



# CompTIA

## Exam Questions N10-009

CompTIA Network+ Exam

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Guarantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

- (Exam Topic 1)

An administrator is writing a script to periodically log the IPv6 and MAC addresses of all the devices on a network segment. Which of the following switch features will MOST likely be used to assist with this task?

- A. Spanning Tree Protocol
- B. Neighbor Discovery Protocol
- C. Link Aggregation Control Protocol
- D. Address Resolution Protocol

**Answer:** B

#### Explanation:

Short explanation

The switch feature that is most likely to be used to assist with logging IPv6 and MAC addresses of devices on a network segment is Neighbor Discovery Protocol (NDP). NDP is used by IPv6 to discover and maintain information about other nodes on the network, including their IPv6 and MAC addresses. By periodically querying NDP, the administrator can log this information for auditing purposes.

References:

> CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.1: Compare and contrast TCP and UDP ports, protocols, and their purposes.

### NEW QUESTION 2

- (Exam Topic 1)

Which of the following is used to prioritize Internet usage per application and per user on the network?

- A. Bandwidth management
- B. Load balance routing
- C. Border Gateway Protocol
- D. Administrative distance

**Answer:** A

#### Explanation:

Bandwidth management is used to prioritize Internet usage per application and per user on the network. This allows an organization to allocate network resources to mission-critical applications and users, while limiting the bandwidth available to non-business-critical applications. References: Network+ Certification Study Guide, Chapter 2: Network Operations

### NEW QUESTION 3

- (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 4

- (Exam Topic 1)

A network administrator is installing a wireless network at a client's office. Which of the following IEEE 802.11 standards would be BEST to use for multiple simultaneous client access?

- A. CDMA
- B. CSMA/CD
- C. CSMA/CA
- D. GSM

**Answer:** C

#### Explanation:

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is an IEEE 802.11 standard that would be best to use for multiple simultaneous client access on a wireless network. CSMA/CA is a media access control method that allows multiple devices to share the same wireless channel without causing collisions or interference. It works by having each device sense the channel before transmitting data and waiting for an acknowledgment from the receiver after each transmission. If the channel is busy or no acknowledgment is received, the device will back off and retry later with a random delay. References:

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-csma-ca.html>

### NEW QUESTION 5

- (Exam Topic 1)

A technician is installing a new fiber connection to a network device in a datacenter. The connection from the device to the switch also traverses a patch panel

connection. The chain of connections is in the following order:

- Device
- LC/LC patch cable Patch panel
- Cross-connect fiber cable Patch panel
- LC/LC patch cable Switch

The connection is not working. The technician has changed both patch cables with known working patch cables. The device had been tested and was working properly before being installed. Which of the following is the MOST likely cause of the issue?

- A. TX/RX is reversed
- B. An incorrect cable was used
- C. The device failed during installation
- D. Attenuation is occurring

**Answer: A**

**Explanation:**

The most likely cause of the issue where the fiber connection from a device to a switch is not working is that the TX/RX (transmit/receive) is reversed. When connecting fiber optic cables, it is important to ensure that the TX of one device is connected to the RX of the other device and vice versa. If the TX/RX is reversed, data cannot be transmitted successfully.

References:

> CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 5: Network Operations, Objective 5.1: Given a scenario, use appropriate documentation and diagrams to manage the network.

**NEW QUESTION 6**

- (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 7**

- (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 8**

- (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 9

- (Exam Topic 1)

Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPsec site-to-site connections?

- A. Layer 3 switch
- B. VPN headend
- C. Next-generation firewall
- D. Proxy server
- E. Intrusion prevention

**Answer: C**

#### Explanation:

Next-generation firewalls can provide content filtering and threat protection, and can manage multiple IPsec site-to-site connections. References: CompTIA Network+ Certification Study Guide, Chapter 5: Network Security.

#### NEW QUESTION 10

- (Exam Topic 1)

Which of the following ports is commonly used by VoIP phones?

- A. 20
- B. 143
- C. 445
- D. 5060

**Answer: D**

#### Explanation:

TCP/UDP port 5060 is commonly used by VoIP phones. It is the default port for SIP (Session Initiation Protocol), which is a signaling protocol that establishes, modifies, and terminates multimedia sessions over IP networks. SIP is widely used for VoIP applications such as voice and video calls. References: <https://www.voip-info.org/session-initiation-protocol/>

#### NEW QUESTION 10

- (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 11

- (Exam Topic 1)

Which of the following is the LARGEST MTU for a standard Ethernet frame?

- A. 1452
- B. 1492
- C. 1500
- D. 2304

**Answer: C**

#### Explanation:

The maximum transmission unit (MTU) is the largest size of a data packet that can be transmitted over a network. A standard Ethernet frame supports an MTU of 1500 bytes, which is the default value for most Ethernet networks. Larger MTUs are possible with jumbo frames, but they are not widely supported and may cause fragmentation or compatibility issues. 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://en.wikipedia.org/wiki/Maximum\\_transmission\\_unit](https://en.wikipedia.org/wiki/Maximum_transmission_unit)

#### NEW QUESTION 16

- (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 20**

- (Exam Topic 1)

A technician needs to configure a Linux computer for network monitoring. The technician has the following information:

Linux computer details:

Interface	IP address	MAC address
eth0	10.1.2.24	A1:B2:C3:F4:E5:D6

Switch mirror port details:

Interface	IP address	MAC address
eth1	10.1.2.3	A1:B2:C3:D4:E5:F6

After connecting the Linux computer to the mirror port on the switch, which of the following commands should the technician run on the Linux computer?

- A. `ifconfig eth0 promisc`
- B. `ifconfig eth1 up`
- C. `ifconfig eth0 10.1.2.3`
- D. `ifconfig eth1 hw ether A1:B2:C3:D4:E5:F6`

**Answer:** A

**Explanation:**

The `ifconfig eth0 promisc` command should be run on the Linux computer to enable promiscuous mode, which allows the computer to capture all network traffic passing through the switch mirror port. References: CompTIA Network+ Certification Study Guide, Chapter 7: Network Devices.

**NEW QUESTION 24**

- (Exam Topic 1)

A network device is configured to send critical events to a syslog server; however, the following alerts are not being received:

Severity 5 LINK-UPDOWN: Interface 1/1, changed state to down Severity 5 LINK-UPDOWN: Interface 1/3, changed state to down

Which of the following describes the reason why the events are not being received?

- A. The network device is not configured to log that level to the syslog server
- B. The network device was down and could not send the event
- C. The syslog server is not compatible with the network device
- D. The syslog server did not have the correct MIB loaded to receive the message

**Answer:** A

**Explanation:**

The reason why the alerts are not being received is that the network device is not configured to log that level to the syslog server. The severity level for the events may need to be adjusted in order for them to be sent to the syslog server. References: Network+ Certification Study Guide, Chapter 8: Network Troubleshooting

**NEW QUESTION 28**

- (Exam Topic 1)

A company hired a technician to find all the devices connected within a network. Which of the following software tools would BEST assist the technician in completing this task?

- A. IP scanner
- B. Terminal emulator
- C. NetFlow analyzer
- D. Port scanner

**Answer:** A

**Explanation:**

To find all devices connected within a network, a technician can use an IP scanner. An IP scanner sends a ping request to all IP addresses within a specified range and then identifies the active devices that respond to the request.

**NEW QUESTION 29**

- (Exam Topic 1)

Which of the following is the physical topology for an Ethernet LAN?

- A. Bus
- B. Ring

- C. Mesh
- D. Star

**Answer:** D

**Explanation:**

In a star topology, all devices on a network connect to a central hub or switch, which acts as a common connection point. Ethernet LANs typically use a star topology, with each device connected to a central switch. References:

➤ Network+ N10-008 Objectives: 2.2 Explain common logical network topologies and their characteristics.

**NEW QUESTION 33**

- (Exam Topic 1)

A network administrator walks into a datacenter and notices an unknown person is following closely. The administrator stops and directs the person to the security desk. Which of the following attacks did the network administrator prevent?

- A. Evil twin
- B. Tailgating
- C. Piggybacking
- D. Shoulder surfing

**Answer:** B

**Explanation:**

:

Tailgating is a physical security attack where an unauthorized person follows an authorized person into a restricted area without proper identification or authorization. The network administrator prevented this attack by stopping and directing the person to the security desk. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 3.0 Network Security, Objective 3.1 Compare and contrast risk-related concepts.

**NEW QUESTION 35**

- (Exam Topic 1)

Which of the following factors should be considered when evaluating a firewall to protect a datacenter's east-west traffic?

