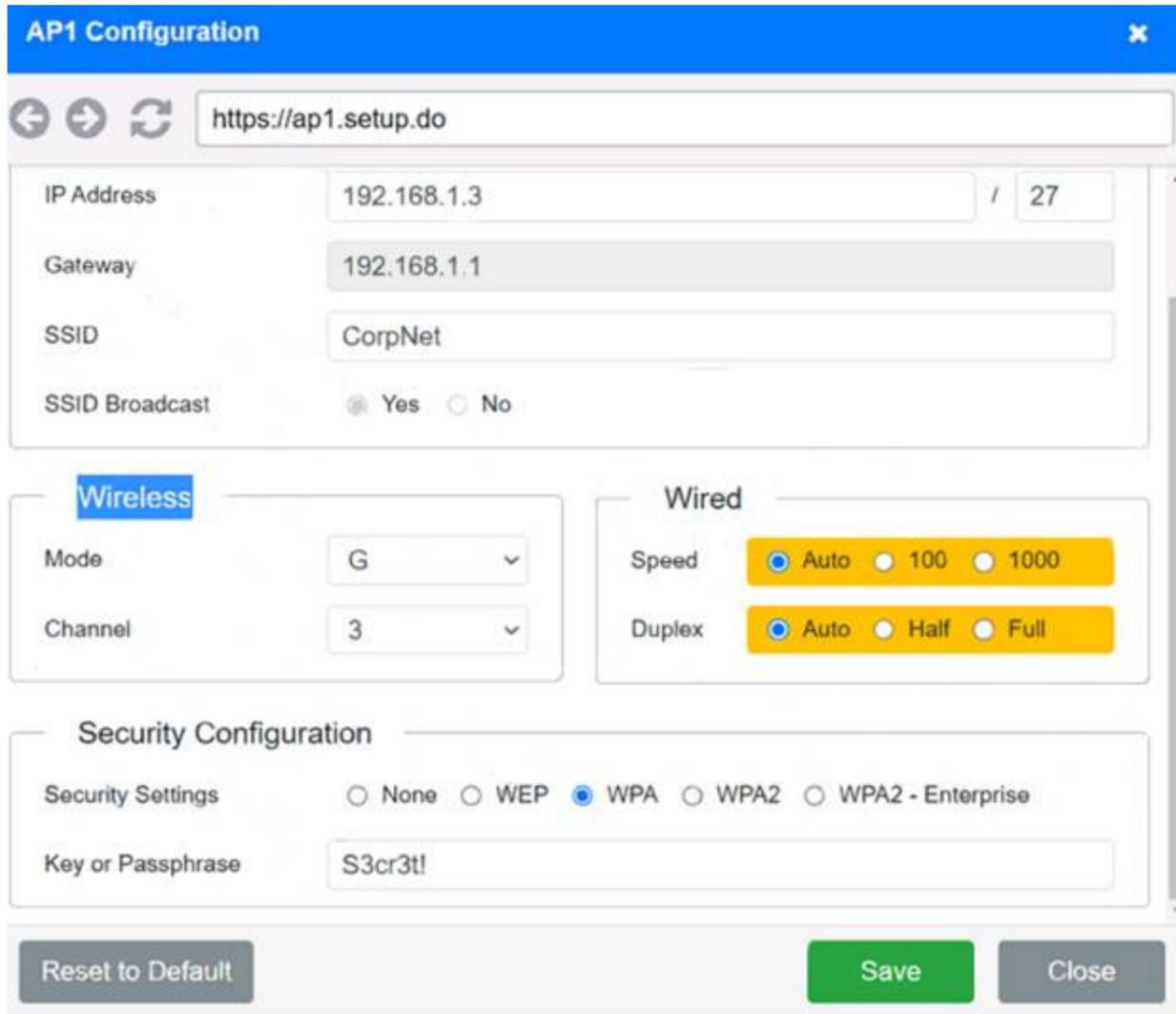
Graphical user interface Description automatically generated



Graphical user interface, text, application, chat or text message Description automatically generated

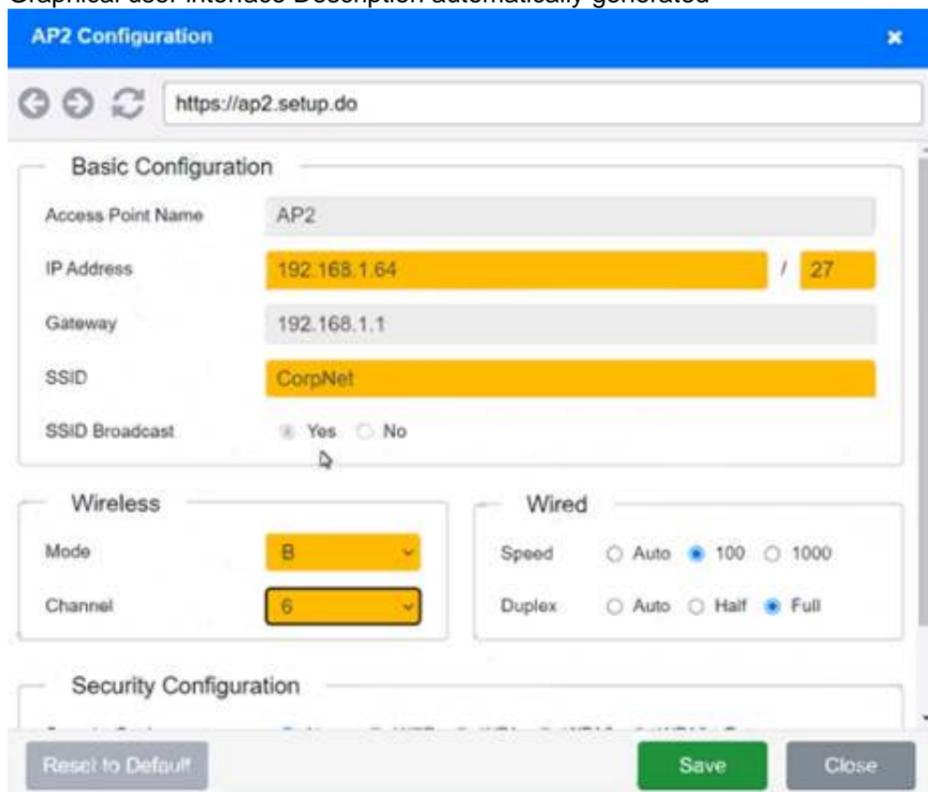


Graphical user interface Description automatically generated



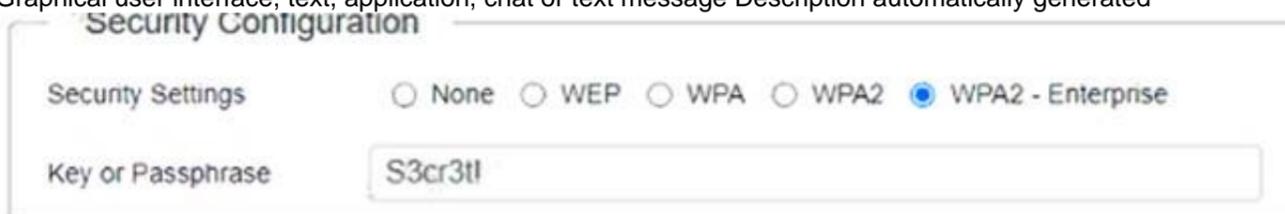
The screenshot shows the 'AP1 Configuration' web interface. At the top, there is a blue header with the title and a close button. Below the header is a navigation bar with back, forward, and refresh icons, and a URL field containing 'https://ap1.setup.do'. The main configuration area is divided into several sections: 'Basic Configuration' with fields for IP Address (192.168.1.3), Gateway (192.168.1.1), SSID (CorpNet), and SSID Broadcast (Yes); 'Wireless' section with Mode (G) and Channel (3); 'Wired' section with Speed (Auto) and Duplex (Auto); and 'Security Configuration' with Security Settings (WPA) and Key or Passphrase (S3cr3t!). At the bottom, there are three buttons: 'Reset to Default', 'Save', and 'Close'.

Exhibit 2 as follows Access Point Name AP2
Graphical user interface Description automatically generated



The screenshot shows the 'AP2 Configuration' web interface. It has a similar layout to AP1. The 'Basic Configuration' section shows Access Point Name (AP2), IP Address (192.168.1.64), Gateway (192.168.1.1), and SSID (CorpNet). The 'Wireless' section shows Mode (B) and Channel (6). The 'Wired' section shows Speed (100) and Duplex (Full). The 'Security Configuration' section is partially visible at the bottom. Buttons for 'Reset to Default', 'Save', and 'Close' are at the bottom.

Graphical user interface, text, application, chat or text message Description automatically generated



This is a close-up of the 'Security Configuration' section from the AP2 configuration page. It shows 'Security Settings' with radio buttons for None, WEP, WPA, WPA2, and WPA2 - Enterprise (which is selected). Below it is a text field for 'Key or Passphrase' containing 'S3cr3t!'.

Graphical user interface Description automatically generated

The screenshot shows the 'AP2 Configuration' web interface. At the top, there is a navigation bar with a title and a close button. Below it is a browser address bar showing 'https://ap2.setup.do'. The main configuration area is divided into several sections: 'Basic Configuration' with fields for IP Address (192.168.1.4), Gateway (192.168.1.1), SSID (CorpNet), and SSID Broadcast (Yes); 'Wireless' section with Mode (G) and Channel (6); 'Wired' section with Speed (Auto) and Duplex (Auto); and 'Security Configuration' with Security Settings (WPA) and Key or Passphrase (S3cr3t!). At the bottom, there are three buttons: 'Reset to Default', 'Save', and 'Close'.

