Number: N10-008
Passing Score: 800
Time Limit: 120
File Version: 21.0

Exam Code: N10-008
Exam Name: CompTIA Network+

Exam A

QUESTION 1
Which of the following is the LARGEST MTU for a standard Ethernet frame?

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

Correct Answer: C
Section:
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. Reference: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam- objectives-(2-0), https://en.wikipedia.org/wiki/Maximum_transmission_unit

QUESTION 2
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

Correct Answer: D
Section:
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. Reference: 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

QUESTION 3
According to troubleshooting methodology, which of the following should the technician do NEXT after determining the most likely probable cause of an issue?

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

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

QUESTION 4
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

Correct Answer: D
Section:
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. Reference: 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

QUESTION 5
A technician is installing a cable modem in a SOHO. Which of the following cable types will the technician MOST likely use to connect a modem to the ISP?

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

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

QUESTION 6
A network technician is reviewing the interface counters on a router interface. The technician is attempting to confirm a cable issue. Given the following information:

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

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

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

Correct Answer: C
Section:
Explanation:
CRC stands for Cyclic Redundancy Check, and it is a type of error-detecting code used to detect accidental changes to raw data. If the CRC count is increasing on a particular interface, it indicates that there might be an issue with the cabling, which is causing data corruption. Reference:
Network+ N10-008 Objectives: 2.1 Given a scenario, troubleshoot common physical connectivity issues.

QUESTION 7
Which of the following is the physical topology for an Ethernet LAN?

A. Bus
B. Ring
C. Mesh
D. Star

Correct Answer: D
Section:
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. Reference: Network+ N10-008 Objectives: 2.2 Explain common logical network topologies and their characteristics.

QUESTION 8
An IT director is setting up new disaster and HA policies for a company. Limited downtime is critical to operations. To meet corporate requirements, the director set up two different datacenters across the country that will stay current on data and applications. In the event of an outage, the company can immediately switch from one datacenter to another. Which of the following does this BEST describe?

A. A warm site
B. Data mirroring
C. Multipathing
D. Load balancing

E. A hot site

Correct Answer: E
Section:
Explanation:
A hot site is a fully redundant site that can take over operations immediately if the primary site goes down. In this scenario, the company has set up two different datacenters across the country that are current on data and applications, and they can immediately switch from one datacenter to another in case of an outage. Reference:
Network+ N10-008 Objectives: 1.5 Compare and contrast disaster recovery concepts and methodologies.

QUESTION 9
The management team needs to ensure unnecessary modifications to the corporate network are not permitted and version control is maintained. Which of the following documents would BEST support this?

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

Correct Answer: C
Section:
Explanation:
A change management policy is a document that outlines the procedures and guidelines for making changes to a network or system, including how changes are approved, tested, and implemented. By following a change management policy, organizations can ensure that unnecessary modifications to the network are not permitted and version control is maintained. Reference:
Network+ N10-008 Objectives: 1.6 Given a scenario, implement network configuration and change management best practices.

QUESTION 10
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

Correct Answer: B
Section:
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. Reference:
Network+ N10-008 Objectives: 3.3 Given a scenario, implement secure network architecture concepts.

QUESTION 11
A technician is troubleshooting a network switch that seems to stop responding to requests intermittently whenever the logging level is set for debugging. Which of the following metrics should the technician check to begin troubleshooting the issue?

A. Audit logs
B. CPU utilization
C. CRC errors
D. Jitter

Correct Answer: B
Section:
Explanation:
CPU utilization is a metric that measures the percentage of time a CPU spends executing instructions. When the logging level is set for debugging, the router may generate a large amount of logging data, which can increase CPU utilization and cause the router to stop responding to requests intermittently. Reference:
Network+ N10-008 Objectives: 2.1 Given a scenario, troubleshoot common physical connectivity issues.

QUESTION 12
A technician wants to deploy a new wireless network that comprises 30 WAPs installed throughout a three-story office building. All the APs will broadcast the same SSID for client access. Which of the following BEST describes this deployment?