- A. Replication traffic between an on-premises server and a remote backup facility
- B. Traffic between VMs running on different hosts
- C. Concurrent connections generated by Internet DDoS attacks
- D. VPN traffic from remote offices to the datacenter's VMs

**Answer:** B

**Explanation:**

When evaluating a firewall to protect a datacenter's east-west traffic, it is important to consider traffic between VMs running on different hosts. This type of traffic is referred to as east-west traffic and is often protected by internal firewalls. By implementing firewalls, an organization can protect their internal network against threats such as lateral movement, which can be caused by attackers who have breached a perimeter firewall. References: Network+ Certification Study Guide, Chapter 5: Network Security

**NEW QUESTION 40**

- (Exam Topic 1)

Which of the following is MOST likely to generate significant East-West traffic in a datacenter?

- A. A backup of a large video presentation to cloud storage for archival purposes
- B. A duplication of a hosted virtual server to another physical server for redundancy
- C. A download of navigation data to a portable device for offline access
- D. A query from an IoT device to a cloud-hosted server for a firmware update

**Answer:** B

**Explanation:**

East-West traffic refers to data flows between servers or devices within the same datacenter. When a hosted virtual server is duplicated to another physical server for redundancy, it generates significant East-West traffic as the data is replicated between the two servers. References:

➤ Network+ N10-008 Objectives: 3.3 Given a scenario, implement secure network architecture concepts.

**NEW QUESTION 44**

- (Exam Topic 1)

Which of the following service models would MOST likely be used to replace on-premises servers with a cloud solution?

- A. PaaS
- B. IaaS
- C. SaaS
- D. Disaster recovery as a Service (DRaaS)

**Answer:** B

**Explanation:**

IaaS stands for Infrastructure as a Service, which is a cloud service model that provides virtualized computing resources over the Internet, such as servers, storage, networking, and operating systems. IaaS allows customers to replace their on-premises servers with cloud servers that can be scaled up or down on demand and pay only for what they use. PaaS stands for Platform as a Service, which provides customers with a cloud-based platform for developing, testing, and deploying applications without managing the underlying infrastructure. SaaS stands for Software as a Service, which provides customers with access to cloud-based software applications over the Internet without installing or maintaining them on their devices. Disaster recovery as a Service (DRaaS) is a type of cloud

service that provides customers with backup and recovery solutions for their data and applications in case of a disaster.

**NEW QUESTION 45**

- (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 49**

- (Exam Topic 1)

You are tasked with verifying the following requirements are met in order to ensure network security. Requirements:

Datacenter

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic Building A

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide devices to support 5 additional different office users

Add an additional mobile user

Replace the Telnet Server with a more secure solution Screened subnet

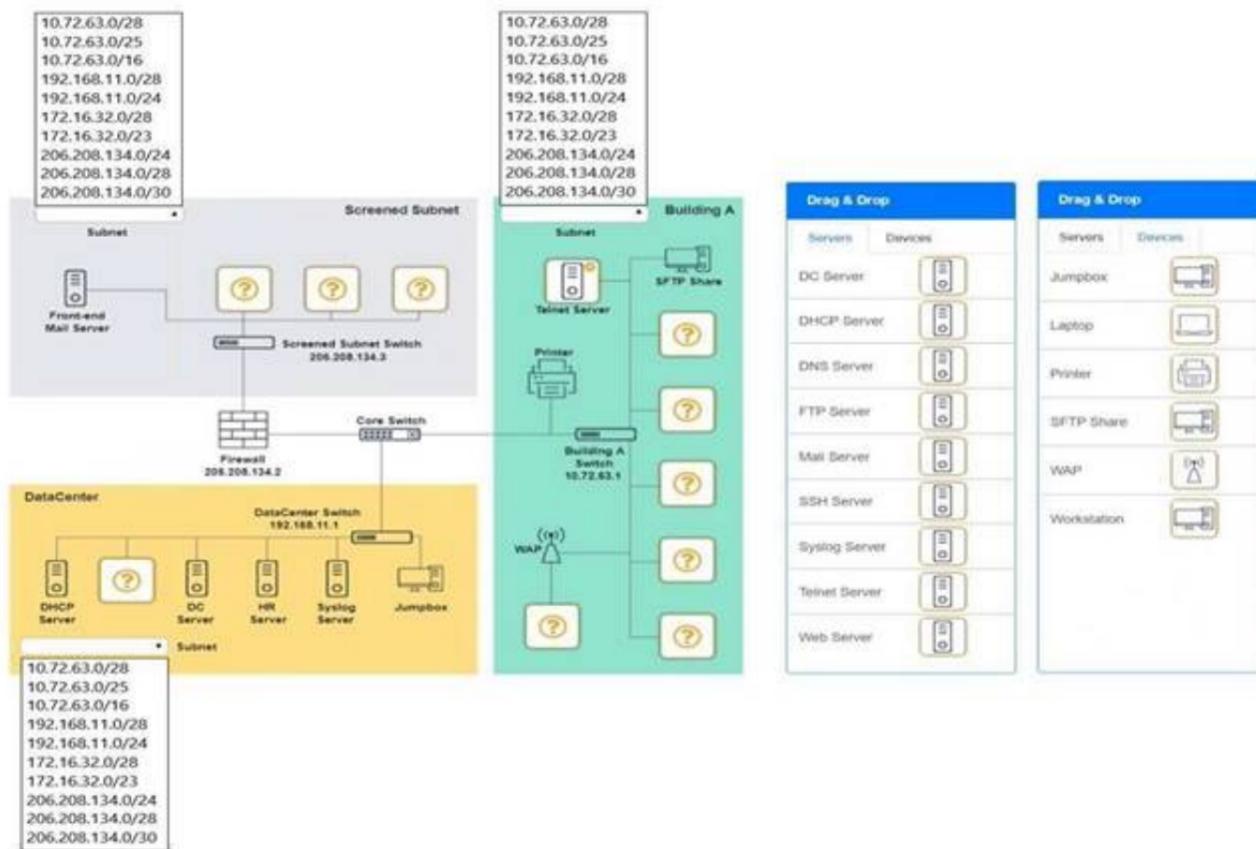
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide a server to handle external 80/443 traffic Provide a server to handle port 20/21 traffic INSTRUCTIONS

Drag and drop objects onto the appropriate locations. Objects can be used multiple times and not all placeholders need to be filled.

Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.

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



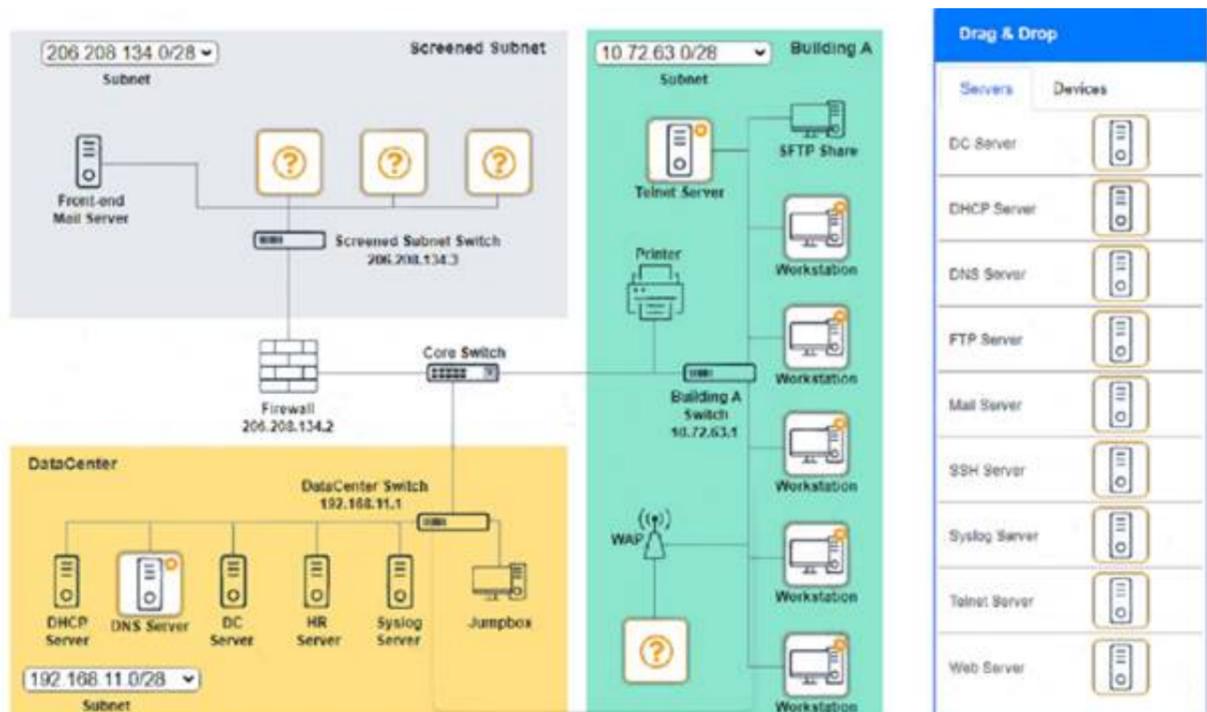
- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Screened Subnet devices – Web server, FTP server

Building A devices – SSH server top left, workstations on all 5 on the right, laptop on bottom left DataCenter devices – DNS server.