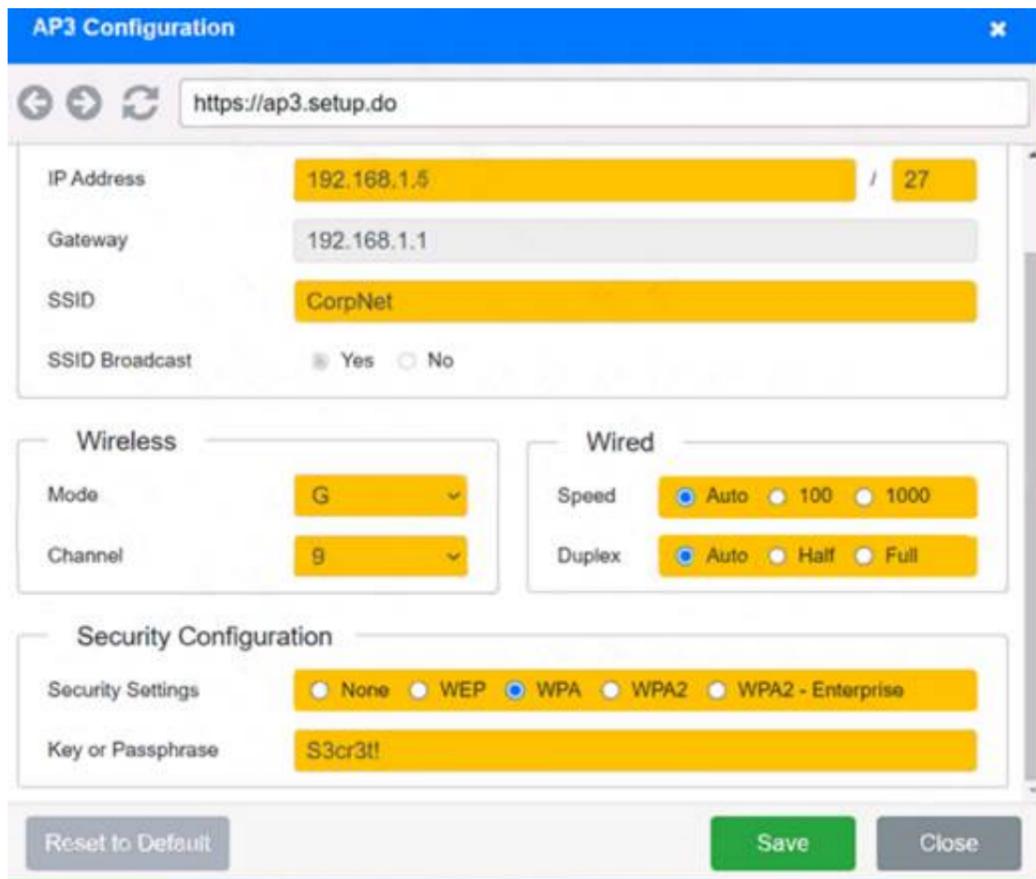
Exhibit 3 as follows Access Point Name AP3
Graphical user interface Description automatically generated

The screenshot shows the 'AP3 Configuration' web interface. It has a similar layout to AP2 but with different settings. The 'Basic Configuration' section shows Access Point Name (AP3), IP Address (192.168.1.96), Gateway (192.168.1.1), and SSID (CorpNet). The 'Wireless' section shows Mode (B) and Channel (9). The 'Wired' section shows Speed (100) and Duplex (Full). The 'Security Configuration' section is partially visible at the bottom. Buttons for 'Reset to Default', 'Save', and 'Close' are at the bottom.

Graphical user interface, text, application, chat or text message Description automatically generated

This is a close-up of the 'Security Configuration' section from the AP3 interface. It shows 'Security Settings' with radio buttons for None, WEP, WPA, WPA2, and WPA2 - Enterprise (which is selected). Below it is a text input field for 'Key or Passphrase' containing the text 'S3cr3t!'.

Graphical user interface Description automatically generated



The screenshot shows the AP3 Configuration web interface. At the top, there is a browser address bar with the URL 'https://ap3.setup.do'. Below the address bar, there are several configuration fields:

- IP Address:** 192.168.1.5 / 27
- Gateway:** 192.168.1.1
- SSID:** CorpNet
- SSID Broadcast:** Yes (selected), No

Below these fields, there are two sections: **Wireless** and **Wired**.

- Wireless:** Mode is set to G, Channel is set to 9.
- Wired:** Speed is set to Auto, Duplex is set to Auto.

At the bottom, there is a **Security Configuration** section:

- Security Settings:** WPA (selected), None, WEP, WPA2, WPA2 - Enterprise.
- Key or Passphrase:** S3cr3t!

At the very bottom, there are three buttons: 'Reset to Default', 'Save', and 'Close'.

NEW QUESTION 63

- (Exam Topic 1)

Which of the following routing protocols is used to exchange route information between public autonomous systems?

- A. OSPF
- B. BGP
- C. EGRIP
- D. RIP

Answer: B

Explanation:

BGP (Border Gateway Protocol) is a routing protocol used to exchange route information between public autonomous systems (AS). OSPF (Open Shortest Path First), EGRIP (Enhanced Interior Gateway Routing Protocol), and RIP (Routing Information Protocol) are all used for internal routing within a single AS. Therefore, BGP is the correct option to choose for this question.

References:

- > Network+ N10-007 Certification Exam Objectives, Objective 3.3: Given a scenario, configure and apply the appropriate routing protocol.
- > Cisco: Border Gateway Protocol (BGP) Overview

NEW QUESTION 65

- (Exam Topic 1)

A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

- A. OTDR
- B. Tone generator
- C. Fusion splicer
- D. Cable tester
- E. PoE injector

Answer: A

Explanation:

To detect the exact break point of a fiber link, an engineer should use an OTDR (Optical Time Domain Reflectometer). This device sends a series of pulses into the fiber, measuring the time it takes for the pulses to reflect back, and can pinpoint the exact location of the break.

References:

- > Network+ N10-007 Certification Exam Objectives, Objective 2.5: Given a scenario, troubleshoot copper cable issues.
- > FS: OTDR (Optical Time Domain Reflectometer) Testing Principle and Applications

NEW QUESTION 69

- (Exam Topic 1)

An IT organization needs to optimize speeds for global content distribution and wants to reduce latency in high-density user locations. Which of the following technologies BEST meets the organization's requirements?

- A. Load balancing
- B. Geofencing
- C. Public cloud
- D. Content delivery network
- E. Infrastructure as a service

Answer: D

Explanation:

A content delivery network (CDN) is a distributed network of servers that delivers web content to users based on their geographic location. By replicating content across multiple servers in various locations, a CDN can optimize speed and reduce latency in high-density user locations.

NEW QUESTION 74

- (Exam Topic 1)

Client devices cannot enter a network, and the network administrator determines the DHCP scope is exhausted. The administrator wants to avoid creating a new DHCP pool. Which of the following can the administrator perform to resolve the issue?

- A. Install load balancers
- B. Install more switches
- C. Decrease the number of VLANs
- D. Reduce the lease time

Answer: D

Explanation:

To resolve the issue of DHCP scope exhaustion without creating a new DHCP pool, the administrator can reduce the lease time. By decreasing the lease time, the IP addresses assigned by DHCP will be released back to the DHCP scope more quickly, allowing them to be assigned to new devices.

References:

- > CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.3: Given a scenario, implement and configure the appropriate addressing schema.
- > <https://www.networkcomputing.com/data-centers/10-tips-optimizing-dhcp-performance>

NEW QUESTION 76

- (Exam Topic 1)

A technician is assisting a user who cannot connect to a network resource. The technician first checks for a link light. According to troubleshooting methodology, this is an example of:

- A. using a bottom-to-top approach.
- B. establishing a plan of action.
- C. documenting a finding.
- D. questioning the obvious.

Answer: A

Explanation:

Using a bottom-to-top approach means starting from the physical layer and moving up the OSI model to troubleshoot a network problem. Checking for a link light is a physical layer check that verifies the connectivity of the network cable and device. References:

<https://www.professormesser.com/network-plus/n10-007/troubleshooting-methodologies-2/>

NEW QUESTION 81

- (Exam Topic 1)

A systems administrator needs to improve WiFi performance in a densely populated office tower and use the latest standard. There is a mix of devices that use 2.4 GHz and 5 GHz. Which of the following should the systems administrator select to meet this requirement?

- A. 802.11ac
- B. 802.11ax
- C. 802.11g
- D. 802.11n

Answer: B

Explanation:

* 802.11 ax is the latest WiFi standard that improves WiFi performance in densely populated environments and supports both 2.4 GHz and 5 GHz bands. 802.11ac is the previous standard that only supports 5 GHz band. 802.11g and 802.11n are older standards that support 2.4 GHz band only or both bands respectively.

References:

- [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),
- <https://www.techtarget.com/searchnetworking/tip/Whats-the-difference-between-80211ax-vs-80211ac>

NEW QUESTION 85

- (Exam Topic 1)

Which of the following BEST describes a network appliance that warns of unapproved devices that are accessing the network?

- A. Firewall
- B. AP
- C. Proxy server
- D. IDS

Answer: D

Explanation:

IDS stands for intrusion detection system, which is a network appliance that monitors network traffic and alerts administrators of any suspicious or malicious activity. An IDS can warn of unapproved devices that are accessing the network by detecting anomalies, signatures, or behaviors that indicate unauthorized access attempts or attacks. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.cisco.com/c/en/us/products/security/what-is-an-intrusion-detection-system-ids.html>

NEW QUESTION 89

- (Exam Topic 1)

A branch of a company recently switched to a new ISP. The network engineer was given a new IP range to assign. The ISP assigned 196.26.4.0/26, and the branch gateway router now has the following configurations on the interface that peers to the ISP:

```
IP address:      196.26.4.30
Subnet mask:     255.255.255.224
Gateway:        196.24.4.1
```

The network engineer observes that all users have lost Internet connectivity. Which of the following describes the issue?

- A. The incorrect subnet mask was configured
- B. The incorrect gateway was configured
- C. The incorrect IP address was configured
- D. The incorrect interface was configured

Answer: C

Explanation:

The IP address configured on the router interface is 196.26.4.1/26, which belongs to the IP range assigned by the ISP (196.26.4.0/26). However, this IP address is not valid for this interface because it is the network address of the subnet, which cannot be assigned to any host device. The network address is the first address of a subnet that identifies the subnet itself. The valid IP addresses for this subnet are from 196.26.4.1 to 196.26.4.62, excluding the network address (196.26.4.0) and the broadcast address (196.26.4.63). The router interface should be configured with a valid IP address within this range to restore Internet connectivity for all users. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.techopedia.com/definition/24136/network-address>

NEW QUESTION 92

- (Exam Topic 1)

Which of the following systems would MOST likely be found in a screened subnet?

- A. RADIUS
- B. FTP
- C. SQL
- D. LDAP

Answer: B

Explanation:

FTP (File Transfer Protocol) is a system that would most likely be found in a screened subnet. A screened subnet, or triple-homed firewall, is a network architecture where a single firewall is used with three network interfaces. It provides additional protection from outside cyber attacks by adding a perimeter network to

isolate or separate the internal network from the public-facing internet. A screened subnet typically hosts systems that need to be accessed by both internal and external users, such as web servers, email servers, or FTP servers. References:

[https://www.techtarget.com/searchsecurity/definition/screened-subnet#:~:text=A%20screened%20subnet%2C%](https://www.techtarget.com/searchsecurity/definition/screened-subnet#:~:text=A%20screened%20subnet%2C%20)

1

NEW QUESTION 97

- (Exam Topic 1)

A network technician needs to ensure outside users are unable to telnet into any of the servers at the datacenter. Which of the following ports should be blocked when checking firewall configuration?

- A. 22
- B. 23
- C. 80
- D. 3389
- E. 8080

Answer: B

Explanation:

Port 23 should be blocked when checking firewall configuration to prevent outside users from telnetting into any of the servers at the datacenter. Port 23 is the default port for Telnet, which is an insecure protocol that allows remote access to servers and network devices. Telnet sends data in clear text, which can be easily intercepted and compromised by attackers. A more secure alternative is SSH, which uses port 22 and encrypts data. References:

<https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION 101

- (Exam Topic 1)

A network administrator needs to query the NSs for a remote application. Which of the following commands would BEST help the administrator accomplish this task?