A. Extended service set
B. Basic service set
C. Unified service set
D. Independent basic service set

Correct Answer: A
Section:
Explanation:
An extended service set (ESS) is a wireless network that consists of multiple access points (APs) that share the same SSID and are connected by a wired network. An ESS allows wireless clients to roam seamlessly between different APs without losing connectivity. A basic service set (BSS) is a wireless network that consists of a single AP and its associated clients. An independent basic service set (IBSS) is a wireless network that consists of a group of clients that communicate directly without an AP. A unified service set is not a standard term for a wireless network. Reference:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam- objectives-(2-0), https://en.wikipedia.org/wiki/Service_set_(802.11_network)

QUESTION 13
A user tries to ping 192.168.1.100 from the command prompt on the 192.168.2.101 network but gets the following response: U.U.U.U. Which of the following needs to be configured for these networks to reach each other?

A. Network address translation
B. Default gateway
C. Loopback
D. Routing protocol

Correct Answer: B
Section:
Explanation:
A default gateway is a device that routes traffic from one network to another network, such as the Internet. A default gateway is usually configured on each host device to specify the IP address of the router that connects the host's network to other networks. In this case, the user's device and the destination device are on different networks (192.168.1.0/24 and 192.168.2.0/24), so the user needs to configure a default gateway on their device to reach the destination device. Reference:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam- objectives-(2-0), https://www.techopedia.com/definition/25761/default-gateway

QUESTION 14
A branch of a company recently switched to a new ISP. The network engineer was given a new IP range to assign. The ISP assigned 196.26.4.0/26, and the branch gateway router now has the following configurations on the interface that peers to the ISP:

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

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

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

Correct Answer: C
Section:
Explanation:
The IP address configured on the router interface is 196.26.4.1/26, which belongs to the IP range assigned by the ISP (196.26.4.0/26). However, this IP address is not valid for this interface because it is the network address of the subnet, which cannot be assigned to any host device. The network address is the first address of a subnet that identifies the subnet itself. The valid IP addresses for this subnet are from 196.26.4.1 to 196.26.4.62, excluding the network address (196.26.4.0) and the broadcast address (196.26.4.63). The router interface should be configured with a valid IP address within this range to restore Internet connectivity for all users. Reference: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam- objectives-(2-0), https://www.techopedia.com/definition/24136/network-address

QUESTION 15
Within the realm of network security, Zero Trust:

A. prevents attackers from moving laterally through a system.
B. allows a server to communicate with outside networks without a firewall.
C. block malicious software that is too new to be found in virus definitions.
D. stops infected files from being downloaded via websites.

Correct Answer: A
Section:
Explanation:
Zero Trust is a security framework that requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust prevents attackers from moving laterally through a system by applying granular policies and controls based on the principle of least privilege and by segmenting and encrypting data flows across the network.
Reference: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008- exam-objectives-(2-0), https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

QUESTION 16
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)

Correct Answer: B
Section:
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.

QUESTION 17

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

Correct Answer: B
Section:
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. Reference: Network+ Certification Study Guide, Chapter 5:
Network Security

QUESTION 18
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

Correct Answer: A
Section:
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. Reference:
Network+ Certification Study Guide, Chapter 2: Network Operations

QUESTION 19
A network administrator needs to query the NSs for a remote application. Which of the following commands would BEST help the administrator accomplish this task?

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

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

QUESTION 20
Which of the following would MOST likely be used to review previous upgrades to a system?

A. Business continuity plan

B. Change management
C. System life cycle
D. Standard operating procedures

Correct Answer: B
Section:
Explanation:
Change management is the process of reviewing previous upgrades to a system. It is a systematic approach to managing changes to an organization's IT systems and infrastructure. Change management involves the assessment of potential risks associated with a change, as well as the identification of any necessary resources required to implement the change. Reference: Network+ Certification Study Guide, Chapter 8: Network Troubleshooting

QUESTION 21
A technician is deploying a new switch model and would like to add it to the existing network monitoring software. The technician wants to know what metrics can be gathered from a given switch. Which of the following should the technician utilize for the switch?

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

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

QUESTION 22
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

Correct Answer: A
Section:
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. Reference: Network+ Certification Study Guide, Chapter 8: Network Troubleshooting

QUESTION 23
A network administrator is implementing OSPF on all of a company’s network devices. Which of the following will MOST likely replace all the company’s hubs?

A. A Layer 3 switch

B. A proxy server
C. A NGFW
D. A WLAN controller

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

QUESTION 24
A network administrator discovers that users in an adjacent building are connecting to the company's guest wireless network to download inappropriate material. Which of the following can the administrator do to MOST easily mitigate this issue?