**NEW QUESTION 52**

- (Exam Topic 1)

The following configuration is applied to a DHCP server connected to a VPN concentrator:

```
IP address:      10.0.0.1
Subnet mask:    255.255.255.0
Gateway:       10.0.0.254
```

There are 300 non-concurrent sales representatives who log in for one hour a day to upload reports, and 252 of these representatives are able to connect to the VPN without any Issues. The remaining sales representatives cannot connect to the VPN over the course of the day. Which of the following can be done to resolve the issue without utilizing additional resources?

- A. Decrease the lease duration
- B. Reboot the DHCP server
- C. Install a new VPN concentrator
- D. Configure a new router

**Answer: A**

**Explanation:**

Decreasing the lease duration on the DHCP server will cause clients to renew their IP address leases more frequently, freeing up IP addresses for other clients to use. References: CompTIA Network+ Certification Study Guide, Chapter 3: IP Addressing.

**NEW QUESTION 56**

- (Exam Topic 2)

Which of the following uses the destination IP address to forward packets?

- A. A bridge
- B. A Layer 2 switch
- C. A router
- D. A repeater

**Answer: C**

**Explanation:**

A router is a device that uses the destination IP address to forward packets between different networks. A bridge and a Layer 2 switch operate at the data link layer and use MAC addresses to forward frames within the same network. A repeater is a device that amplifies or regenerates signals at the physical layer.

**NEW QUESTION 59**

- (Exam Topic 2)

A network technician is observing the behavior of an unmanaged switch when a new device is added to the network and transmits data. Which of the following BEST describes how the switch processes this information?

- A. The data is flooded out of every port including the one on which it came in.
- B. including the one on which it came in.
- C. The data is flooded out of every port but only in the VLAN where it is located.
- D. The data is flooded out of every port, except the one on which it came in
- E. The data is flooded out of every port, excluding the VLAN where it is located

**Answer: C**

**Explanation:**

The switch processes the data by flooding it out of every port, except the one on which it came in. Flooding is a process where a switch sends a data frame to all ports except the source port when it does not have an entry for the destination MAC address in its MAC address table. Flooding allows the switch to learn the MAC addresses of the devices connected to its ports and update its MAC address table accordingly. Flooding also ensures that the data frame reaches its intended destination, even if the switch does not know its location. References: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree->

protocol/10556-16.html

### NEW QUESTION 61

- (Exam Topic 2)

A network technician is reviewing an upcoming project's requirements to implement IaaS. Which of the following should the technician consider?

- A. Software installation processes
- B. Type of database to be installed
- C. Operating system maintenance
- D. Server hardware requirements

**Answer: D**

#### Explanation:

IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources such as servers, storage, and networking over the Internet. When implementing IaaS, the network technician should consider the server hardware requirements, such as CPU, RAM, disk space, and network bandwidth, that are needed to run the applications and services on the cloud. The other options are not relevant to IaaS, as they are either handled by the cloud provider or by the end-user. References: <https://www.comptia.org/blog/what-is-iaas>

### NEW QUESTION 63

- (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 65

- (Exam Topic 2)

A network administrator is downloading a large patch that will be uploaded to several enterprise switches simultaneously during the day's upgrade cycle. Which of the following should the administrator do to help ensure the upgrade process will be less likely to cause problems with the switches?

- A. Confirm the patch's MD5 hash prior to the upgrade
- B. Schedule the switches to reboot after an appropriate amount of time.
- C. Download each switch's current configuration before the upgrade
- D. Utilize FTP rather than TFTP to upload the patch

**Answer: A**

#### Explanation:

The network administrator should confirm the patch's MD5 hash prior to the upgrade to help ensure the upgrade process will be less likely to cause problems with the switches. MD5 (Message Digest 5) is a cryptographic hash function that produces a 128-bit hash value for any given input. It can be used to verify the integrity and authenticity of a file by comparing its hash value with a known or expected value. If the hash values match, it means that the file has not been corrupted or tampered with during transmission or storage. If the hash values do not match, it means that the file may be damaged or malicious and should not be used for the upgrade. References:

<https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/15292-scp.html>

### NEW QUESTION 70

- (Exam Topic 2)

There are two managed legacy switches running that cannot be replaced or upgraded. These switches do not support cryptographic functions, but they are password protected. Which of the following should a network administrator configure to BEST prevent unauthorized access?

- A. Enable a management access list
- B. Disable access to unnecessary services.
- C. Configure a stronger password for access
- D. Disable access to remote management
- E. Use an out-of-band access method.

**Answer: E**

#### Explanation:

Using an out-of-band access method is the best way to prevent unauthorized access to the legacy switches that do not support cryptographic functions. Out-of-band access is a method of accessing a network device through a dedicated channel that is separate from the main network traffic. Out-of-band access can use physical connections such as serial console ports or dial-up modems, or logical connections such as VPNs or firewalls. Out-of-band access provides more security and reliability than in-band access, which uses the same network as the data traffic and may be vulnerable to attacks or failures. References:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15mt/fundamentals-15-mt-book/>

#### NEW QUESTION 72

- (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 74

- (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 76

- (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 77

- (Exam Topic 2)

A network administrator is talking to different vendors about acquiring technology to support a new project for a large company. Which of the following documents will MOST likely need to be signed before information about the project is shared?

- A. BYOD policy
- B. NDA
- C. SLA
- D. MOU

**Answer: B**

#### Explanation:

NDA stands for Non-Disclosure Agreement, which is a legal contract between two or more parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to by others. A network administrator may need to sign an NDA before sharing information about a new project with different vendors, as the project may involve sensitive or proprietary data that the company wants to protect from competitors or unauthorized use. References: <https://www.adobe.com/sign/esignature-resources/sign-nda.html>

#### NEW QUESTION 79

- (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 84**

- (Exam Topic 2)

A network technician is investigating an issue with a desktop that is not connecting to the network. The desktop was connecting successfully the previous day, and no changes were made to the environment. The technician locates the switchport where the device is connected and observes the LED status light on the switchport is not lit even though the desktop is turned on. Other devices that are plugged into the switch are connecting to the network successfully. Which of the following is MOST likely the cause of the desktop not connecting?

- A. Transceiver mismatch
- B. VLAN mismatch
- C. Port security
- D. Damaged cable
- E. Duplex mismatch

**Answer: D**

**Explanation:**

A damaged cable is most likely the cause of the desktop not connecting to the network. A damaged cable can cause physical layer issues such as loss of signal, attenuation, interference, or crosstalk. These issues can prevent the desktop from establishing a link with the switch and result in the LED status light on the switchport being off. Other possible causes of physical layer issues are faulty connectors, ports, or transceivers. References:

<https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/14119-37.html>

**NEW QUESTION 86**

- (Exam Topic 2)

A company is being acquired by a large corporation. As part of the acquisition process, the company's address should now redirect clients to the corporate organization page. Which of the following DNS records needs to be created?

- A. SOA
- B. NS
- C. CNAME
- D. TXT

**Answer: C**

**Explanation:**

Reference:

<https://www.namecheap.com/support/knowledgebase/article.aspx/9604/2237/types-of-domain-redirects-301-302>

CNAME (Canonical Name) is a type of DNS record that maps an alias name to another name, which can be either another alias or the canonical name of a host or domain. A CNAME record can be used to redirect clients from one domain name to another domain name, such as from the company's address to the corporate organization page. SOA (Start of Authority) is a type of DNS record that specifies authoritative information about a DNS zone, such as the primary name server, contact email address, serial number, refresh interval, etc., which does not redirect clients to another domain name. NS (Name Server) is a type of DNS record that specifies which name server is authoritative for a domain or subdomain, which does not redirect clients to another domain name. TXT (Text) is a type of DNS record that provides arbitrary text information about a domain or subdomain, such as SPF (Sender Policy Framework) records or DKIM (DomainKeys Identified Mail) records, which does not redirect clients to another domain name.

**NEW QUESTION 90**

- (Exam Topic 2)

An IDS was installed behind the edge firewall after a network was breached. The network was then breached again even though the IDS logged the attack. Which of the following should be used in place of these devices to prevent future attacks?

- A. A network tap
- B. A proxy server
- C. A UTM appliance
- D. A content filter

**Answer: C**

**Explanation:**

A UTM appliance stands for Unified Threat Management appliance, which is a device that combines multiple security functions into one solution. A UTM appliance can provide firewall, IDS/IPS, antivirus, VPN, web filtering, and other security features. A network technician can use a UTM appliance in place of an edge firewall and an IDS to prevent future attacks, as a UTM appliance can block malicious traffic and detect and respond to intrusions more effectively. References:

<https://www.comptia.org/blog/what-is-utm>

### NEW QUESTION 95

- (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 98

- (Exam Topic 2)

A network technician is configuring a new firewall for a company with the necessary access requirements to be allowed through the firewall. Which of the following would normally be applied as the LAST rule in the firewall?