- A. dig
- B. arp
- C. show interface
- D. hostname

Answer: A

Explanation:

The dig command is used to query the NSs for a remote application. It is a command-line tool that is commonly used to troubleshoot DNS issues. When used with specific options, dig can be used to obtain information about domain names, IP addresses, and DNS records. References: Network+ Certification Study Guide, Chapter 3: Network Infrastructure

NEW QUESTION 102

- (Exam Topic 2)

A network technician needs to correlate security events to analyze a suspected intrusion. Which of the following should the technician use?

- A. SNMP
- B. Log review
- C. Vulnerability scanning
- D. SIEM

Answer: D

Explanation:

SIEM stands for Security Information and Event Management, which is a tool that collects, analyzes, and correlates data from various network devices and sources to provide alerts and reports on security incidents and events. A network technician can use SIEM to correlate security events to analyze a suspected intrusion, as SIEM can help identify the source, target, method, and impact of an attack, as well as provide recommendations for remediation. References: <https://www.comptia.org/blog/what-is-siem>

NEW QUESTION 104

- (Exam Topic 2)

A business is using the local cable company to provide Internet access. Which of the following types of cabling will the cable company MOST likely use from the demarcation point back to the central office?

- A. Multimode
- B. Cat 5e
- C. RG-6
- D. Cat 6
- E. 100BASE-T

Answer: C

Explanation:

RG-6 is a type of coaxial cable that is commonly used by cable companies to provide Internet access from the demarcation point back to the central office. It has a thicker conductor and better shielding than RG-59, which is another type of coaxial cable. Multimode and Cat 5e are types of fiber optic and twisted pair cables respectively, which are not typically used by cable companies. Cat 6 and 100BASE-T are standards for twisted pair cables, not types of cabling.

NEW QUESTION 108

- (Exam Topic 2)

A network technician was troubleshooting an issue for a user who was being directed to cloned websites that were stealing credentials. The URLs were correct for the websites but an incorrect IP address was revealed when the technician used ping on the user's PC. After checking the DNS settings, the technician found the DNS server address was incorrect. Which of the following describes the issue?

- A. Rogue DHCP server
- B. Misconfigured HSRP
- C. DNS poisoning
- D. Exhausted IP scope

Answer: C

Explanation:

DNS poisoning is a type of attack that modifies the DNS records of a domain name to point to a malicious IP address instead of the legitimate one. This can result in users being directed to cloned websites that are stealing credentials, even if they enter the correct URL for the website. The incorrect DNS server address on the user's PC could be a sign of DNS poisoning, as the attacker could have compromised the DNS server or spoofed its response to redirect the user's queries. References: <https://www.comptia.org/blog/what-is-dns-poisoning>

NEW QUESTION 110

- (Exam Topic 2)

A technician is troubleshooting a previously encountered issue. Which of the following should the technician reference to find what solution was implemented to resolve the issue?

- A. Standard operating procedures
- B. Configuration baseline documents
- C. Work instructions
- D. Change management documentation

Answer: D

Explanation:

Change management documentation is a record of the changes that have been made to a system or process, including the reason, date, time, and impact of each change. A technician can reference this documentation to find what solution was implemented to resolve a previously encountered issue, as well as any potential side effects or dependencies of the change. References: <https://www.comptia.org/blog/what-is-change-management>

NEW QUESTION 111

- (Exam Topic 2)

Which of the following is used to provide networking capability for VMs at Layer 2 of the OSI model?

- A. VPN
- B. VRRP
- C. vSwitch
- D. VIP

Answer: C

Explanation:

A vSwitch (virtual switch) is a software-based switch that provides networking capability for VMs (virtual machines) at Layer 2 of the OSI model. It connects the VMs to each other or to external networks using virtual NICs (network interface cards). A VPN (virtual private network) is a technology that creates a secure tunnel over a public network for remote access or site-to-site connectivity. VRRP (Virtual Router Redundancy Protocol) is a protocol that provides high availability for routers by creating a virtual router with multiple physical routers. A VIP (virtual IP) is an IP address that can be shared by multiple servers or devices for load balancing or failover purposes.

NEW QUESTION 112

- (Exam Topic 2)

A network administrator is reviewing interface errors on a switch. Which of the following indicates that a switchport is receiving packets in excess of the configured MTU?

- A. CRC errors
- B. Giants
- C. Runts
- D. Flooding

Answer: B

Explanation:

Giants are packets that exceed the configured MTU (Maximum Transmission Unit) of a switchport or interface, which causes them to be dropped or fragmented by the switch or router. The MTU is the maximum size of a packet that can be transmitted without fragmentation on a given medium or protocol. Giants can indicate misconfiguration or mismatch of MTU values between devices or interfaces on a network, which can cause performance issues or errors. CRC errors are errors that occur when the cyclic redundancy check (CRC) value of a packet does not match the calculated CRC value at the destination, which indicates corruption or alteration of data during transmission due to noise, interference, faulty cabling, etc., but not necessarily exceeding MTU values. Runts are packets that are smaller than the minimum size allowed by the medium or protocol, which causes them to be dropped or ignored by the switch or router. Flooding is a technique where a switch sends packets to all ports except the source port when it does not have an entry for the destination MAC address in its MAC address table, which can cause congestion or broadcast storms on a network.

NEW QUESTION 114

- (Exam Topic 2)

A lab environment hosts Internet-facing web servers and other experimental machines, which technicians use for various tasks. A technician installs software on one of the web servers to allow communication to the company's file server, but it is unable to connect to it. Other machines in the building are able to retrieve files from the file server. Which of the following is the MOST likely reason the web server cannot retrieve the files, and what should be done to resolve the problem?

- A. The lab environment's IDS is blocking the network traffic. The technician can whitelist the new application in the IDS.
- B. The lab environment is located in the DMZ, and traffic to the LAN zone is denied by default.
- C. The technician can move the computer to another zone or request an exception from the administrator.
- D. The lab environment has lost connectivity to the company router, and the switch needs to be rebooted. The technician can get the key to the wiring closet and manually restart the switch.
- E. The lab environment is currently set up with hubs instead of switches, and the requests are getting bounced back. The technician can submit a request for upgraded equipment to management.

Answer: B

Explanation:

The lab environment is located in the DMZ, and traffic to the LAN zone is denied by default. This is the most likely reason why the web server cannot retrieve files from the file server, and the technician can either move the computer to another zone or request an exception from the administrator to resolve the problem. A DMZ (Demilitarized Zone) is a network segment that separates the internal network (LAN) from the external network (Internet). It usually hosts public-facing servers such as web servers, email servers, or FTP servers that need to be accessed by both internal and external users. A firewall is used to control the traffic between the DMZ and the LAN zones, and usually denies traffic from the DMZ to the LAN by default for security reasons. Therefore, if a web server in the DMZ needs to communicate with a file server in the LAN, it would need a special rule or permission from the firewall administrator. References: <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

NEW QUESTION 118

- (Exam Topic 2)

Which of the following protocol types describes secure communication on port 443?

- A. ICMP
- B. UDP
- C. TCP
- D. IP

Answer: C

Explanation:

TCP is the protocol type that describes secure communication on port 443. TCP (Transmission Control Protocol) is a connection-oriented protocol that provides reliable and ordered delivery of data packets over an IP network. TCP uses port numbers to identify different applications or services on a device. Port 443 is the default port for HTTPS (Hypertext Transfer Protocol Secure), which is an extension of HTTP that uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security) encryption to protect data in transit between a web server and a web browser. References:

<https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION 119

- (Exam Topic 2)

Two remote offices need to be connected securely over an untrustworthy MAN. Each office needs to access network shares at the other site. Which of the following will BEST provide this functionality?

- A. Client-to-site VPN
- B. Third-party VPN service
- C. Site-to-site VPN
- D. Split-tunnel VPN

Answer: C

Explanation:

A site-to-site VPN is a type of VPN that connects two or more remote offices securely over an untrustworthy network, such as the Internet. A site-to-site VPN allows each office to access network shares and resources at the other site, as if they were on the same local network. A site-to-site VPN encrypts and tunnels the traffic between the offices, ensuring privacy and integrity of the data. References: <https://www.comptia.org/blog/what-is-a-site-to-site-vpn>

NEW QUESTION 121

- (Exam Topic 2)

A user is having difficulty with video conferencing and is looking for assistance. Which of the following would BEST improve performance?

- A. Packet shaping
- B. Quality of service
- C. Port mirroring
- D. Load balancing

Answer: B

Explanation:

Quality of service (QoS) is a mechanism that prioritizes network traffic based on different criteria, such as application type, source and destination address, port number, etc., and allocates bandwidth and resources accordingly. QoS would best improve performance for video conferencing, as it would ensure that video traffic gets higher priority and lower latency than other types of traffic on the network. Packet shaping is a technique that controls the rate or volume of network traffic by delaying or dropping packets that exceed certain thresholds or violate certain policies, which may not improve performance for video conferencing if it causes packet loss or jitter. Port mirroring is a technique that copies traffic from one port to another port on a switch for monitoring or analysis purposes, which does not improve performance for video conferencing at all. Load balancing is a technique that distributes network traffic across multiple servers or devices for improved availability and scalability, which does not

NEW QUESTION 126

- (Exam Topic 2)

A wireless network was installed in a warehouse for employees to scan crates with a wireless handheld scanner. The wireless network was placed in the corner of the building near the ceiling for maximum coverage. However, users in the offices adjacent to the warehouse have noticed a large amount of signal overlap from the new network. Additionally, warehouse employees report difficulty connecting to the wireless network from the other side of the building; however, they have no issues when they are near the antenna. Which of the following is MOST likely the cause?

- A. The wireless signal is being refracted by the warehouse's windows
- B. The antenna's power level was set too high and is overlapping
- C. An omnidirectional antenna was used instead of a unidirectional antenna
- D. The wireless access points are using channels from the 5GHz spectrum

Answer: C

Explanation:

An omnidirectional antenna was used instead of a unidirectional antenna, which is most likely the cause of the wireless network issues. An omnidirectional antenna provides wireless coverage in all directions from the antenna, which can cause signal overlap with adjacent offices and interference with other wireless networks. A unidirectional antenna, on the other hand, provides wireless coverage in a specific direction from the antenna, which can reduce signal overlap and interference and increase signal range and quality. A unidirectional antenna would be more suitable for a warehouse environment where users are located on one side of the building. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html> 1

NEW QUESTION 131

- (Exam Topic 2)

A network technician is investigating an IP phone that does not register in the VoIP system. Although it received an IP address, it did not receive the necessary DHCP options. The information that is needed for the registration is distributed by the DHCP scope. All other IP phones are working properly. Which of the following does the technician need to verify?

- A. VLAN mismatch
- B. Transceiver mismatch
- C. Latency
- D. DHCP exhaustion

Answer: A

Explanation:

A VLAN mismatch is the most likely reason why an IP phone does not receive the necessary DHCP options for registration. A VLAN mismatch occurs when a device is connected to a switch port that belongs to a different VLAN than the device's intended VLAN. This can cause communication problems or prevent access to network resources. For example, if an IP phone is connected to a switch port that belongs to the data VLAN instead of the voice VLAN, it may not receive the DHCP options that contain information such as the TFTP server address, the NTP server address, or the default gateway address for the voice VLAN.