A. Reduce the wireless power levels
B. Adjust the wireless channels
C. Enable wireless client isolation
D. Enable wireless port security

Correct Answer: A
Section:
Explanation:
Reducing the wireless power levels can limit the range of the guest wireless network and prevent users in an adjacent building from connecting to it. Adjusting the wireless channels or enabling wireless client isolation will not affect the signal strength or coverage of the guest network. Enabling wireless port security will not work on a guest network that does not use authentication or MAC address filtering. Reference: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 2.0 Network Operations, Objective 2.5 Given a scenario, implement appropriate wireless configuration settings; Guest WiFi Security - Cisco Umbrella

QUESTION 25
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

Correct Answer: D
Section:
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. Reference: CompTIA Network+ Certification Study Guide, Chapter 5: Network Security.

QUESTION 26
An attacker is attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt. Which of the following attack types BEST describes this action?

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

D. Dictionary attack

Correct Answer: D
Section:
Explanation:
The attacker attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt is using a dictionary attack. Reference: CompTIA Network+ Certification Study Guide, Chapter 6: Network Attacks and Mitigation.

QUESTION 27
Which of the following technologies provides a failover mechanism for the default gateway?

A. FHRP
B. LACP
C. OSPF
D. STP

Correct Answer: A
Section:
Explanation:
First Hop Redundancy Protocol (FHRP) provides a failover mechanism for the default gateway, allowing a backup gateway to take over if the primary gateway fails. Reference: CompTIA Network+ Certification Study Guide, Chapter 4: Infrastructure.

QUESTION 28
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

Correct Answer: A
Section:
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. Reference: CompTIA Network+ Certification Study Guide, Chapter 3: IP Addressing.

QUESTION 29
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 ecth0 promisc
B. ifconfig eth1 up
C. ifconfig eth0 10.1.2.3
D. ifconfig eth1 hw ether A1:B2:C3:D4:E5:F6

Correct Answer: A
Section:
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. Reference: CompTIA Network+ Certification Study Guide, Chapter 7: Network Devices.

QUESTION 30
A network engineer is investigating reports of poor network performance. Upon reviewing a device configuration, the engineer finds that duplex settings are mismatched on both ends. Which of the following would be the MOST likely result of this finding?

A. Increased CRC errors
B. Increased giants and runts
C. Increased switching loops
D. Increased device temperature

Correct Answer: A
Section:
Explanation:
Mismatched duplex settings can cause an increase in CRC errors, which are errors in data transmission that can result in corrupted data. Reference: CompTIA Network+ Certification Study Guide, Chapter 4: Infrastructure.

QUESTION 31
Which of the following devices would be used to manage a corporate WLAN?

A. A wireless NAS
B. A wireless bridge
C. A wireless router
D. A wireless controller

Correct Answer: D
Section:
Explanation:
A wireless controller is used to manage a corporate WLAN, providing centralized management and configuration of access points. Reference: CompTIA Network+ Certification Study Guide, Chapter 8: Wireless Networks.

QUESTION 32
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

Correct Answer: C
Section:
Explanation:
Next-generation firewalls can provide content filtering and threat protection, and can manage multiple IPSec site-to-site connections. Reference: CompTIA Network+ Certification Study Guide, Chapter 5: Network Security.

QUESTION 33
An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex. Which of the following is the MOST likely cause of this issue?

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

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

QUESTION 34
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

Correct Answer: A
Section:
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.
Reference:
CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 6: Network Servers, p. 300

QUESTION 35
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

Correct Answer: C
Section:
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.

QUESTION 36
A network engineer configured new firewalls with the correct configuration to be deployed to each remote branch. Unneeded services were disabled, and all firewall rules were applied successfully. Which of the following should the network engineer perform NEXT to ensure all the firewalls are hardened successfully?

A. Ensure an implicit permit rule is enabled
B. Configure the log settings on the firewalls to the central syslog server
C. Update the firewalls with current firmware and software
D. Use the same complex passwords on all firewalls

Correct Answer: C
Section:
Explanation:
Updating the firewalls with current firmware and software is an important step to ensure all the firewalls are hardened successfully, as it can fix any known vulnerabilities or bugs and provide new features or enhancements. Enabling an implicit permit rule is not a good practice for firewall hardening, as it can allow unwanted traffic to pass through the firewall. Configuring the log settings on the firewalls to the central syslog server is a good practice for monitoring and auditing purposes, but it does not harden the firewalls themselves. Using the same complex passwords on all firewalls is not a good practice for password security, as it can increase the risk of compromise if one firewall is breached. Reference: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number:
N10-006), Domain 3.0 Network Security, Objective 3.3 Given a scenario, implement network hardening techniques.