- A. Secure SNMP
- B. Port security
- C. Implicit deny
- D. DHCP snooping

**Answer: C**

#### Explanation:

Implicit deny is a firewall rule that blocks all traffic that is not explicitly allowed by other rules. Implicit deny is usually applied as the last rule in the firewall to ensure that only the necessary access requirements are allowed through the firewall and that any unwanted or malicious traffic is rejected. Implicit deny can also provide a default security policy and a baseline for auditing and logging purposes.

Secure SNMP is a protocol that allows network devices to send event messages to a centralized server or console for logging and analysis. Secure SNMP can be used to monitor and manage the status, performance, and configuration of network devices. Secure SNMP can also help to detect and respond to potential problems or faults on the network. However, secure SNMP is not a firewall rule; it is a network management protocol.

Port security is a feature that allows a switch to restrict the devices that can connect to a specific port based on their MAC addresses. Port security can help to prevent unauthorized access, spoofing, or MAC flooding attacks on the switch. However, port security is not a firewall rule; it is a switch feature.

DHCP snooping is a feature that allows a switch to filter DHCP messages and prevent rogue DHCP servers from assigning IP addresses to devices on the network. DHCP snooping can help to prevent IP address conflicts, spoofing, or denial-of-service attacks on the network. However, DHCP snooping is not a firewall rule; it is a switch feature.

### NEW QUESTION 102

- (Exam Topic 2)

A client moving into a new office wants the IP network set up to accommodate 412 network-connected devices that are all on the same subnet. The subnet needs to be as small as possible. Which of the following subnet masks should be used to achieve the required result?

- A. 255.255.0.0
- B. 255.255.252.0
- C. 255.255.254.0
- D. 255.255.255.0

**Answer: B**

#### Explanation:

\* 255.255.252.1 is a subnet mask that allows for 1022 network-connected devices on the same subnet, which is the smallest subnet that can accommodate 412 devices. The subnet mask determines how many bits are used for the network portion and how many bits are used for the host portion of an IP address. A smaller subnet mask means more bits are used for the network portion and less bits are used for the host portion, which reduces the number of available hosts on the subnet. 255.255.0.0 allows for 65534 hosts on the same subnet, which is too large. 255.255.254.0 allows for 510 hosts on the same subnet, which is also too large. 255.255.255.0 allows for 254 hosts on the same subnet, which is too small.

### NEW QUESTION 103

- (Exam Topic 2)

A small, family-run business uses a single SOHO router to provide Internet and WiFi to its employees. At the start of a new week, employees come in and find their usual WiFi network is no longer available, and there is a new wireless network to which they cannot connect. Given that information, which of the following should have been done to avoid this situation?

- A. The device firmware should have been kept current.
- B. Unsecure protocols should have been disabled.
- C. Parental controls should have been enabled.
- D. The default credentials should have been changed.

**Answer: D**

#### Explanation:

The default credentials are the username and password that come with a device or service when it is first installed or configured. They are often easy to guess or find online, which makes them vulnerable to unauthorized access or attacks. The default credentials should be changed to something unique and strong as soon

as possible to avoid this situation. If the default credentials were not changed, someone could have accessed the SOHO router and changed the WiFi settings without the employees' knowledge. References: <https://www.comptia.org/blog/network-security-basics-6-easy-ways-to-protect-your-network>

#### NEW QUESTION 106

- (Exam Topic 3)

A technician is investigating a misconfiguration on a Layer 3 switch. When the technician logs in and runs a command, the following data is shown: Which of the following commands generated this output?

- A. show route
- B. show config
- C. show interface
- D. tcpdump
- E. netstat —s

**Answer: C**

#### Explanation:

The output shown in the image is from the show interface command, which displays information about the status and configuration of a network interface on a switch or router. The output includes the interface name, description, MAC address, IP address, speed, duplex mode, status, and statistics. The show route command displays the routing table of the device. The show config command displays the current configuration of the device. The tcpdump command captures and analyzes network traffic. The netstat -s command displays statistics for each protocol.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.4: Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

#### NEW QUESTION 109

- (Exam Topic 3)

Which of the following network devices can perform routing between VLANs?

- A. Layer 2 switch
- B. Layer 3 switch
- C. Load balancer
- D. Bridge

**Answer: B**

#### Explanation:

<https://www.practicalnetworking.net/stand-alone/routing-between-vlans/#:~:text=A%20router%20will%20perfo>

#### NEW QUESTION 112

- (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 117

- (Exam Topic 3)

Which of the following has the capability to centrally manage configuration, logging, and firmware versioning for distributed devices?

- A. WLAN controller
- B. Load balancer
- C. SIEM solution
- D. Syslog server

**Answer: A**

#### Explanation:

A WLAN controller is a device that manages and controls multiple wireless access points (WAPs) in a wireless LAN (WLAN). A WLAN controller has the capability to centrally manage configuration, logging, and firmware versioning for distributed WAPs. A WLAN controller can also provide load balancing, security, and quality of service (QoS) for the WLAN.

References: Network+ Study Guide Objective 3.1: Explain the purposes and use cases for advanced networking devices.

#### NEW QUESTION 121

- (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 123**

- (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 128**

- (Exam Topic 3)

An administrator is attempting to add a new system to monitoring but is unsuccessful. The administrator notices the system is similar to another one on the network; however, the new one has an updated OS version. Which of the following should the administrator consider updating?

- A. Management information bases
- B. System baseline
- C. Network device logs
- D. SNMP traps

**Answer:** A

**NEW QUESTION 131**

- (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 136**

- (Exam Topic 3)

An administrator needs to connect two laptops directly to each other using 802.11ac but does not have an AP available. Which of the following describes this configuration?

- A. Basic service set
- B. Extended service set
- C. Independent basic service set
- D. MU-MIMO

**Answer:** C

**NEW QUESTION 139**

- (Exam Topic 3)

Which of the following commands can be used to display the IP address, subnet address, gateway address, and DNS address on a Windows computer?

- A. netstat -a

- B. ifconfig
- C. ip addr
- D. ipconfig /all

**Answer:** D

**Explanation:**

The ipconfig command is a utility that allows you to view and modify the network configuration of a Windows computer. By running the command "ipconfig /all", you can view detailed information about the network configuration of your computer, including the IP address, subnet mask, default gateway, and DNS server addresses.

Option A (netstat -a) is a command that displays active network connections and their status, but it does not display IP address or other network configuration information. Option B (ifconfig) is a command used on Linux and Unix systems to view and modify network configuration, but it is not available on Windows. Option C (ip addr) is a command used on Linux and Unix systems to view and modify network configuration, but it is not available on Windows.

**NEW QUESTION 143**

- (Exam Topic 3)

Which of the following would be the MOST cost-effective recovery solution for a company's lower-priority applications?

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

**Answer:** C

**NEW QUESTION 146**

- (Exam Topic 3)

A network administrator installed an additional IDF during a building expansion project. Which of the following documents need to be updated to reflect the change? (Select TWO).

- A. Data loss prevention policy
- B. BYOD policy
- C. Acceptable use policy
- D. Non-disclosure agreement
- E. Disaster recovery plan
- F. Physical network diagram

**Answer:** BF

**NEW QUESTION 151**

- (Exam Topic 3)

A user reports that a new VoIP phone works properly but the computer that is connected to the phone cannot access any network resources. Which of the following MOST Likely needs to be configured correctly to provide network connectivity to the computer?

- A. Port duplex settings
- B. Port aggregation
- C. ARP settings
- D. VLAN tags
- E. MDIX settings

**Answer:** D

**Explanation:**

VLAN (virtual LAN) tags are used to identify packets as belonging to a particular VLAN. VLANs are used to segment a network into logical sub-networks, and each VLAN is assigned a unique VLAN tag. If the VLAN tag is not configured correctly, the computer may not be able to access network resources.

**NEW QUESTION 155**

- (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-568-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 159**

- (Exam Topic 3)

A network administrator would like to purchase a device that provides access ports to endpoints and has the ability to route between networks. Which of the following would be BEST for the administrator to purchase?

- A. An IPS
- B. A Layer 3 switch
- C. A router
- D. A wireless LAN controller

**Answer: B**

**NEW QUESTION 161**

- (Exam Topic 3)

A help desk technician is concerned that a client's network cable issues may be causing intermittent connectivity. Which of the following would help the technician determine if this is the issue?

- A. Run the show interface command on the switch
- B. Run the traceroute command on the server
- C. Run iperf on the technician's desktop
- D. Ping the client's computer from the router
- E. Run a port scanner on the client's IP address

**Answer: A**

**Explanation:**

To determine if a client's network cable issues may be causing intermittent connectivity, the help desk technician can run the show interface command on the switch. This command allows the technician to view the status and statistics of the various interfaces on the switch, including the physical link status and the number of transmitted and received packets. If the interface is experiencing a large number of errors or dropped packets, this could indicate a problem with the network cable or with the connection between the client's device and the switch.