These DHCP options are essential for the IP phone to register with the VoIP system and function properly. References:
<https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-c>

NEW QUESTION 132

- (Exam Topic 2)

A network technician has multimode fiber optic cable available in an existing IDF. Which of the following Ethernet standards should the technician use to connect the network switch to the existing fiber?

- A. 10GBaseT
- B. 1000BaseT
- C. 1000BaseSX
- D. 1000BaseLX

Answer: C

Explanation:

1000BaseSX is an Ethernet standard that should be used to connect the network switch to the existing multimode fiber optic cable. 1000BaseSX is a Gigabit Ethernet standard that uses short-wavelength laser (850 nm) over multimode fiber optic cable. It can support distances up to 550 meters depending on the cable type and quality. It is suitable for short-range network segments such as campus or building backbone networks. References:
<https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/produ>

NEW QUESTION 133

- (Exam Topic 2)

An ARP request is broadcasted and sends the following request. "Who is 192.168.1.200? Tell 192.168.1.55"

At which of the following layers of the OSI model does this request operate?

- A. Application
- B. Data link
- C. Transport
- D. Network
- E. Session

Answer: B

Explanation:

An ARP request operates at the data link layer of the OSI model. ARP (Address Resolution Protocol) is a protocol that maps IP addresses to MAC addresses on a local area network. It allows devices to communicate with each other without knowing their MAC addresses beforehand. ARP operates at the data link layer (layer 2) of the OSI model, which is responsible for framing and addressing data packets on a physical medium. References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION 136

- (Exam Topic 2)

A user reports a weak signal when walking 20ft (61 m) away from the WAP in one direction, but a strong signal when walking 20ft in the opposite direction The technician has reviewed the configuration and confirmed the channel type is correct There is no jitter or latency on the connection Which of the following would be the MOST likely cause of the issue?

- A. Antenna type
- B. Power levels
- C. Frequency
- D. Encryption type

Answer: A

Explanation:

The antenna type affects the signal strength and coverage of a WAP. Different types of antennas have different radiation patterns and gain, which determine how far and wide the signal can reach. If the user experiences a weak signal in one direction but a strong signal in the opposite direction, it could mean that the antenna type is not suitable for the desired coverage area. The technician should consider changing the antenna type to one that has a more balanced or directional radiation pattern. References:
<https://community.cisco.com/t5/wireless-small-business/wap200-poor-signal-strength/td-p/1565796>

NEW QUESTION 138

- (Exam Topic 2)

A network technician is investigating an issue with handheld devices in a warehouse. Devices have not been connecting to the nearest APs, but they have been connecting to an AP on the far side of the warehouse. Which of the following is the MOST likely cause of this issue?

- A. The nearest APs are configured for 802.11g.
- B. An incorrect channel assignment is on the nearest APs.
- C. The power level is too high for the AP on the far side.
- D. Interference exists around the AP on the far side.

Answer: C

Explanation:

The power level is a setting that determines how strong the wireless signal is from an access point (AP). If the power level is too high for an AP on the far side of a warehouse, it can cause interference and overlap with other APs on the same channel or frequency. This can result in handheld devices not connecting to the nearest APs, but connecting to the AP on the far side instead. A technician should adjust the power level of the AP on the far side to reduce interference and improve connectivity. References:
<https://www.comptia.org/blog/what-is-power-level>

NEW QUESTION 139

- (Exam Topic 2)

Which of the following security devices would be BEST to use to provide mechanical access control to the MDF/IDF?

- A. A smart card
- B. A key fob
- C. An employee badge
- D. A door lock

Answer: D

Explanation:

A door lock would be the best security device to use to provide mechanical access control to the MDF/IDF. A door lock is a device that prevents unauthorized access to a physical area by requiring a key, a code, a card, a biometric scan, or a combination of these factors to open it. A door lock can provide mechanical access control to the MDF/IDF, which are rooms that house network equipment such as switches, routers, servers, or patch panels. A door lock can prevent unauthorized persons from tampering with or stealing the network equipment or data. References:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_6.html

NEW QUESTION 141

- (Exam Topic 2)

A local firm has hired a consulting company to clean up its IT infrastructure. The consulting company notices remote printing is accomplished by port forwarding via publicly accessible IPs through the firm's firewall. Which of the following would be the MOST appropriate way to enable secure remote printing?

- A. SSH
- B. VPN
- C. Telnet
- D. SSL

Answer: B

Explanation:

VPN (Virtual Private Network) is the most appropriate way to enable secure remote printing. VPN is a technology that creates a secure and encrypted tunnel over a public network such as the Internet. It allows remote users or sites to access a private network as if they were directly connected to it. VPN can be used for various purposes such as accessing corporate resources, bypassing geo-restrictions, or enhancing privacy and security. VPN can also be used for remote printing by allowing users to connect to a printer on the private network and send print jobs securely over the VPN tunnel. References:

<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-work>

NEW QUESTION 146

- (Exam Topic 2)

A network administrator is required to ensure that auditors have read-only access to the system logs, while systems administrators have read and write access to the system logs, and operators have no access to the system logs. The network administrator has configured security groups for each of these functional categories. Which of the following security capabilities will allow the network administrator to maintain these permissions with the LEAST administrative effort?

- A. Mandatory access control
- B. User-based permissions
- C. Role-based access
- D. Least privilege

Answer: C

Explanation:

Role-based access is a security capability that assigns permissions to users based on their roles or functions within an organization. It allows the network administrator to maintain these permissions with the least administrative effort, as they only need to configure the security groups for each role once and then assign users to those groups. Mandatory access control is a security capability that assigns permissions based on security labels or classifications, which requires more administrative effort to maintain. User-based permissions are a security capability that assigns permissions to individual users, which is not scalable or efficient for large organizations. Least privilege is a security principle that states that users should only have the minimum level of access required to perform their tasks, which is not a security capability by itself.

NEW QUESTION 147

- (Exam Topic 2)

An organization with one core and five distribution switches is transitioning from a star to a full-mesh topology. Which of the following is the number of additional network connections needed?

- A. 5
- B. 7
- C. 10
- D. 15

Answer: C

Explanation:

10 additional network connections are needed to transition from a star to a full-mesh topology. A star topology is a network topology where each device is connected to a central device, such as a switch or a hub. A full-mesh topology is a network topology where each device is directly connected to every other device. The number of connections needed for a full-mesh topology can be calculated by the formula $n(n-1)/2$, where n is the number of devices. In this case, there are six devices (one core and five distribution switches), so the number of connections needed for a full-mesh topology is $6(6-1)/2 = 15$. Since there are already five connections in the star topology (one from each distribution switch to the core switch), the number of additional connections needed is $15 - 5 = 10$. References:

<https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION 151

- (Exam Topic 2)

A firewall administrator is implementing a rule that directs HTTP traffic to an internal server listening on a non-standard socket. Which of the following types of rules is the administrator implementing?

- A. NAT
- B. PAT
- C. STP
- D. SNAT
- E. ARP

Answer: B

Explanation:

The firewall administrator is implementing a PAT (Port Address Translation) rule that directs HTTP traffic to an internal server listening on a non-standard socket. PAT is a type of NAT (Network Address Translation) that allows multiple devices to share a single public IP address by using different port numbers. PAT can also be used to redirect traffic from one port to another port on the same or different IP address. This can be useful for security or load balancing purposes. For example, a firewall administrator can configure a PAT rule that redirects HTTP traffic (port 80) from the public IP address of the firewall to an internal server that listens on a non-standard port (such as 8080) on its private IP address. References: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html>

NEW QUESTION 152

- (Exam Topic 2)

A network administrator has been directed to present the network alerts from the past week to the company's executive staff. Which of the following will provide the BEST collection and presentation of this data?

- A. A port scan printout
- B. A consolidated report of various network devices
- C. A report from the SIEM tool
- D. A report from a vulnerability scan done yesterday

Answer: C

Explanation:

SIEM stands for Security Information and Event Management, which is a tool that collects, analyzes, and correlates data from various network devices and sources to provide alerts and reports on security incidents and events. A report from the SIEM tool can provide a comprehensive overview of the network alerts from the past week to the executive staff, highlighting any potential threats, vulnerabilities, or anomalies. References: <https://www.comptia.org/blog/what-is-siem>

NEW QUESTION 154

- (Exam Topic 2)

An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch. Which of the following command-line tools should the technician use to determine where the incident is occurring?

- A. nslookup
- B. show config
- C. netstat
- D. show interface
- E. show counters

Answer: D

Explanation:

show interface is a command-line tool that displays information about the status, configuration, and statistics of an interface on a network device. A technician can use show interface to determine where the incident is occurring in a network by checking the uplink status, speed, duplex mode, errors, collisions, and other parameters of each interface. References: <https://www.comptia.org/blog/what-is-show-interface>

NEW QUESTION 156

- (Exam Topic 2)

During the security audit of a financial firm the Chief Executive Officer (CEO) questions why there are three employees who perform very distinct functions on the server. There is an administrator for creating users another for assigning the users to groups and a third who is the only administrator to perform file rights assignment. Which of the following mitigation techniques is being applied?

- A. Privileged user accounts
- B. Role separation
- C. Container administration
- D. Job rotation

Answer: B

Explanation:

Role separation is a security principle that involves dividing the tasks and privileges for a specific business process among multiple users. This reduces the risk of fraud and errors, as no one user has complete control over the process. In the scenario, there are three employees who perform very distinct functions on the server, which is an example of role separation. References: <https://hyperproof.io/resource/segregation-of-duties/>

NEW QUESTION 160

- (Exam Topic 2)

A systems administrator is running a VoIP network and is experiencing jitter and high latency. Which of the following would BEST help the administrator determine the cause of these issues?

- A. Enabling RADIUS on the network
- B. Configuring SNMP traps on the network
- C. Implementing LDAP on the network
- D. Establishing NTP on the network

Answer: B

Explanation:

SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate with a network management system (NMS) for monitoring and configuration purposes. SNMP traps are unsolicited messages sent by network devices to the NMS when certain events or conditions occur, such as errors, failures, or thresholds. Configuring SNMP traps on the network would best help the administrator determine the cause of jitter and high latency on a VoIP network, as they would provide real-time alerts and information about the network performance and status. Enabling RADIUS on the network is not relevant to troubleshooting VoIP issues, as RADIUS is a protocol that provides authentication, authorization, and accounting services for network access. Implementing LDAP on the network is also not relevant to troubleshooting VoIP issues, as LDAP is a protocol that provides directory services for storing and querying information about users, groups, devices, etc. Establishing NTP on the network is not directly related to troubleshooting VoIP issues, as NTP is a protocol that synchronizes the clocks of network devices.

NEW QUESTION 164

- (Exam Topic 2)

A technician is connecting DSL for a new customer. After installing and connecting the on-premises equipment, the technician verifies DSL synchronization. When connecting to a workstation, however, the link LEDs on the workstation and modem do not light up. Which of the following should the technician perform during troubleshooting?