QUESTION 37
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

Correct Answer: C
Section:
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.
Reference:
CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: Network Models, p. 82

QUESTION 38
An engineer is configuring redundant network links between switches. Which of the following should the engineer enable to prevent network stability issues?

A. 802.1Q
B. STP

C. Flow control
D. CSMA/CD

Correct Answer: B
Section:
Explanation:
Spanning Tree Protocol (STP) should be enabled when configuring redundant network links between switches. STP ensures that only one active path is used at a time, preventing network loops and stability issues.
Reference:
CompTIA Network+ Certification Study Guide

QUESTION 39
Several WIFI users are reporting the inability to connect to the network. WLAN users on the guest network are able to access all network resources without any performance issues. The following table summarizes the findings after a site survey of the area in question:

Location	AP 1	AP 2	AP 3	AP 4
SSID	Corp1	Corp1	Corp1/Guest	Corp1/Guest
Channel	2	1	5	11
RSSI	-81dBm	-82dBm	-44dBm	-41dBm
Antenna type	Omni	Omni	Directional	Directional

Which of the following should a wireless technician do NEXT to troubleshoot this issue?

A. Reconfigure the channels to reduce overlap
B. Replace the omni antennas with directional antennas
C. Update the SSIDs on all the APs
D. Decrease power in AP 3 and AP 4

Correct Answer: B
Section:
Explanation:

QUESTION 40

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

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

Correct Answer: B
Section:
Explanation:
BGP (Border Gateway Protocol) is a routing protocol used to exchange route information between public autonomous systems (AS). OSPF (Open Shortest Path First), EGRIP (Enhanced Interior Gateway Routing Protocol), and RIP (Routing Information Protocol) are all used for internal routing within a single AS. Therefore, BGP is the correct option to choose for this question.
Reference:
Network+ N10-007 Certification Exam Objectives, Objective 3.3: Given a scenario, configure and apply the appropriate routing protocol.
Cisco: Border Gateway Protocol (BGP) Overview

QUESTION 41
A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

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

Correct Answer: A
Section:
Explanation:
To detect the exact break point of a fiber link, an engineer should use an OTDR (Optical Time Domain Reflectometer). This device sends a series of pulses into the fiber, measuring the time it takes for the pulses to reflect back, and can pinpoint the exact location of the break.
Reference:
Network+ N10-007 Certification Exam Objectives, Objective 2.5: Given a scenario, troubleshoot copper cable issues.
FS: OTDR (Optical Time Domain Reflectometer) Testing Principle and Applications

QUESTION 42
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

Correct Answer: B
Section:
Explanation:
TACACS+ (Terminal Access Controller Access Control System Plus) can be used to centrally manage credentials for various types of administrative privileges on configured network devices. This protocol separates

authentication, authorization, and accounting (AAA) functions, providing more granular control over access to network resources.
Reference:
Network+ N10-007 Certification Exam Objectives, Objective 4.2: Given a scenario, implement secure network administration principles.

QUESTION 43
A network technician is installing new software on a Windows-based server in a different geographical location. Which of the following would be BEST for the technician to use to perform this task?

A. RDP
B. SSH
C. FTP
D. DNS

Correct Answer: A
Section:
Explanation:
RDP (Remote Desktop Protocol) is the best option for a network technician to use when installing new software on a Windows-based server in a different geographical location. This protocol allows the technician to connect to the server remotely and control it as if they were physically present.
Reference:
Network+ N10-007 Certification Exam Objectives, Objective 2.2: Given a scenario, implement the appropriate network-based security and troubleshoot common connectivity issues.

QUESTION 44
Branch users are experiencing issues with videoconferencing. Which of the following will the company MOST likely configure to improve performance for these applications?

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

Correct Answer: C
Section:
Explanation:
To improve performance for videoconferencing, the company should configure Quality of Service (QoS). This technology allows for the prioritization of network traffic, ensuring that videoconferencing traffic is given higher priority and therefore better performance. Link Aggregation Control Protocol (LACP), Dynamic routing, Network load balancer, and Static IP addresses are not directly related to improving performance for videoconferencing.
Reference:
Network+ N10-007 Certification Exam Objectives, Objective 2.6: Given a scenario, implement and configure the appropriate wireless security and implement the appropriate QoS concepts.