"Cisco routers and switches have a show interfaces IOS command that provides interface statistics/status information, including link state (up/down), speed/duplex, send/receive traffic, cyclic redundancy checks (CRCs), and protocol packet and byte counts."

**NEW QUESTION 165**

- (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 an printer ports to VLAN 20.
- D. Enable all ports that are shut down on me stack.
- E. Reconfigure me VLAN on the printer ports on Switch 3.
- F. Enable wireless APs on Switch 3.

**Answer: AE**

**NEW QUESTION 170**

- (Exam Topic 3)

When accessing corporate network resources, users are required to authenticate to each application they try to access. Which of the following concepts does this BEST represent?

- A. SSO
- B. Zero Trust
- C. VPN
- D. Role-based access control

**Answer: B**

#### NEW QUESTION 172

- (Exam Topic 3)

A technician knows the MAC address of a device and is attempting to find the device's IP address. Which of the following should the technician look at to find the IP address? (Select TWO).

- A. ARP table
- B. DHCP leases
- C. IP route table
- D. DNS cache
- E. MAC address table
- F. STP topology

**Answer:** BE

#### NEW QUESTION 177

- (Exam Topic 3)

A user calls the IT department to report being unable to log in after locking the computer. The user resets the password, but later in the day the user is again unable to log in after locking the computer. Which of the following attacks against the user is MOST likely taking place?

- A. Brute-force
- B. On-path
- C. Deauthentication
- D. Phishing

**Answer:** A

#### NEW QUESTION 181

- (Exam Topic 3)

Which of the following would be the BEST choice to connect branch sites to a main office securely?

- A. VPN headend
- B. Proxy server
- C. Bridge
- D. Load balancer

**Answer:** A

#### Explanation:

Host-to-Site, or Client-to-Site, VPN allows for remote servers, clients, and other hosts to establish tunnels through a VPN gateway (or VPN headend) via a private network. The tunnel between the headend and the client host encapsulates and encrypts data.

#### NEW QUESTION 183

- (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 185

- (Exam Topic 3)

Which of the following bandwidth management techniques uses buffers at the client side to prevent TCP retransmissions from occurring when the ISP starts to drop packets of specific types that exceed the agreed traffic rate?

- A. Traffic shaping
- B. Traffic policing
- C. Traffic marking
- D. Traffic prioritization

**Answer:** D

#### NEW QUESTION 188

- (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 193

- (Exam Topic 3)

A large metropolitan city is looking to standardize the ability for police department laptops to connect to the city government's VPN. The city would like a wireless solution that provides the largest coverage across the city with a minimal number of transmission towers. Latency and overall bandwidth needs are not high priorities. Which of the following would BEST meet the city's needs?

- A. 5G
- B. LTE
- C. Wi-Fi 4
- D. Wi-Fi 5
- E. Wi-Fi 6

**Answer: B**

#### NEW QUESTION 194

- (Exam Topic 3)

Which of the following layers of the OSI model receives data from the application layer and converts it into syntax that is readable by other devices on the network?

- A. Layer 1
- B. Layer 3
- C. Layer 6
- D. Layer 7

**Answer: C**

#### NEW QUESTION 198

- (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 200

- (Exam Topic 3)

A network administrator is investigating reports about network performance and finds high utilization on a switch uplink. The administrator is unsure whether this is an anomaly or normal behavior that will require an upgrade to resolve. Which of the following should the administrator reference to gain historical perspective?

- A. Device configuration review
- B. ARP table export
- C. Service-level agreement
- D. Network performance baseline

**Answer: D**

#### Explanation:

A network performance baseline is a set of metrics that represents the normal or expected behavior of a network under various conditions and scenarios. A network performance baseline can help a network administrator to investigate reports about network performance by comparing the current metrics with the historical metrics and identifying any deviations or anomalies. A network performance baseline can also help to plan and justify network upgrades by showing the trends and patterns of network utilization and performance over time.

A device configuration review is a process that involves checking and verifying the settings and parameters of a network device, such as a switch, router, firewall, or server. A device configuration review can help a network administrator to troubleshoot network issues by finding and fixing any errors, inconsistencies, or vulnerabilities in the device configuration. A device configuration review can also help to ensure compliance with security policies and best practices by applying the latest updates and patches to the device.

An ARP table export is a file that contains the contents of the ARP (Address Resolution Protocol) table of a network device. The ARP table is a data structure that maps IP addresses to MAC addresses on a local network. An ARP table export can help a network administrator to monitor and manage the network devices on a local network by showing their IP addresses and MAC addresses. An ARP table export can also help to detect and prevent ARP spoofing attacks by identifying any duplicate or malicious entries in the ARP table.

A service-level agreement (SLA) is a contract that defines the expectations and responsibilities of both parties in terms of service quality, availability, performance, and response time. An SLA can help a network administrator to provide and maintain a satisfactory level of service to the customers or users of the network by setting and measuring specific goals and metrics. An SLA can also help to resolve any disputes or issues that may arise between the service provider and the

service consumer by establishing clear terms and conditions for the service delivery.

#### NEW QUESTION 204

- (Exam Topic 3)

A company's web server is hosted at a local ISP. This is an example of:

- A. allocation.
- B. an on-premises data center.
- C. a branch office.
- D. a cloud provider.

**Answer: D**

#### NEW QUESTION 207

- (Exam Topic 3)

Which of the following is used when a workstation sends a DHCP broadcast to a server on another LAN?

- A. Reservation
- B. Dynamic assignment
- C. Helper address
- D. DHCP offer

**Answer: C**

#### Explanation:

A helper address is an IP address that is configured on a router interface to forward DHCP broadcast messages to a DHCP server on another LAN. A DHCP broadcast message is a message that a workstation sends when it needs to obtain an IP address from a DHCP server. Since broadcast messages are not routed across different networks, a helper address is needed to relay the DHCP broadcast message to the DHCP server on another network. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 199)

#### NEW QUESTION 212

- (Exam Topic 3)

A building was recently remodeled in order to expand the front lobby. Some mobile users have been unable to connect to the available network jacks within the new lobby, while others have had no issues. Which of the following is the MOST likely cause of the connectivity issues?

- A. LACP
- B. Port security
- C. 802.11ax
- D. Duplex settings

**Answer: B**

#### Explanation:

Port security is a feature that allows a network device to limit the number and type of MAC addresses that can access a port. Port security can prevent unauthorized devices from connecting to the network through an available network jack. Therefore, port security is the most likely cause of the connectivity issues for some mobile users in the new lobby.

#### NEW QUESTION 214

- (Exam Topic 3)

Which of the following topologies is designed to fully support applications hosted in on-premises data centers, public or private clouds, and SaaS services?

- A. SDWAN
- B. MAN
- C. PAN
- D. MPLS

**Answer: A**

#### NEW QUESTION 217

- (Exam Topic 3)

Due to space constraints in an IDF, a network administrator can only do a single switch to accommodate three data networks. The administrator needs a configuration that will allow each device to access its expected network without additional connections. The configuration must also allow each device to access the rest of the network. Which of the following should the administrator do to meet these requirements? (Select TWO).

- A. Untag the three VLANs across the uplink
- B. Tag an individual VLAN across the uplink
- C. Untag an individual VLAN per device port
- D. Tag an individual VLAN per device port
- E. Tag the three VLANs across the uplink.
- F. Tag the three VLANs per device port.

**Answer: AC**

#### Explanation:

To achieve this, you should do two things:

➤ Tag the three VLANs across the uplink port that connects to another switch or router. This will allow data packets from different VLANs to cross over into other networks.

➤ Untag an individual VLAN per device port that connects to an end device. This will assign each device to its expected network without additional connections.

#### NEW QUESTION 220

- (Exam Topic 3)

A network engineer is concerned about VLAN hopping happening on the network. Which of the following should the engineer do to address this concern?

- A. Configure private VLANs.
- B. Change the default VLAN.
- C. Implement ACLs on the VLAN.
- D. Enable dynamic ARP inspection.

**Answer: B**

#### Explanation:

VLAN hopping is a type of attack that allows an attacker to access or manipulate traffic on a different VLAN than the one they are connected to. One way to prevent VLAN hopping is to change the default VLAN on a switch. The default VLAN is the VLAN that is assigned to all ports on a switch by default, usually VLAN 1. If an attacker connects to an unused port on a switch that has not been configured with a specific VLAN, they can access or spoof traffic on the default VLAN. By changing the default VLAN to an unused or isolated VLAN, the network administrator can prevent unauthorized access or interference with legitimate traffic on other VLANs. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 308)

#### NEW QUESTION 224

- (Exam Topic 3)

An ISP configured an internet connection to provide 20Mbps, but actual data rates are occurring at 10Mbps and causing a significant delay in data transmission. Which of the following specifications should the ISP check?