- A. Identify the switching loops between the modem and the workstation.
- B. Check for asymmetrical routing on the modem.
- C. Look for a rogue DHCP server on the network.
- D. Replace the cable connecting the modem and the workstation.

Answer: D

Explanation:

If the link LEDs on the workstation and modem do not light up when connecting to a workstation, it could indicate a problem with the cable connecting them. The cable could be damaged, defective, or incompatible with the devices. A technician should replace the cable with a known good one and check if the link LEDs light up. If not, the problem could be with the network interface cards (NICs) on the workstation or modem. References: <https://www.comptia.org/blog/what-is-link-light>

NEW QUESTION 165

- (Exam Topic 2)

Which of the following is MOST commonly used to address CVEs on network equipment and/or operating systems?

- A. Vulnerability assessment
- B. Factory reset
- C. Firmware update
- D. Screened subnet

Answer: C

Explanation:

Firmware is a type of software that controls the low-level functions of a hardware device, such as a router, switch, printer, or camera. Firmware updates are patches or upgrades that fix bugs, improve performance, add features, or address security vulnerabilities in firmware. Firmware updates are commonly used to address CVEs (Common Vulnerabilities and Exposures) on network equipment and operating systems, as CVEs are publicly known flaws that can be exploited by attackers. References: <https://www.comptia.org/blog/what-is-firmware>

NEW QUESTION 169

- (Exam Topic 2)

A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

- A. nslookup
- B. netstat -a
- C. ipconfig /a
- D. arp -a

Answer: B

Explanation:

netstat -a is a command that displays information about active TCP connections and listening ports on a system. A network administrator can use netstat -a to check if the database engine is listening on a certain port, as well as verify if there are any connections established to or from that port. References: <https://www.comptia.org/blog/what-is-netstat>

NEW QUESTION 173

- (Exam Topic 2)

A user recently made changes to a PC that caused it to be unable to access websites by both FQDN and IP Local resources, such as the file server remain accessible. Which of the following settings did the user MOST likely misconfigure?

- A. Static IP
- B. Default gateway
- C. DNS entries
- D. Local host file

Answer: B

Explanation:

The default gateway is the setting that the user most likely misconfigured on the PC that caused it to be unable to access websites by both FQDN and IP. The default gateway is a device, usually a router or a firewall, that connects a local network to other networks such as the Internet. It acts as an intermediary between devices on different networks and forwards packets based on their destination IP addresses. If the default gateway is not configured correctly on a PC, it will not be able to communicate with devices outside its local network, such as web servers or DNS servers. References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/16448-default-gateway.html>

NEW QUESTION 174

- (Exam Topic 2)

A customer wants to segregate the traffic between guests on a hypervisor. Which of the following does a technician need to configure to meet the requirement?

- A. Virtual switches
- B. OSPF routing
- C. Load balancers
- D. NIC teaming
- E. Fibre Channel

Answer: A

Explanation:

A virtual switch is a software-based switch that connects virtual machines on a hypervisor. A virtual switch can create and manage VLANs, which are logical segments of a network that isolate traffic between different groups of devices. A customer can use virtual switches to segregate the traffic between guests on a hypervisor by creating a separate VLAN for each guest and assigning it to a virtual switch port. References: <https://www.comptia.org/blog/what-is-a-virtual-switch>

NEW QUESTION 177

- (Exam Topic 2)

A city has hired a new employee who needs to be able to work when traveling at home and at the municipal sourcing of a neighboring city that snares services. The employee is issued a laptop, and a technician needs to train the employee on the appropriate solutions for secure access to the network from all the possible locations On which of the following solutions would the technician MOST likely train the employee?

- A. Site-to-site VPNs between the two city locations and client-to-site software on the employee's laptop for all other remote access
- B. Client-to-site VPNs between the travel locations and site-to-site software on the employee's laptop for all other remote access
- C. Client-to-site VPNs between the two city locations and site-to-site software on the employee's laptop for all other remote access
- D. Site-to-site VPNs between the home and city locations and site-to-site software on the employee's laptop for all other remote access

Answer: A

Explanation:

The technician would most likely train the employee on using site-to-site VPNs between the two city locations and client-to-site software on the employee's laptop for all other remote access. A VPN (Virtual Private Network) is a technology that creates a secure and encrypted tunnel over a public network such as the Internet. It allows remote users or sites to access a private network as if they were directly connected to it. A site-to-site VPN connects two or more networks, such as branch offices or data centers, using a VPN gateway device at each site. A client-to-site VPN connects individual users, such as mobile workers or telecommuters, using a VPN client software on their devices. In this scenario, the employee needs to access the network from different locations, such as home, travel, or another city. Therefore, the technician would train the employee on how to use site-to-site VPNs to connect to the network from another city location that shares services, and how to use client-to-site software to connect to the network from home or travel locations. References: <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-work>

NEW QUESTION 178

- (Exam Topic 2)

Which of the following would be used to expedite MX record updates to authoritative NSs?

- A. UDP forwarding
- B. DNS caching
- C. Recursive lookup
- D. Time to live

Answer: D

Explanation:

Time to live (TTL) is a value that indicates how long a DNS record can be cached by authoritative NSs (name servers) or other DNS servers before it expires and needs to be updated. A lower TTL value would expedite MX record updates to authoritative NSs, as they would refresh the record more frequently. UDP forwarding is not a DNS term, but a technique of sending UDP packets from one host to another. DNS caching is the process of storing DNS records locally for faster resolution, which does not expedite MX record updates. Recursive lookup is a type of DNS query where a DNS server queries other DNS servers on behalf of a client until it finds the answer, which does not expedite MX record updates.

NEW QUESTION 181

- (Exam Topic 3)

A network technician needs to ensure the company's external mail server can pass reverse lookup checks. Which of the following records would the technician MOST likely configure? (Choose Correct option and give explanation directly from CompTIA Network+ Study guide or documents)

- A. PTR
- B. AAAA
- C. SPF
- D. CNAME

Answer: A

Explanation:

A PTR (Pointer) record is used to map an IP address to a domain name, which is necessary for reverse lookup checks. Reverse lookup checks are performed by external mail servers to verify the identity of the sender of the email. By configuring a PTR record, the network technician can ensure that the company's external mail server can pass these checks. According to the CompTIA Network+ Study Guide, "A PTR record is used to map an IP address to a domain name, and it is often used for email authentication."

NEW QUESTION 184

- (Exam Topic 3)

Which of the following is used to elect an STP root?

- A. A bridge ID
- B. A bridge protocol data unit
- C. Interface port priority
- D. A switch's root port

Answer: B

Explanation:

"Using special STP frames known as bridge protocol data units (BPDUs), switches communicate with other switches to prevent loops from happening in the first place. Configuration BPDUs establish the topology, where one switch is elected root bridge and acts as the center of the STP universe. Each switch then uses the root bridge as a reference point to maintain a loop-free topology."

NEW QUESTION 189

- (Exam Topic 3)

An administrator is investigating reports of network slowness in a building. While looking at the uplink interface statistics in the switch's CLI, the administrator discovers the uplink is at 100% utilization. However, the administrator is unsure how to identify what traffic is causing the saturation. Which of the following tools should the administrator utilize to identify the source and destination addresses of the traffic?

- A. SNMP
- B. Traps
- C. Syslog
- D. NetFlow

Answer: D

Explanation:

To identify the source and destination addresses of the traffic causing network saturation, the network administrator should use a network protocol analyzer that supports the NetFlow protocol. NetFlow is a network protocol that collects IP traffic information as it enters or exits an interface and sends it to a NetFlow collector for analysis. This data includes the source and destination addresses of the traffic, the ports used, and the number of bytes and packets transferred. Therefore, the correct answer is option D, NetFlow.

Reference: CompTIA Network+ Study Guide, Exam N10-007, Fourth Edition, by Todd Lammle (Chapter 6: Network Devices)

NEW QUESTION 192

- (Exam Topic 3)

A technician performed a manual reconfiguration of a firewall, and network connectivity was reestablished. Some connection events that were previously sent to a syslog server are no longer being generated by the firewall. Which of the following should the technician perform to fix the issue?

- A. Adjust the proper logging level on the new firewall.
- B. Tune the filter for logging the severity level on the syslog server.
- C. Activate NetFlow traffic between the syslog server and the firewall.
- D. Restart the SNMP service running on the syslog server.

Answer: A

Explanation:

Logging level is a setting that determines what types of events are recorded by a device and sent to a syslog server. Different logging levels have different severity levels, ranging from emergency to debug. If the technician performed a manual reconfiguration of the firewall, it is possible that the logging level was changed or reset to a lower level that does not include the connection events that were previously sent to the syslog server. To fix the issue, the technician should adjust the proper logging level on the new firewall to match the desired level of detail and severity for the connection events. References: Network+ Study Guide Objective 3.4: Explain common scanning, monitoring and patching processes and summarize their expected outputs. Subobjective: Syslog.

NEW QUESTION 196

- (Exam Topic 3)

A network administrator is installing a new server in the data center. The administrator is concerned the amount of traffic generated will exceed 1GB, and higher-throughput NICs are not available for installation. Which of the following is the BEST solution for this issue?

- A. Install an additional NIC and configure LACP.
- B. Remove some of the applications from the server.
- C. Configure the NIC to use full duplex.
- D. Configure port mirroring to send traffic to another server.
- E. Install a SSD to decrease data processing time.

Answer: A

NEW QUESTION 201

- (Exam Topic 3)

A technician is investigating an issue with connectivity at customer's location. The technician confirms that users can access resources locally but not over the

internet The technician theorizes that the local router has failed and investigates further. The technician's testing results show that the route is functional: however, users still are unable to reach resources on the internal. Which of the following describes what the technician should do NEXT?

- A. Document the lessons learned
- B. Escalate the issue
- C. identify the symptoms.
- D. Question users for additional information

Answer: C

Explanation:

According to the CompTIA Network+ troubleshooting model123, this is the first step in troubleshooting a network problem. The technician should gather information about the current state of the network, such as error messages, device status, network topology, and user feedback. This can help narrow down the scope of the problem and eliminate possible causes.

NEW QUESTION 204

- (Exam Topic 3)

A company has wireless APS that were deployed with 802.11g. A network engineer has noticed more frequent reports of wireless performance issues during the lunch hour in comparison to the rest of the day. The engineer thinks bandwidth consumption will increase while users are on their breaks, but network utilization logs do not show increased bandwidth numbers. Which Of the following would MOST likely resolve this issue?

- A. Adding more wireless APS
- B. Increasing power settings to expand coverage
- C. Configuring the APS to be compatible with 802.11a
- D. Changing the wireless channel used

Answer: C

Explanation:

* 802.11 g is an older wireless standard that operates in the 2.4 GHz frequency band and has a maximum data rate of 54 Mbps. 802.11a is a newer wireless standard that operates in the 5 GHz frequency band and has a maximum data rate of 54 Mbps. By configuring the APS to be compatible with 802.11a, the network engineer can reduce interference and congestion in the 2.4 GHz band and improve wireless performance.