QUESTION 45
A technician is assisting a user who cannot connect to a network resource. The technician first checks for a link light. According to troubleshooting methodology, this is an example of:

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

Correct Answer: A
Section:
Explanation:

Using a bottom-to-top approach means starting from the physical layer and moving up the OSI model to troubleshoot a network problem. Checking for a link light is a physical layer check that verifies the connectivity of the network cable and device. Reference:
https://www.professormesser.com/network-plus/n10-007/troubleshooting-methodologies-2/

QUESTION 46
Which of the following transceiver types can support up to 40Gbps?

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

Correct Answer: B
Section:
Explanation:
QSFP+ is a transceiver type that can support up to 40Gbps. It stands for Quad Small Form-factor Pluggable Plus and uses four lanes of data to achieve high-speed transmission. It is commonly used for data center and high-performance computing applications. Reference:
https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver- modules/data_sheet_c78-660083.html

QUESTION 47
Which of the following TCP ports is used by the Windows OS for file sharing?

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

Correct Answer: C
Section:
Explanation:
TCP port 445 is used by the Windows OS for file sharing. It is also known as SMB (Server Message Block) or CIFS (Common Internet File System) and allows users to access files, printers, and other shared resources on a network. Reference: https://docs.microsoft.com/en-us/windows- server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

QUESTION 48
A network administrator redesigned the positioning of the APs to create adjacent areas of wireless coverage. After project validation, some users still report poor connectivity when their devices maintain an association to a distanced AP. Which of the following should the network administrator check FIRST?

A. Validate the roaming settings on the APs and WLAN clients
B. Verify that the AP antenna type is correct for the new layout
C. Check to see if MU-MIMO was properly activated on the APs
D. Deactivate the 2.4GHz band on the APS

Correct Answer: A
Section:
Explanation:
The network administrator should check the roaming settings on the APs and WLAN clients first. Roaming is the process of switching from one AP to another without losing connectivity. If the roaming settings are not configured properly, some users may experience poor connectivity when their devices stay connected to a distant AP instead of switching to a closer one. Reference:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-roam- faq.html

QUESTION 49
Which of the following connector types would have the MOST flexibility?

A. SFP
B. BNC
C. LC
D. RJ45

Correct Answer: A
Section:
Explanation:
SFP (Small Form-factor Pluggable) is a connector type that has the most flexibility. It is a hot- swappable transceiver that can support different speeds, distances, and media types depending on the module inserted. It can be used for both copper and fiber connections and supports various protocols such as Ethernet, Fibre Channel, and SONET. Reference: https://www.fs.com/what-is-sfp- transceiver-aid-11.html

QUESTION 50
Which of the following ports is commonly used by VoIP phones?

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

Correct Answer: D
Section:
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.
Reference: https://www.voip-info.org/session-initiation-protocol/

QUESTION 51
A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds that jitter at the office is greater than 10ms on the only WAN connection available. Which of the following would be MOST affected by this statistic?

A. A VoIP sales call with a customer
B. An in-office video call with a coworker
C. Routing table from the ISP
D. Firewall CPU processing time

Correct Answer: A
Section:
Explanation:
A VoIP sales call with a customer would be most affected by jitter greater than 10ms on the WAN connection. Jitter is the variation in delay of packets arriving at the destination. It can cause choppy or distorted audio quality for VoIP applications, especially over WAN links that have limited bandwidth and high latency. The recommended jitter for VoIP is less than 10ms. Reference:
https://www.voip-info.org/voip-jitter/

QUESTION 52
A network technician needs to ensure outside users are unable to telnet into any of the servers at the datacenter. Which of the following ports should be blocked when checking firewall configuration?

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

Correct Answer: B
Section:
Explanation:
Port 23 should be blocked when checking firewall configuration to prevent outside users from telnetting into any of the servers at the datacenter. Port 23 is the default port for Telnet, which is an insecure protocol that allows remote access to servers and network devices. Telnet sends data in clear text, which can be easily intercepted and compromised by attackers. A more secure alternative is SSH, which uses port 22 and encrypts data.
Reference:
https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

QUESTION 53
A technician is writing documentation regarding a company's server farm. The technician needs to confirm the server name for all Linux servers. Which of the following commands should the technician run?