- A. Throughput
- B. Latency
- C. Bandwidth
- D. Jitter

**Answer: A**

#### Explanation:

Throughput is the actual amount of data that can be transferred over a network in a given time. Throughput can be affected by various factors such as congestion, interference, errors, or hardware limitations. If the throughput is lower than the configured internet connection speed, it can cause a significant delay in data transmission. The ISP should check the throughput and identify the source of the problem.

References: Network+ Study Guide Objective 2.2: Explain the concepts and characteristics of routing and switching.

#### NEW QUESTION 225

- (Exam Topic 3)

Which of the following would be used to forward requests and replies between a DHCP server and client?

- A. Relay
- B. Lease
- C. Scope
- D. Range

**Answer: A**

#### NEW QUESTION 226

- (Exam Topic 3)

A network engineer receives the following when connecting to a switch to configure a port:

```
telnet 10.1.200.1
Connecting to 10.1.200.1...Could not open connection to the host, on port 23: Connect failed.
```

Which of the following is the MOST likely cause for the failure?

- A. The network engineer is using the wrong protocol
- B. The network engineer does not have permission to configure the device
- C. SNMP has been secured with an ACL
- D. The switchport the engineer is trying to configure is down

**Answer: D**

#### NEW QUESTION 230

- (Exam Topic 3)

Which of the following types of attacks can be used to gain credentials by setting up rogue APs with identical corporate SSIDs?

- A. VLAN hopping
- B. Evil twin
- C. DNS poisoning
- D. Social engineering

**Answer: B**

#### NEW QUESTION 232

- (Exam Topic 3)

A user in a branch office reports that access to all files has been lost after receiving a new PC. All other users in the branch can access fileshares. The IT engineer who is troubleshooting this incident is able to ping the workstation from the branch router, but the machine cannot ping the router. Which of the following is MOST likely the cause of the incident?

- A. Incorrect subnet mask
- B. Incorrect DNS server
- C. Incorrect IP class
- D. Incorrect TCP port

**Answer:** A

#### NEW QUESTION 235

- (Exam Topic 3)

A consultant is working with two international companies. The companies will be sharing cloud resources for a project. Which of the following documents would provide an agreement on how to utilize the resources?

- A. MOU
- B. NDA
- C. AUP
- D. SLA

**Answer:** A

#### Explanation:

A memorandum of understanding (MOU) is a document that describes an agreement between two or more parties on how to utilize shared resources for a project. An MOU is not legally binding, but it outlines the expectations and responsibilities of each party involved in the collaboration. An MOU can be used when two international companies want to share cloud resources for a project without creating a formal contract. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 405)

#### NEW QUESTION 236

- (Exam Topic 3)

Which of the following issues are present with RIPv2? (Select TWO).

- A. Route poisoning
- B. Time to converge
- C. Scalability
- D. Unicast
- E. Adjacent neighbors
- F. Maximum transmission unit

**Answer:** BC

#### Explanation:

The disadvantages of RIP (Routing Information Protocol) include the following.

---Outdated, insecure, and slow. This is your parents' protocol. It was a thing before the Web was born.

---The more well-known problem of the 15 hop limitation in which data must travel

---Convergence time is terrible for information propagation in a network

---Metrics. It determines the number of hops from source to destination, and gives no regard to other factors when determining the best path for data to travel

---Overhead. A good example would be routing tables. These are broadcast at half-minute intervals to other routers regardless of whether the data has changed or not. It's essentially like those old cartoons where the

town guard in the walled city cries out, '10 o' the clock and all is well!'

RIPv2 introduced more security and reduced broadcast traffic, which is relevant for some available answers here.

#### NEW QUESTION 238

- (Exam Topic 3)

A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds hundreds of CRC errors on an interface. Which of the following is the MOST likely cause of these errors?

- A. A bad wire on the Cat 5e cable
- B. The wrong VLAN assignment to the switchport
- C. A misconfigured QoS setting on the router
- D. Both sides of the switch trunk set to full duplex

**Answer:** A

#### NEW QUESTION 240

- (Exam Topic 3)

Which of the following would be increased by adding encryption to data communication across the network?

- A. Availability
- B. Integrity
- C. Accountability
- D. Confidentiality

**Answer:** D

#### Explanation:

Confidentiality is the property of preventing unauthorized access or disclosure of data. Encryption is a method of transforming data into an unreadable format that can only be decrypted by authorized parties who have the correct key. Encryption can increase the confidentiality of data communication across the network by

making it harder for attackers to intercept or eavesdrop on the data. References: Network+ Study Guide Objective 4.1: Summarize the purposes of physical security devices. Subobjective: Encryption.

**NEW QUESTION 245**

- (Exam Topic 3)

Which of the following DHCP settings would be used to ensure a device gets the same IP address each time it is connected to the network?

- A. Scope options
- B. Reservation
- C. Exclusion
- D. Relay
- E. Pool

**Answer: A**

**NEW QUESTION 246**

- (Exam Topic 3)

Which of the following protocols uses Dijkstra's algorithm to calculate the LOWEST cost between routers?

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

**Answer: B**

**Explanation:**

OSPF stands for Open Shortest Path First and is a link-state routing protocol that uses Dijkstra's algorithm to calculate the lowest cost between routers. OSPF assigns a cost value to each link based on factors such as bandwidth, delay, or reliability, and builds a map of the network topology. OSPF then uses Dijkstra's algorithm to find the shortest path from each router to every other router in the network. RIP stands for Routing Information Protocol and is a distance-vector routing protocol that uses hop count as the metric to find the best path. BGP stands for Border Gateway Protocol and is a path-vector routing protocol that uses attributes such as AS path, local preference, or origin to select the best route. EIGRP stands for Enhanced Interior Gateway Routing Protocol and is a hybrid routing protocol that uses a composite metric based on bandwidth, delay, load, and reliability.

References: 1 Dijkstra's algorithm - Wikipedia ([https://en.wikipedia.org/wiki/Dijkstra%27s\\_algorithm](https://en.wikipedia.org/wiki/Dijkstra%27s_algorithm))

**NEW QUESTION 248**

- (Exam Topic 3)

Which of the following describes when an active exploit is used to gain access to a network?

- A. Penetration testing
- B. Vulnerability testing
- C. Risk assessment
- D. Posture assessment
- E. Baseline testing

**Answer: A**

**Explanation:**

Penetration testing is a type of security testing that is used to assess the security of a system or network by actively exploiting known vulnerabilities. It is used to simulate an attack on the system and identify any weaknesses that may be exploited by malicious actors. As stated in the CompTIA Security+ Study Guide, "penetration testing is a type of security assessment that attempts to gain unauthorized access to networks and systems by exploiting security vulnerabilities."

**NEW QUESTION 253**

- (Exam Topic 3)

A network technician receives a report from the server team that a server's network connection is not working correctly. The server team confirms the server is operating correctly except for the network connection. The technician checks the switchport connected to the server and reviews the following data;

Metric	Value
Bytes input	441,164,698
Bytes output	2,625,115,257
Runts	0
CRCs	5,489
Collisions	1
MDIX	On
Speed	1,000
Duplex	Full

Which of the following should the network technician perform to correct the issue?

- A. Replace the Cat 5 patch cable with a Cat 6 cable
- B. Install a crossover cable between the server and the switch
- C. Reset the switchport configuration.
- D. Use NetFlow data from the switch to isolate the issue.
- E. Disable MDIX on the switchport and reboot the server.

**Answer: A**

**Explanation:**

"Bad cables, incorrect pinouts, or bent pins: Faulty cables (with electrical characteristics preventing successful transmission) or faulty connectors (which do not properly make connections) can prevent successful data transmission at Layer 1. A bad cable could simply be an incorrect category of cable being used for a specific purpose. For example, using a Cat 5 cable (instead of a Cat 6 or higher cable) to connect two 1000BASE-TX devices would result in data corruption. Bent pins in a connector or incorrect pinouts could also cause data to become corrupted."

**NEW QUESTION 254**

- (Exam Topic 3)

Several users with older devices are reporting intermittent connectivity while in an outdoor patio area. After some research, the network administrator determines that an outdoor WAP might help with the issue. However, the company does not want the signal to bleed into the building and cause interference. Which of the following should the network administrator perform to BEST resolve the issue?

- A. Disable the SSID broadcast on the WAP in the patio area.
- B. Install a WAP and enable 5GHz only within the patio area.
- C. Install a directional WAP in the direction of the patio.
- D. Install a repeater on the back wall of the patio area.

**Answer:** C

**NEW QUESTION 258**

- (Exam Topic 3)

Which of the following would be used when connecting devices that have different physical characteristics?

- A. A proxy server
- B. An industrial control system
- C. A load balancer
- D. A media converter

**Answer:** D

**NEW QUESTION 262**

- (Exam Topic 3)

Which of the following is the IEEE link cost for a Fast Ethernet interface in STP calculations?