References: Network+ Study Guide Objective 2.5: Implement network troubleshooting methodologies

NEW QUESTION 208

- (Exam Topic 3)

A network administrator notices excessive wireless traffic occurring on an access point after normal business hours. The access point is located on an exterior wall. Which of the following should the administrator do to limit wireless access outside the building?

- A. Set up a private VLAN.
- B. Disable roaming on the WAP.
- C. Change to a directional antenna.
- D. Stop broadcasting of the SSID.

Answer: C

Explanation:

A directional antenna is a type of antenna that radiates or receives radio waves in a specific direction. This can help limit wireless access outside the building by focusing the signal towards the intended area and reducing the signal strength in other directions. A private VLAN is a feature that isolates network devices within a VLAN. Disabling roaming on the WAP prevents wireless clients from switching to another WAP when the signal is weak. Stopping broadcasting of the SSID hides the network name from wireless clients, but does not prevent them from connecting if they know the SSID.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.1: Given a scenario, install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.

NEW QUESTION 209

- (Exam Topic 3)

Which of the following layers of the OSI model has new protocols activated when a user moves from a wireless to a wired connection?

- A. Data link
- B. Network
- C. Transport
- D. Session

Answer: A

Explanation:

"The Data Link layer also determines how data is placed on the wire by using an access method. The wired access method, carrier-sense multiple access with collision detection (CSMA/CD), was once used by all wired Ethernet networks, but is automatically disabled on switched full-duplex links, which have been the norm for decades. Carrier-sense multiple access with collision avoidance (CSMA/CA) is used by wireless networks, in a similar fashion."

NEW QUESTION 211

- (Exam Topic 3)

Which of the following devices would be used to extend the range of a wireless network?

- A. A repeater
- B. A media converter
- C. A router
- D. A switch

Answer: A

Explanation:

A repeater is a device used to extend the range of a wireless network by receiving, amplifying, and retransmitting wireless signals. It is typically used to extend the range of a wireless network in a large area, such as an office building or a campus. Repeaters can also be used to connect multiple wireless networks together, allowing users to move seamlessly between networks. As stated in the CompTIA Network+ Study Manual, "a wireless repeater is used to extend the range of a wireless network by repeating the signal from one access point to another."

NEW QUESTION 214

- (Exam Topic 3)

Which of the following would MOST likely utilize PoE?

- A. A camera
- B. A printer
- C. A hub
- D. A modem

Answer: A

Explanation:

A camera is most likely to utilize PoE (Power over Ethernet). PoE is a technology that allows electrical power to be delivered over Ethernet cables. It is used to power a variety of devices, such as cameras, phones, access points, and other networking equipment. Cameras are particularly well-suited for PoE because they are often installed in locations where it is difficult or impossible to run electrical power. By using PoE, cameras can be powered directly over the Ethernet cable, eliminating the need for separate power cables and outlets. Other devices, such as printers, hubs, and modems, are less likely to utilize PoE because they typically do not need to be powered over Ethernet. These devices are usually powered by AC (alternating current) power and are typically connected to a power outlet rather than an Ethernet cable.

NEW QUESTION 219

- (Exam Topic 3)

Which of the following OSI model layers would allow a user to access and download files from a remote computer?

- A. Session
- B. Presentation
- C. Network
- D. Application

Answer: D

Explanation:

The application layer of the OSI model (Open Systems Interconnection) is responsible for providing services to applications that allow users to access and download files from a remote computer. These services include file transfer, email, and web access, as well as other related services. In order for a user to access and download files from a remote computer, the application layer must provide the necessary services that allow the user to interact with the remote computer.

NEW QUESTION 224

- (Exam Topic 3)

A security vendor needs to add a note to the DNS to validate the ownership of a company domain before services begin. Which of the following records did the security company MOST likely ask the company to configure?

- A. TXT
- B. AAAA
- C. CNAME
- D. SRV

Answer: A

Explanation:

TXT stands for Text and is a type of DNS record that can store arbitrary text data associated with a domain name. TXT records can be used for various purposes, such as verifying the ownership of a domain, providing information about a domain, or implementing security mechanisms such as SPF (Sender Policy Framework) or DKIM (DomainKeys Identified Mail). In this scenario, the security company most likely asked the company to configure a TXT record with a specific value that can prove the ownership of the domain. AAAA stands for IPv6 Address and is a type of DNS record that maps a domain name to an IPv6 address. CNAME stands for Canonical Name and is a type of DNS record that maps an alias name to another name. SRV stands for Service and is a type of DNS record that specifies the location of a service on a network.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.8: Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 229

- (Exam Topic 3)

A large number of PCs are obtaining an APIPA IP address, and a number of new computers were added to the network. Which of the following is MOST likely causing the PCs to obtain an APIPA address?

- A. Rogue DHCP server
- B. Network collision
- C. Incorrect DNS settings
- D. DHCP scope exhaustion

Answer: D

Explanation:

DHCP scope exhaustion means that there are no more available IP addresses in the DHCP server's pool of addresses to assign to new devices on the network. When this happens, the devices will use APIPA (Automatic Private IP Addressing) to self-configure an IP address in the range of 169.254.0.1 to 169.254.255.254. These addresses are not routable and can only communicate with other devices on the same local network.

A rogue DHCP server (A) is an unauthorized DHCP server that can cause IP address conflicts or security issues by assigning IP addresses to devices on the network. A network collision (B) is a situation where two or more devices try to send data on the same network segment at the same time, causing interference and data loss. Incorrect DNS settings © can prevent devices from resolving domain names to IP addresses, but they do not affect the DHCP process.

NEW QUESTION 233

- (Exam Topic 3)

A technician thinks one of the router ports is flapping. Which of the following available resources should the technician use in order to determine if the router is flapping?

- A. Audit logs
- B. NetFlow
- C. Syslog
- D. Traffic logs

Answer: C

Explanation:

Syslog is a protocol that allows network devices to send event messages to a centralized server or console for logging and analysis¹. Syslog can help a technician to determine if a router port is flapping by providing timestamps, severity levels, and descriptions of the events that occur on the router, such as interface up or down, link state change, or error messages. Syslog can also help to identify the cause and frequency of the port flapping and troubleshoot the issue.

Audit logs are records of actions or events that occur on a system or network, such as user login, file access, configuration change, or policy violation. Audit logs can help to monitor and verify the activities and behaviors of users, devices, or applications on a system or network. Audit logs can also help to detect and investigate security incidents, compliance issues, or performance problems. However, audit logs do not provide detailed information about router port flapping.

NetFlow is a protocol that collects and analyzes network traffic data for monitoring and troubleshooting purposes². NetFlow can help to identify the sources, destinations, volumes, and types of traffic on a network. NetFlow can also help to optimize network performance, security, and capacity planning. However, NetFlow does not provide detailed information about router port flapping.

Traffic logs are records of network traffic that pass through a device or application, such as a firewall, proxy, or web server. Traffic logs can help to monitor and filter the network traffic based on rules or policies. Traffic logs can also help to detect and prevent malicious traffic, such as malware, attacks, or unauthorized access. However, traffic logs do not provide detailed information about router port flapping.

NEW QUESTION 237

- (Exam Topic 3)

Due to a surge in business, a company is onboarding an unusually high number of salespeople. The salespeople are assigned desktops that are wired to the network. The last few salespeople to be onboarded are able to access corporate materials on the network but not sales-specific resources. Which of the following is MOST likely the cause?

- A. The switch was configured with port security.
- B. Newly added machines are running into DHCP conflicts.
- C. The IPS was not configured to recognize the new users.
- D. Recently added users were assigned to the wrong VLAN

Answer: D

NEW QUESTION 239

- (Exam Topic 3)

Which of the following is the MOST cost-effective alternative that provides proper cabling and supports gigabit Ethernet devices?

- A. Twisted cable with a minimum Cat 5e certification
- B. Multimode fiber with an SC connector
- C. Twinaxial cabling using an F-type connector
- D. Cable termination using TIA/EIA-568-B

Answer: A

Explanation:

twisted cable with a minimum Cat 5e certification is the MOST cost-effective alternative that provides proper cabling and supports gigabit Ethernet devices.

NEW QUESTION 243

- (Exam Topic 3)

During a risk assessment which of the following should be considered when planning to mitigate high CPU utilization of a firewall?

- A. Recovery time objective
- B. Uninterruptible power supply
- C. NIC teaming
- D. Load balancing

Answer: D

Explanation:

The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs. This does nothing to help with CPU utilization. Load balancing does this.

NEW QUESTION 244

- (Exam Topic 3)

A technician wants to monitor and provide traffic segmentation across the network. The technician would like to assign each department a specific identifier. Which of the following will the technician MOST likely use?

- A. Flow control
- B. Traffic shaping
- C. VLAN tagging
- D. Network performance baselines

Answer: C

Explanation:

To monitor and provide traffic segmentation across the network, a technician may use the concept of VLANs (Virtual Local Area Networks). VLANs are a way of dividing a single physical network into multiple logical networks, each with its own unique identifier or "tag."

By assigning each department a specific VLAN identifier, the technician can segment the network traffic and ensure that the different departments' traffic is kept separate from one another. This can help to improve network security, performance, and scalability, as well as allowing for better monitoring and control of the network traffic.

To implement VLANs, the technician will need to configure VLAN tagging on the network devices, such as switches and routers, and assign each department's devices to the appropriate VLAN. The technician may also need to configure VLAN trunking to allow the different VLANs to communicate with each other.

By using VLANs, the technician can effectively monitor and segment the network traffic, providing better control and visibility into the network.

NEW QUESTION 249

- (Exam Topic 3)

A company with multiple routers would like to implement an HA network gateway with the least amount of downtime possible. This solution should not require changes on the gateway setting of the network clients. Which of the following should a technician configure?

- A. Automate a continuous backup and restore process of the system's state of the active gateway.
- B. Use a static assignment of the gateway IP address on the network clients.
- C. Configure DHCP relay and allow clients to receive a new IP setting.
- D. Configure a shared VIP and deploy VRRP on the routers.

Answer: D

Explanation:

The open standard protocol Virtual Router Redundancy Protocol (VRRP) is similar to HSRP, the differences mainly being in terminology and packet formats. In VRRP, the active router is known as the master, and all other routers in the group are known as backup routers. There is no specific standby router; instead, all backup routers monitor the status of the master, and in the event of a failure, a new master router is selected from the available backup routers based on priority.

NEW QUESTION 250

- (Exam Topic 3)

An ISP is providing Internet to a retail store and has terminated its point of connection using a standard Cat 6 pin-out. Which of the following terminations should the technician use when running a cable from the ISP's port to the front desk?

- A. F-type connector
- B. TIA/EIA-56S-B
- C. LC
- D. SC

Answer: B

Explanation:

The termination that the technician should use when running a cable from the ISP's port to the front desk is B. TIA/EIA-568-B. This is a standard pin-out for Cat 6 cables that is used for Ethernet and other network physical layers. It specifies how to arrange the eight wires in an RJ45 connector, which is a common type of connector for network cables.