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

Correct Answer: B
Section:
Explanation:
The nslookup command should be run to confirm the server name for all Linux servers. Nslookup is a tool that queries DNS servers to resolve hostnames to IP addresses or vice versa. It can also provide other information about DNS records, such as MX, NS, SOA, etc. By running nslookup with the IP address of a Linux server, the technician can obtain its hostname. Reference:
https://www.howtogeek.com/663056/how-to-use-the-nslookup-command-on-linux/

QUESTION 54
A local firm has hired a consulting company to clean up its IT infrastructure. The consulting company notices remote printing is accomplished by port forwarding via publicly accessible IPs through the firm's firewall Which of the following would be the MOST appropriate way to enable secure remote printing?

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

Correct Answer: B
Section:
Explanation:
VPN (Virtual Private Network) is the most appropriate way to enable secure remote printing. VPN is a technology that creates a secure and encrypted tunnel over a public network such as the Internet. It allows remote users or sites to access a private network as if they were directly connected to it. VPN can be used for various purposes such as accessing corporate resources, bypassing geo-restrictions, or enhancing privacy and security. VPN can also be used for remote printing by allowing users to connect to a printer on the private network and send print jobs securely over the VPN tunnel.
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike- protocols/14106-how-vpn-works.html

QUESTION 55
A user recently made changes to a PC that caused it to be unable to access websites by both FQDN and IP Local resources, such as the file server remain accessible. Which of the following settings did the user MOST likely

misconfigure?

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

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

QUESTION 56
Which of the following policies is MOST commonly used for guest captive portals?

A. AUP
B. DLP
C. BYOD
D. NDA

Correct Answer: A
Section:
Explanation:
AUP stands for Acceptable Use Policy, which is a policy that defines the rules and guidelines for using a network or service. A guest captive portal is a web page that requires users to agree to the AUP before accessing the Internet or other network resources. This is a common way to enforce security and legal compliance for guest users. Reference:
https://www.arubanetworks.com/techdocs/Instant_87_WebHelp/Content/instant-ug/captive- portal/captive-portal.htm

QUESTION 57
A network administrator has been directed to present the network alerts from the past week to the company's executive staff. Which of the following will provide the BEST collection and presentation of this data?

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

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

QUESTION 58
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

Correct Answer: D
Section:
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. Reference: https://www.comptia.org/blog/network-security- basics-6-easy-ways-to-protect-your-network

QUESTION 59
A network technician is reviewing an upcoming project's requirements to implement laaS. 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

Correct Answer: D
Section:
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. Reference: https://www.comptia.org/blog/what-is-iaas

QUESTION 60
A user reports a weak signal when walking 20ft (61 m) away from the WAP in one direction, but a strong signal when walking 20ft in the opposite direction The technician has reviewed the configuration and confirmed the channel type is correct There is no jitter or latency on the connection Which of the following would be the MOST likely cause of the issue?

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

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

QUESTION 61
A network technician was troubleshooting an issue for a user who was being directed to cloned websites that were stealing credentials. The URLs were correct for the websites but an incorrect IP address was revealed when the technician used ping on the user's PC After checking the is setting, the technician found the DNS server address was incorrect Which of the following describes the issue?

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

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

QUESTION 62
A network technician needs to correlate security events to analyze a suspected intrusion. Which of the following should the technician use?

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

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

QUESTION 63
A network administrator is setting up several loT devices on a new VLAN and wants to accomplish the following

A. Reduce manual configuration on each system
B. Assign a specific IP address to each system
C. Allow devices to move to different switchports on the same VLAN
Which of the following should the network administrator do to accomplish these requirements?
D. Set up a reservation for each device
E. Configure a static IP on each device
F. Implement private VLANs for each device
G. Use DHCP exclusions to address each device

Correct Answer: A
Section:
Explanation:
A reservation is a feature of DHCP that assigns a specific IP address to a device based on its MAC address. This way, the device will always receive the same IP address from the DHCP server, regardless of its location or connection time. A network administrator can set up a reservation for each loT device to accomplish the requirements of reducing manual configuration, assigning a specific IP address, and allowing devices to move to

different switchports on the same VLAN.
Reference: https://www.comptia.org/blog/what-is-dhcp

QUESTION 64
During the security audit of a financial firm the Chief Executive Officer (CEO) questions why there are three employees who perform very distinct functions on the server. There is an administrator for creating users another for assigning the users lo groups and a third who is the only administrator to perform file rights assignment Which of the following mitigation techniques is being applied'

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

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

QUESTION 65
A technician is troubleshooting a previously encountered issue. Which of the following should the technician reference to find what solution was implemented to resolve the issue?