- A. 2
- B. 4
- C. 19
- D. 100

**Answer:** D

**Explanation:**

The IEEE standard for link cost for a Fast Ethernet interface is 100, and for a Gigabit Ethernet interface is 19. These values are based on the bandwidth of the interface, with lower values indicating a higher-bandwidth interface.

**NEW QUESTION 263**

- (Exam Topic 3)

A network engineer developed a plan of action to resolve an ongoing issue. Which of the following steps should the engineer take NEXT?

- A. Verify full system functionality and implement preventative measures.
- B. Implement the solution to resolve the problem.
- C. Document findings, actions, outcomes, and lessons learned.
- D. Establish a theory of probable cause.

**Answer:** B

**Explanation:**

Network troubleshooting is a repeatable process, which means that you can break it down into clear steps that anyone can follow. Identify the Problem. ... Develop a Theory. ... Test the Theory. ... Plan of Action. ...

Implement the Solution. ... Verify System Functionality. ... Document the Issue.

Theory of probable cause is before Plan of action. <https://www.comptia.org/content/guides/a-guide-to-network-troubleshooting>

**NEW QUESTION 265**

- (Exam Topic 3)

A company is designing a SAN and would like to use STP as its medium for communication. Which of the following protocols would BEST suit the company's needs?

- A. SFTP
- B. Fibre Channel
- C. iSCSI
- D. FTP

**Answer:** B

**Explanation:**

A SAN also employs a series of protocols enabling software to communicate or prepare data for storage. The most common protocol is the Fibre Channel Protocol (FCP), which maps SCSI commands over FC technology. The iSCSI SANs will employ an iSCSI protocol that maps SCSI commands over TCP/IP.

STP (Spanning Tree Protocol) is a protocol used to prevent loops in Ethernet networks, and it is not a medium for communication in a storage area network (SAN). However, Fibre Channel is a protocol that is specifically designed for high-speed data transfer in SAN environments. It is a dedicated channel technology that provides high throughput and low latency, making it ideal for SANs. Therefore, Fibre Channel would be the best protocol for the company to use for its SAN. SFTP (Secure File Transfer Protocol), iSCSI (Internet Small Computer System Interface), and FTP (File Transfer Protocol) are protocols used for transferring files over a network and are not suitable for use in a SAN environment.

#### NEW QUESTION 267

- (Exam Topic 3)

A network administrator is designing a wireless network. The administrator must ensure a rented office space has a sufficient signal. Reducing exposure to the wireless network is important, but it is secondary to the primary objective. Which of the following would MOST likely facilitate the correct accessibility to the Wi-Fi network?

- A. Polarization
- B. Channel utilization
- C. Channel bonding
- D. Antenna type
- E. MU-MIMO

**Answer:** B

#### NEW QUESTION 272

- (Exam Topic 3)

A newly installed multifunction copier needs to be set up so scanned documents can be emailed to recipients. Which of the following ports from the copier's IP address should be allowed?

- A. 22
- B. 25
- C. 53
- D. 80

**Answer:** B

#### Explanation:

Port 25 is the port number that is commonly used for Simple Mail Transfer Protocol (SMTP), which is a protocol that allows sending and receiving email messages over a network. Port 25 from the copier's IP address should be allowed so that scanned documents can be emailed to recipients.

Port 22 is the port number that is commonly used for Secure Shell (SSH), which is a protocol that allows secure and encrypted remote access and control of a device over a network. Port 22 from the copier's IP address is not necessary for emailing scanned documents.

Port 53 is the port number that is commonly used for Domain Name System (DNS), which is a protocol that allows resolving domain names to IP addresses and vice versa on a network. Port 53 from the copier's IP address is not necessary for emailing scanned documents.

Port 80 is the port number that is commonly used for Hypertext Transfer Protocol (HTTP), which is a protocol that allows transferring web pages and other resources over a network. Port 80 from the copier's IP address is not necessary for emailing scanned documents.

#### NEW QUESTION 273

- (Exam Topic 3)

An IT administrator received an assignment with the following objectives

- Conduct a total scan within the company's network for all connected hosts
- Detect all the types of operating systems running on all devices
- Discover all services offered by hosts on the network
- Find open ports and detect security risks.

Which of the following command-line tools can be used to achieve these objectives?

- A. nmap
- B. arp
- C. netat
- D. tcpdump

**Answer:** A

#### Explanation:

Nmap (Network Mapper) is a free and open source command line tool that can be used to scan a network for all connected hosts, detect the types of operating systems running on all devices, discover all services offered by hosts on the network, find open ports, and detect security risks. Nmap is commonly used by system administrators and security professionals to audit a network's security and identify possible vulnerabilities. Nmap can be used to discover active hosts, scan ports, fingerprint operating systems, detect running services, and more. Reference: CompTIA Network+ Study Manual, 8th Edition, page 592.

#### NEW QUESTION 276

- (Exam Topic 3)

A network administrator is given the network 80.87.78.0/26 for specific device assignments. Which of the following describes this network?

- A. 80.87.78.0 - 80.87.78.14
- B. 80.87.78.0 - 80.87.78.110
- C. 80.87.78.1 - 80.87.78.62
- D. 80.87.78.1 - 80.87.78.158

**Answer:** C

#### Explanation:

The network 80.87.78.0/26 is a Class A network with a subnet mask of /26, which means that it contains 26 bits of network information and 6 bits of host information. The range of valid host addresses for this network is 80.87.78.1 to 80.87.78.62. Any addresses outside of this range are reserved for special purposes.

or are not used.

#### NEW QUESTION 277

- (Exam Topic 3)

A network engineer needs to reduce the overhead of file transfers. Which of the following configuration changes would accomplish that goal?

- A. Link aggregation
- B. Jumbo frames
- C. Port security
- D. Flow control
- E. Lower FTP port

**Answer:** A

#### NEW QUESTION 280

- (Exam Topic 3)

An engineer recently decided to upgrade the firmware on a router. During the upgrade, the help desk received calls about a network outage, and a critical ticket was opened. The network manager would like to create a policy to prevent this from happening in the future. Which of the following documents should the manager create?

- A. Change management
- B. incident response
- C. Standard operating procedure
- D. System life cycle

**Answer:** A

#### NEW QUESTION 284

- (Exam Topic 3)

Which of the following records can be used to track the number of changes on a DNS zone?

- A. SOA
- B. SRV
- C. PTR
- D. NS

**Answer:** A

#### Explanation:

The DNS 'start of authority' (SOA) record stores important information about a domain or zone such as the email address of the administrator, when the domain was last updated, and how long the server should wait between refreshes. All DNS zones need an SOA record in order to conform to IETF standards. SOA records are also important for zone transfers.

#### NEW QUESTION 285

- (Exam Topic 3)

A technician uses a badge to enter a security checkpoint on a corporate campus. An unknown individual quickly walks in behind the technician without speaking. Which of the following types of attacks did the technician experience?

- A. Tailgating
- B. Evil twin
- C. On-path
- D. Piggybacking

**Answer:** A

#### Explanation:

Tailgating is a type of physical security attack where an unauthorized person follows an authorized person into a restricted area without their consent or knowledge. Tailgating can allow an attacker to bypass security measures and gain access to sensitive information or resources. In this scenario, the technician experienced tailgating when the unknown individual walked in behind the technician without speaking. Piggybacking is similar to tailgating, but it involves the consent or cooperation of the authorized person. Evil twin is a type of wireless network attack where an attacker sets up a rogue access point that mimics a legitimate one. On-path is a type of network attack where an attacker intercepts and modifies traffic between two parties.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.2: Given a scenario, use appropriate network hardening techniques.

#### NEW QUESTION 289

- (Exam Topic 3)

A network engineer is designing a wireless network that has the following requirements:

- Network speed must be higher than 100Mbps
- Must use the 2.4GHz and 5GHz bands

Which of the following 802.11 standards should the engineer select?

- A. 802.11a
- B. 802.11b
- C. 802.11g
- D. 802.11n

**Answer:** D

**Explanation:**

\* 802.11 n is a wireless standard that supports up to 600 Mbps data rate and operates in both the 2.4 GHz and 5 GHz frequency bands. 802.11n uses multiple-input multiple-output (MIMO) technology to increase the number of spatial streams and improve the wireless performance and range. 802.11n meets the requirements of the wireless network design.

References: Network+ Study Guide Objective 1.6: Explain the functions of network services.

**NEW QUESTION 292**

- (Exam Topic 3)

A technician is monitoring a network interface and notices the device is dropping packets. The cable and interfaces, however, are in working order. Which of the following is MOST likely the cause?

- A. OID duplication
- B. MIB mismatch
- C. CPU usage
- D. Encapsulation errors

**Answer: C**

**NEW QUESTION 293**

- (Exam Topic 3)

A company is deploying a SAN at headquarters and a branch office 1,000mi (1,609km) away that will access small amounts of data. Which of the following types of connections would be MOST cost effective to implement?