NEW QUESTION 254

- (Exam Topic 3)

An administrator would like to create a fault-tolerant ring between three switches within a Layer 2 network. Which of the following Ethernet features should the administrator employ?

- A. Spanning Tree Protocol
- B. Open Shortest Path First
- C. Port mirroring
- D. An interior gateway protocol

Answer: A

Explanation:

Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology in Ethernet networks by actively blocking certain links and enabling others.

STP prevents loops by putting some of the links in a blocking state, effectively creating a loop-free topology. This ensures that there is only one active path between two devices, which helps prevent network loops and the associated problems (such as broadcast storms) that can result from them. STP is used to create a fault-tolerant ring between three switches within a Layer 2 network.

NEW QUESTION 259

- (Exam Topic 3)

A network technician is implementing a solution that will allow end users to gain access to multiple applications after logging on. Which of the following authentication methods would allow this type of access?

- A. SSO
- B. LDAP

- C. EAP
- D. TACACS+

Answer: A

NEW QUESTION 261

- (Exam Topic 3)

An administrator is setting up a multicast server on a network, but the firewall seems to be dropping the traffic. After logging in to the device, the administrator sees the following entries:

Rule	Action	Source	Destination	Port
1	Deny	Any	172.30.10.50	Any
2	Deny	Any	232.1.4.9	Any
3	Deny	Any	242.9.15.4	Any
4	Deny	Any	175.50.10.10	Any

Which of the following firewall rules is MOST likely causing the issue?

- A. Rule 1
- B. Rule 2
- C. Rule 3
- D. Rule 4

Answer: A

NEW QUESTION 264

- (Exam Topic 3)

Switch 3 was recently added to an existing stack to extend connectivity to various parts of the network. After the update, new employees were not able to print to the main networked copiers from their workstations. Following are the port configurations for the switch stack in question:

Switch 1:

	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	60	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Active	Active	Active	Active

Switch 2:

	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	60	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Active	Shut down	Active	Active

Switch 3:

	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	80	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Shut down	Shut down	Shut down	Active

Which of the following should be configured to resolve the issue? (Select TWO).

- A. Enable the printer ports on Switch 3.
- B. Reconfigure the duplex settings on the printer ports on Switch 3.
- C. Reconfigure the VLAN on the printer ports to VLAN 20.
- D. Enable all ports that are shut down on the stack.
- E. Reconfigure the VLAN on the printer ports on Switch 3.
- F. Enable wireless APs on Switch 3.

Answer: AE

NEW QUESTION 269

- (Exam Topic 3)

Which of the following allows for devices within a network to share a highly reliable time source?

- A. NTP
- B. SNMP
- C. SIP
- D. DNS

Answer: A

Explanation:

Network Time Protocol (NTP) is a protocol used to maintain a highly accurate and reliable clock time on all devices within a network. NTP works by synchronizing the time of all the devices within a network to a single, highly accurate time source. This allows for the time of all the devices to be kept in sync with each other, ensuring a consistent and reliable time source for all devices within the network.

NEW QUESTION 271

- (Exam Topic 3)

A public, wireless ISP mounts its access points on top of traffic signal poles. Fiber-optic cables are installed from a fiber switch through the ground and up the pole to a fiber-copper media converter, and then connected to the AP. In one location, the switchport is showing sporadic link loss to the attached AP. A similar link loss is not seen at the AP interface. The fiber-optic cable is moved to another unused switchport with a similar result. Which of the following steps should the assigned technician complete NEXT?

- A. Disable and enable the switchport.
- B. Clean the fiber-optic cable ends.
- C. Replace the media converter.
- D. Replace the copper patch cord.

Answer: B

Explanation:

Fiber-optic cables are cables that use light signals to transmit data over long distances at high speeds.

Fiber-optic cables are sensitive to dirt, dust, moisture, or other contaminants that can interfere with the light signals and cause link loss or signal degradation. To troubleshoot link loss issues with fiber-optic cables, one of the steps that should be completed next is to clean the fiber-optic cable ends with a lint-free cloth or a specialized cleaning tool. Cleaning the fiber-optic cable ends can remove any dirt or debris that may be blocking or reflecting the light signals and restore the link quality.

NEW QUESTION 274

- (Exam Topic 3)

A network is secured and is only accessible via TLS and IPsec VPNs. Which of the following would need to be present to allow a user to access network resources on a laptop without logging in to the VPN application?

- A. Site-to-site
- B. Secure Shell
- C. In-band management
- D. Remote desktop connection

Answer: A

Explanation:

A site-to-site VPN is a type of VPN that connects two or more networks over the Internet using a secure

tunnel. A site-to-site VPN allows users to access network resources on a laptop without logging in to the VPN application, as long as the laptop is connected to one of the networks in the VPN. A site-to-site VPN is transparent to the users and does not require any additional software or configuration on the client devices.

References: Network+ Study Guide Objective 3.4: Explain the purposes and use cases for VPNs.

NEW QUESTION 275

- (Exam Topic 3)

On a network with redundant switches, a network administrator replaced one of the switches but was unable to get a connection with another switch. Which of the following should the administrator check after successfully testing the cable that was wired for TIA/EIA-568A on both ends?

- A. If MDIX is enabled on the new switch
- B. If PoE is enabled
- C. If a plenum cable is being used
- D. If STP is disabled on the switches

Answer: A

Explanation:

Auto-MDIX (or medium dependent interface crossover) is a feature that automatically detects the type of cable connection and configures the interface accordingly (i.e. straight-through or crossover). This ensures that the connection between the two switches is successful. This is referenced in the CompTIA Network+ Study Manual, page 519.

NEW QUESTION 280

- (Exam Topic 3)

A company is opening a new building on the other side of its campus. The distance from the closest building to the new building is 1,804ft (550m). The company needs to connect the networking equipment in the new building to the Other buildings on the campus without using a repeater. Which Of the following transceivers should the company use?

- A. 10GBASE-SW
- B. 10GBASE-LR
- C. 10GBASE-LX4 over multimode fiber
- D. 10GBASE-SR

Answer: B

Explanation:

10GBASE-LR is a standard for 10 Gbps Ethernet over single-mode fiber optic cable. It can support a maximum distance of 6.2 miles (10 km), which is much longer than the distance between the buildings. 10GBASE-SW, 10GBASE-LX4, and 10GBASE-SR are all standards for 10 Gbps Ethernet over multimode fiber optic cable, which have shorter maximum distances ranging from 984ft (300m) to 1,312ft (400m).

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.5: Compare and contrast network cabling types, standards and speeds.

NEW QUESTION 285

- (Exam Topic 3)

Which of the following describes the ability of a corporate IT department to expand its cloud-hosted VM environment with minimal effort?

- A. Scalability
- B. Load balancing
- C. Multitenancy
- D. Geo-redundancy

Answer: A

Explanation:

Scalability is the ability of a corporate IT department to expand its cloud-hosted virtual machine (VM) environment with minimal effort. This allows IT departments to quickly and easily scale up their cloud environment to meet increased demand. Scalability also allows for the efficient use of resources, as IT departments can quickly and easily scale up or down as needed.

NEW QUESTION 287

- (Exam Topic 3)

A network administrator needs to provide evidence to confirm that recent network outages were caused by increased traffic generated by a recently released application. Which of the following actions will BEST support the administrator's response?

- A. Generate a network baseline report for comparison.
- B. Export the firewall traffic logs.
- C. Collect the router's NetFlow data.
- D. Plot interface statistics for dropped packets.

Answer: C

NEW QUESTION 291

- (Exam Topic 3)

A network administrator is getting reports of some internal users who cannot connect to network resources. The users state they were able to connect last week, but not today. No changes have been configured on the network devices or server during the last few weeks. Which of the following is the MOST likely cause of the issue?

- A. The client DHCP scope is fully utilized
- B. The wired network is experiencing electrical interference
- C. The captive portal is down and needs to be restarted
- D. SNMP traps are being received
- E. The packet counter on the router interface is high.

Answer: A

NEW QUESTION 292

- (Exam Topic 3)

A security administrator is trying to prevent incorrect IP addresses from being assigned to clients on the network. Which of the following would MOST likely prevent this and allow the network to continue to operate?

- A. Configuring DHCP snooping on the switch
- B. Preventing broadcast messages leaving the client network
- C. Blocking ports 67/68 on the client network
- D. Enabling port security on access ports

Answer: A

Explanation:

To prevent incorrect IP addresses from being assigned to clients on the network and allow the network to continue to operate, the security administrator should consider configuring DHCP (Dynamic Host Configuration Protocol) snooping on the switch. DHCP snooping is a security feature that is used to prevent unauthorized DHCP servers from operating on a network. It works by allowing the switch to monitor and validate DHCP traffic on the network, ensuring that only legitimate DHCP messages are forwarded to clients. This can help to prevent incorrect IP addresses from being assigned to clients, as it ensures that only authorized DHCP servers are able to provide IP addresses to clients on the network.

NEW QUESTION 295

- (Exam Topic 3)

Which of the following is used to provide disaster recovery capabilities to spin up an critical devices using internet resources?

- A. Cloud site
- B. Hot site
- C. Cold site
- D. Warm site

Answer: A

NEW QUESTION 300

- (Exam Topic 3)

A new company recently moved into an empty office space Within days, users in the next office began noticing increased latency and packet drops with their Wi-Fi-connected devices. Which of the following is the MOST likely reason for this issue?

- A. Channel overlap
- B. Distance from the AP
- C. Bandwidth latency
- D. RF attenuation
- E. Network congestion

Answer: A

NEW QUESTION 302

- (Exam Topic 3)

A network technician receives a report about a performance issue on a client PC that is connected to port 1/3 on a network switch. The technician observes the following configuration output from the switch:

1/1	Client PC	Connected	Full	1000
1/2	Client PC	Connected	Full	1000
1/3	Client PC	Connected	Full	10

Which of the following is a cause of the issue on port 1/3?

- A. Speed
- B. Duplex
- C. Errors
- D. VLAN

Answer: A

NEW QUESTION 303

- (Exam Topic 3)

A network engineer is investigating reports of poor performance on a videoconferencing application. Upon reviewing the report, the engineer finds that available bandwidth at the WAN connection is low.

Which Of the following is the MOST appropriate mechanism to handle this issue?

- A. Traffic shaping
- B. Flow control
- C. NetFlow
- D. Link aggregation

Answer: A

Explanation:

Traffic shaping is a congestion management method that regulates network data transfer by delaying the flow of less important or less desired packets¹. Traffic shaping can help to improve the performance of a videoconferencing application by prioritizing its packets over other types of traffic and smoothing out traffic bursts. Traffic shaping can also help to avoid packet loss and ensure fair allocation of bandwidth among different applications or users.

Flow control is a mechanism that prevents a sender from overwhelming a receiver with more data than it can handle. Flow control can help to avoid buffer overflow and data loss, but it does not prioritize different types of traffic or smooth out traffic bursts. Flow control operates at the data link layer or the transport layer, while traffic shaping operates at the network layer or above.