- A. iSCSI
- B. FCoE
- C. Ethernet
- D. FC

**Answer: A**

**Explanation:**

Mike Meyers

"Internet Small Computer Systems Interface (iSCSI) is built on top of TCP/IP, enabling devices that use the SCSI protocol to communicate across existing networks using cheap, readily available hardware."

Jason Dion "iSCSI (IP Small Computer System Interface)

- Lower cost, built using Ethernet switches (<10 Gbps)
- Relies on configuration allowing jumbo frames over the network"

**NEW QUESTION 295**

- (Exam Topic 3)

A network administrator requires redundant routers on the network, but only one default gateway is configurable on a workstation. Which of the following will allow for redundant routers with a single IP address?

- A. EIGRP
- B. VRRP
- C. MPLS
- D. STP

**Answer: B**

**Explanation:**

Virtual Router Redundancy Protocol (VRRP) is a protocol that allows for redundant routers on the network with a single IP address. VRRP works by creating a virtual router that consists of one master router and one or more backup routers. The virtual router has its own IP address and MAC address that are shared among the routers in the group. The master router responds to traffic sent to the virtual router's IP address, while the backup routers monitor the master router's status. If the master router fails, one of the backup routers takes over as the new master router and continues to respond to traffic. This way, VRRP provides high availability and fault tolerance for the network. References:

<https://www.comptia.org/training/books/network-n10-008-study-guide> (page 230)

**NEW QUESTION 296**

- (Exam Topic 3)

A company needs to virtualize a replica of its internal physical network without changing the logical topology and the way that devices behave and are managed. Which of the following technologies meets this requirement?

- A. NFV
- B. SDWAN
- C. VIP
- D. MPLS

**Answer: A**

**Explanation:**

Network Function Virtualization (NFV) is a technology that allows for the virtualization of a replica of a network's physical topology and the way it behaves without changing the logical topology and the way that devices are managed. NFV allows for the virtualization of network functions such as routers, firewalls, and switches, resulting in increased flexibility and scalability. This makes NFV an ideal technology for companies looking to virtualize a replica of their internal physical network.

**NEW QUESTION 300**

- (Exam Topic 3)

A customer needs to distribute Ethernet to multiple computers in an office. The customer would like to use non-proprietary standards. Which of the following blocks

does the technician need to install?

- A. 110
- B. 66
- C. Bix
- D. Krone

**Answer:** A

**Explanation:**

A 110 block is a type of punch-down block that is used to distribute Ethernet to multiple computers in an office. A punch-down block is a device that connects one group of wires to another group of wires by using a special tool that pushes the wires into slots on the block. A 110 block is a non-proprietary standard that supports up to Category 6 cabling and can be used for voice or data applications. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 64)

**NEW QUESTION 301**

- (Exam Topic 3)

Which of the following compromises internet-connected devices and makes them vulnerable to becoming part of a botnet? (Select TWO).

- A. Deauthentication attack
- B. Malware infection
- C. IP spoofing
- D. Firmware corruption
- E. Use of default credentials
- F. Dictionary attack

**Answer:** BE

**NEW QUESTION 302**

- (Exam Topic 3)

A user reports that a crucial fileshare is unreachable following a network upgrade that was completed the night before. A network technician confirms the problem exists. Which of the following troubleshooting Steps should the network technician perform NEXT?

- A. Establish a theory of probable cause.
- B. Implement a solution to fix the problem.
- C. Create a plan of action to resolve the problem.
- D. Document the problem and the solution.

**Answer:** A

**Explanation:**

s for the problem and testing them to verify or eliminate them. In this scenario, the network technician has confirmed the problem exists and should proceed to establish a theory of probable cause based on the information available, such as the network upgrade that was completed the night before.

Implementing a solution to fix the problem is the fifth step in the general troubleshooting process, after establishing a plan of action. Implementing a solution involves applying the chosen method or technique to resolve the problem and verifying its effectiveness. In this scenario, the network technician has not established a plan of action yet and should not implement a solution without knowing the cause of the problem.

Creating a plan of action to resolve the problem is the fourth step in the general troubleshooting process, after establishing a theory of probable cause. Creating a plan of action involves selecting the best method or technique to address the problem based on the available resources, constraints, and risks. In this scenario, the network technician has not established a theory of probable cause yet and should not create a plan of action without knowing the cause of the problem.

Documenting the problem and the solution is the seventh and final step in the general troubleshooting process, after implementing preventive measures.

Documenting the problem and the solution involves recording the details of the problem, its symptoms, its cause, its solution, and its preventive measures for future reference and improvement. In this scenario, the network technician has not implemented preventive measures yet and should not document the problem and the solution without resolving and preventing it.

**NEW QUESTION 307**

- (Exam Topic 3)

During a client audit, a network analyst is tasked with recommending changes to upgrade the client network and readiness. Afield technician has submitted the following report:

Building B is connected to Building A via site-to-site directional antennas.
Thirty additional users have been added recently and are not shown on the network map.
The IT closet and storage room share a space that has poor ventilation.
Performance reports show optimal network performance but little on system health.

Based on this report, which of the following metrics or sensors would be the BEST recommendation to the client?

- A. Electrical
- B. Humidity
- C. Flooding
- D. Temperature

**Answer:** B

**Explanation:**

Humidity is the amount of water vapor in the air. High humidity can cause corrosion, condensation, and short circuits in electronic devices. Low humidity can cause static electricity and damage sensitive components. The optimal humidity range for a data center is between 40% and 60%. Based on the report, the humidity level in the server room is 70%, which is too high and can affect the performance and reliability of the network equipment. Therefore, the best recommendation to the client is to install a humidity sensor and a dehumidifier to control the humidity level in the server room.

References: Network+ Study Guide Objective 5.1: Summarize the importance of physical security controls.

#### NEW QUESTION 312

- (Exam Topic 3)

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+ is used to authenticate users and authorize access to network resources. This protocol provides greater network security by encrypting the authentication credentials and reducing the risk of unauthorized access. According to the CompTIA Network+ Study Manual, "TACACS+ is an authentication protocol used to centralize authentication and authorization for network devices. It is a more secure alternative to Telnet for handling logins and for granting privileges to users."

#### NEW QUESTION 315

- (Exam Topic 3)

A network administrator is reviewing the network device logs on a syslog server. The messages are normal but the stamps on the messages are incorrect. Which of the following actions should the administrator take to ensure the log message time stamps are correct?

- A. Change the NTP settings on the network device
- B. Change the time on the syslog server
- C. Update the network device firmware
- D. Adjust the timeout settings on the syslog server
- E. Adjust the SSH settings on the network device.

**Answer: A**

#### NEW QUESTION 316

- (Exam Topic 3)

Which of the Mowing architectures reduces network latency by enforcing a limit on the number of switching devices on the frame's path between any internal hosts?

- A. Spine and leaf
- B. Software-defined network
- C. Three-tiered
- D. Collapsed core

**Answer: A**

#### Explanation:

It does this by using a two-level hierarchy of switches, where the spine switches connect to the leaf switches, which in turn connect to the end hosts. This reduces the number of hops a packet must take from one host to another, thus reducing latency. According to the CompTIA Network+ N10-008 Exam Guide, the Spine and Leaf topology is a modern architecture that is used to reduce latency in large networks.

#### NEW QUESTION 318

- (Exam Topic 3)

A network engineer is monitoring a fiber uplink to a remote office and notes the uplink has been operating at 100% capacity for a long duration. Which of the following performance metrics is MOST likely to be impacted with sustained link saturation?

- A. Latency
- B. Jitter
- C. Speed
- D. Bandwidth

**Answer: A**

#### Explanation:

When a fiber uplink is operating at 100% capacity for an extended period of time, it can cause sustained link saturation. This can impact the network's performance by increasing latency. Latency is the time it takes for a packet to travel from the source to its destination. When there is link saturation, packets may have to wait in a queue before being transmitted, which increases the time it takes for them to reach their destination. As a result, users may experience delays or timeouts when accessing network resources.

Other metrics such as jitter, speed, and bandwidth are also important, but they are not as directly impacted by sustained link saturation as latency.

#### NEW QUESTION 320

- (Exam Topic 3)

A technician notices that equipment is being moved around and misplaced in the server room, even though the room has locked doors and cabinets. Which of the following would be the BEST solution to identify who is responsible?

- A. Install motion detection
- B. Install cameras.
- C. Install tamper detection.
- D. Hire a security guard.

**Answer:** B

**Explanation:**

Installing cameras in the server room is the best solution to identify who is responsible for the equipment being moved and misplaced. Cameras provide a way to monitor the server room in real time and can be used to identify suspicious activity. Additionally, they provide a way to review past activity and allow you to review footage to determine who may be responsible for the misplacement of equipment.

**NEW QUESTION 322**

.....

## Relate Links

**100% Pass Your N10-009 Exam with Exam Bible Prep Materials**

<https://www.exambible.com/N10-009-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>