NetFlow is a protocol that collects and analyzes network traffic data for monitoring and troubleshooting purposes². NetFlow can help to identify the sources, destinations, volumes, and types of traffic on a network, but it does not regulate or shape the traffic flow. NetFlow operates at the network layer or above.

Link aggregation is a technique that combines multiple physical links into one logical link for increased bandwidth, redundancy, and load balancing. Link aggregation can help to improve the performance of a videoconferencing application by providing more available bandwidth at the WAN connection, but it does not prioritize different types of traffic or smooth out traffic bursts. Link aggregation operates at the data link layer.

NEW QUESTION 305

- (Exam Topic 3)

An IT technician needs to increase bandwidth to a server. The server has multiple gigabit ports. Which of the following can be used to accomplish this without replacing hardware?

- A. STP
- B. 802.1Q
- C. Duplex
- D. LACP

Answer: D

Explanation:

LACP stands for Link Aggregation Control Protocol and is a protocol that allows multiple physical ports to be combined into a single logical port. This can increase bandwidth, redundancy, and load balancing for a server. LACP is part of the IEEE 802.3ad standard for link aggregation. STP stands for Spanning Tree Protocol and is a protocol that prevents loops in a network by blocking redundant links. 802.1Q is a standard for VLAN (Virtual Local Area Network) tagging, which allows multiple logical networks to share the same physical infrastructure. Duplex is a mode of communication that determines how data is transmitted and received on a link. Full duplex allows simultaneous transmission and reception, while half duplex allows only one direction at a time.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.5: Compare and contrast network cabling types, standards and speeds.

NEW QUESTION 307

- (Exam Topic 3)

Which of the following protocols is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links?

- A. OSPF
- B. RIPv2
- C. QoS
- D. STP

Answer: A

NEW QUESTION 308

- (Exam Topic 3)

A network technician needs to select an AP that will support at least 1.3Gbps and 5GHz only. Which of the following wireless standards must the AP support to meet the requirements?

- A. B
- B. AC
- C. AX
- D. N
- E. G

Answer: B

Explanation:

Wireless AC is a wireless standard that supports up to 1.3Gbps data rate and operates in the 5GHz frequency band only. Wireless AC is also backward compatible with wireless A and N devices that use the 5GHz band. Wireless AC is suitable for high-performance applications such as HD video streaming and online gaming. References: Network+ Study Guide Objective 2.2: Explain the purposes and properties of routing and switching. Subobjective: Wireless standards and their characteristics.

NEW QUESTION 310

- (Exam Topic 3)

A technician is trying to determine whether an LACP bundle is fully operational. Which of the following commands will the technician MOST likely use?

- A. show interface
- B. show config
- C. how route
- D. show arp

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/optical/cpt/r9_3/command/reference/cpt93_cr/cpt93_cr_chapter_01000.h

NEW QUESTION 311

- (Exam Topic 3)

A company wants to add a local redundant data center to its network in case of failure at its primary location. Which of the following would give the LEAST amount of redundancy for the company's network?

- A. Cold site
- B. Hot site
- C. Cloud site
- D. Warm site

Answer: A

NEW QUESTION 315

- (Exam Topic 3)

ARP spoofing would normally be a part of:

- A. an on-path attack.
- B. DNS poisoning.
- C. a DoS attack.
- D. a rogue access point.

Answer: A

NEW QUESTION 316

- (Exam Topic 3)

A network technician is selecting a replacement for a damaged fiber cable that goes directly to an SFP transceiver on a network switch. Which of the following cable connectors should be used?

- A. RJ45
- B. LC
- C. MT
- D. F-type

Answer: C

NEW QUESTION 318

- (Exam Topic 3)

Which of the following is an advanced distance vector routing protocol that automates routing tables and also uses some features of link-state routing protocols?

- A. OSPF
- B. RIP
- C. EIGRP
- D. BGP

Answer: C

Explanation:

EIGRP is an advanced distance vector routing protocol that is able to automatically update routing tables and also uses features of link-state routing protocols, such as the ability to send updates about the current topology of the network. EIGRP also has the ability to use a variety of algorithms to determine the best route for a packet to take, allowing for more efficient routing across the network.

NEW QUESTION 321

- (Exam Topic 3)

A network technician recently installed 35 additional workstations. After installation, some users are unable to access network resources. Many of the original workstations that are experiencing the network access issue were offline when the new workstations were turned on. Which of the following is the MOST likely cause of this issue?

- A. Incorrect VLAN setting
- B. Insufficient DHCP scope
- C. Improper NIC setting
- D. Duplicate IP address

Answer: B

NEW QUESTION 326

- (Exam Topic 3)

A network technician is working at a new office location and needs to connect one laptop to another to transfer files. The laptops are newer models and do not have Ethernet ports. Access points are not available either. Which Of the following types Of wireless network SSIDs does the network technician need to configure to be able to connect the laptops together?

- A. Independent Basic Service Set
- B. Extended Service Set
- C. Distribution System Service
- D. Basic Service Set

Answer: A

Explanation:

An Independent Basic Service Set (IBSS) is a type of wireless network that does not require an access point or a wired network. An IBSS allows wireless devices to communicate directly with each other using ad hoc mode. An IBSS is also known as an ad hoc network or a peer-to-peer network. A network technician can configure an IBSS to connect two laptops together and transfer files.

References: Network+ Study Guide Objective 1.4: Explain the properties and characteristics of TCP/IP

NEW QUESTION 330

- (Exam Topic 3)

A network administrator wants to test the throughput of a new metro Ethernet circuit to verify that its performance matches the requirements specified in the SLA. Which of the following would BEST help measure the throughput?

- A. iPerf
- B. Ping
- C. NetFlow
- D. Netstat

Answer: A

NEW QUESTION 334

- (Exam Topic 3)

An administrator would like to allow Windows clients from outside the office to access workstations without using third-party software. Which of the following access methods would meet this requirement?

- A. Remote desktop gateway
- B. Split tunnel
- C. Site-to-site VPN
- D. VNC

Answer: A

Explanation:

To allow Windows clients from outside the office to access workstations without using third-party software, the administrator can use the Remote Desktop Protocol (RDP). RDP is a built-in feature of the Windows operating system that allows users to remotely connect to and control other Windows computers over a network connection.

To use RDP, the administrator will need to enable the Remote Desktop feature on the workstations that need to be accessed, and ensure that the appropriate firewall rules are in place to allow RDP traffic to pass through. The administrator will also need to provide the remote users with the necessary credentials to access the workstations.

Once RDP is set up and configured, the remote users can use the Remote Desktop client on their own computers to connect to the workstations and access them as if they were physically present in the office. This allows the administrator to provide remote access to the workstations without the need for any additional software or third-party tools.

NEW QUESTION 338

- (Exam Topic 3)

An international company is transferring its IT assets including a number of WAPs from the United States to an office in Europe for deployment. Which of the following considerations should the company research

before implementing the wireless hardware?

- A. WPA2 cipher
- B. Regulatory Impacts
- C. CDMA configuration
- D. 802.11 standards

Answer: B

Explanation:

When transferring IT assets, including wireless access points (WAPs), from one country to another, it's important to research the regulatory impacts of the move. Different countries have different regulations and compliance requirements for wireless devices, such as frequency bands, power levels, and encryption standards. Failing to comply with these regulations can result in fines or other penalties.

NEW QUESTION 341

- (Exam Topic 3)

A network engineer needs to create a subnet that has the capacity for five VLANs. with the following number of clients to be allowed on each:

VLAN 10	50 users
VLAN 20	35 users
VLAN 30	20 users
VLAN 40	75 users
VLAN 50	130 users

Which of the following is the SMALLEST subnet capable of this setup that also has the capacity to double the number of clients in the future?

- A. 10.0.0.0/21
- B. 10.0.0.0/22
- C. 10.0.0.0/23
- D. 10.0.0.0/24

Answer: B

NEW QUESTION 344

- (Exam Topic 3)

An employee working in a warehouse facility is experiencing interruptions in mobile applications while walking around the facility. According to a recent site survey, the WLAN comprises autonomous APs that are directly connected to the internet, providing adequate signal coverage. Which of the following is the BEST solution to improve network stability?

- A. Implement client roaming using an extended service deployment employing a wireless controller.
- B. Remove omnidirectional antennas and adopt a directional bridge.
- C. Ensure all APs of the warehouse support MIMO and Wi-Fi 4.
- D. Verify that the level of EIRP power settings is set to the maximum permitted by regulations.

Answer: A

Explanation:

Client roaming refers to the ability of a wireless device to seamlessly connect to a different access point (AP) as the user moves around the facility. This can help to improve network stability and reduce interruptions in mobile applications. An extended service deployment is a type of wireless network configuration that uses multiple APs to cover a large area, such as a warehouse facility. By using a wireless controller to manage the APs, the network can be better optimized for client roaming, which can improve network stability.

"Roaming With multiple WAPs in an ESS, clients will connect to whichever WAP has the strongest signal. As clients move through the space covered by the broadcast area, they will change WAP connections seamlessly, a process called roaming."

NEW QUESTION 347

- (Exam Topic 3)

While walking from the parking lot to an access-controlled door an employee sees an authorized user open the door. Then the employee notices that another person catches the door before it closes and goes inside Which of the following attacks is taking place?

- A. Tailgating
- B. Piggybacking
- C. Shoulder surfing
- D. Phishing

Answer: A

Explanation:

The difference between piggybacking and tailgating is that with piggybacking, the person is willfully and intentionally letting you in. In this particular case, the person caught the door before it closed, so it is tailgating.

Tailgating is a physical security attack that occurs when an unauthorized person follows an authorized person through a secured door or gate without their knowledge or consent. Tailgating can allow an attacker to bypass access control mechanisms and gain entry to restricted areas or resources. Tailgating can also pose a safety risk for the authorized person and other occupants of the facility.

Piggybacking is a physical security attack that occurs when an unauthorized person follows an authorized person through a secured door or gate with their knowledge or consent. Piggybacking can also allow an attacker to bypass access control mechanisms and gain entry to restricted areas or resources. Piggybacking can also violate security policies and compromise the accountability of the authorized person.

Shoulder surfing is a physical security attack that occurs when an unauthorized person observes or records an authorized person's confidential information, such as passwords, PINs, or credit card numbers. Shoulder surfing can allow an attacker to steal credentials and access sensitive data or systems. Shoulder surfing can also violate privacy and confidentiality rights of the authorized person.

Phishing is a cyber security attack that occurs when an unauthorized person sends fraudulent emails or messages that appear to come from legitimate sources, such as banks, companies, or government agencies. Phishing can trick recipients into clicking on malicious links, opening malicious attachments, or providing

personal or financial information. Phishing can allow an attacker to install malware, steal credentials, or perform identity theft. Phishing does not involve physical access to secured doors or gates.

NEW QUESTION 352

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

N10-009 Practice Exam Features:

- * N10-009 Questions and Answers Updated Frequently
- * N10-009 Practice Questions Verified by Expert Senior Certified Staff
- * N10-009 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * N10-009 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The N10-009 Practice Test Here](#)