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

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

QUESTION 66
A SaaS provider has decided to leave an unpatched VM available via a public DMZ port. With which of the following concepts is this technique MOST closely associated?

A. Insider threat
B. War driving
C. Evil twin
D. Honeypot

Correct Answer: D
Section:
Explanation:
A honeypot is a decoy system that is intentionally left vulnerable or exposed to attract attackers and divert them from the real targets. A honeypot can also be used to collect information about the attackers' techniques and motives. In the scenario, the SaaS provider has left an unpatched VM available via a public DMZ port, which could be a honeypot technique to lure attackers and monitor their activities. Reference:
https://www.comptia.org/blog/what-is-a-honeypot

QUESTION 67
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

Correct Answer: C
Section:
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. Reference:
https://www.comptia.org/blog/what-is-utm

QUESTION 68
A customer wants to segregate the traffic between guests on a hypervisor. Which of the following does a technician need to configure to meet the requirement?

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

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

QUESTION 69
A Chief Information Officer (CIO) wants to improve the availability of a company's SQL database
Which of the following technologies should be utilized to achieve maximum availability?

A. Clustering
B. Port aggregation
C. NIC teaming
D. Snapshots

Correct Answer: A
Section:
Explanation:
Clustering is a technique that involves grouping multiple servers or instances together to provide high availability and fault tolerance for a database. Clustering can help improve the availability of a SQL database by allowing automatic failover and load balancing between the cluster nodes. If one node fails or becomes overloaded, another node can take over the database operations without disrupting the service. Reference:
https://www.educba.com/sql-cluster/

QUESTION 70
A network administrator wants to improve the security of the management console on the company's switches and ensure configuration changes made can be correlated to the administrator who conformed them Which of the following should the network administrator implement?

A. Port security
B. Local authentication
C. TACACS+
D. Access control list

Correct Answer: C
Section:
Explanation:
TACACS+ is a protocol that provides centralized authentication, authorization, and accounting (AAA) for network devices and users. TACACS+ can help improve the security of the management console on the company's switches by verifying the identity and credentials of the administrators, enforcing granular access policies and permissions, and logging the configuration changes made by each administrator. This way, the network administrator can ensure only authorized and authenticated users can access and modify the switch settings, and also track and correlate the changes made by each user. Reference: https://www.comptia.org/blog/what-is-tacacs

QUESTION 71
A network technician is installing an analog desk phone for a new receptionist After running a new phone line, the technician now needs to cnmp on a new connector. Which of the following connectors would MOST likely be used in this case?

A. DB9
B. RJ11
C. RJ45
D. DB25

Correct Answer: B
Section:
Explanation:
RJ11 is a type of connector that is commonly used for analog phone lines. RJ11 has four wires and six positions, but only two or four of them are used. A technician can crimp an RJ11 connector to a new phone line to install an analog desk phone for a new receptionist. Reference:
https://www.comptia.org/blog/what-is-rj11

QUESTION 72
Which of the following attacks encrypts user data and requires a proper backup implementation to recover?

A. DDoS
B. Phishing
C. Ransomware
D. MAC spoofing

Correct Answer: C
Section:
Explanation:
Ransomware is a type of malware that encrypts user data and demands a ransom for its decryption. Ransomware can prevent users from accessing their files and applications, and cause data loss or corruption. A proper backup implementation is essential to recover from a ransomware attack, as it can help restore the encrypted data without paying the ransom or relying on the attackers' decryption key. Reference:
https://www.comptia.org/blog/what-is-ransomware

QUESTION 73
A network administrator wants to analyze attacks directed toward the company's network. Which of the following must the network administrator implement to assist in this goal?

A. A honeypot
B. Network segmentation
C. Antivirus
D. A screened subnet

Correct Answer: A
Section:
Explanation:
A honeypot is a decoy system that is intentionally left vulnerable or exposed to attract attackers and divert them from the real targets. A honeypot can also be used to collect information about the attackers' techniques and motives. A network administrator can implement a honeypot to analyze attacks directed toward the company's network, as a honeypot can help identify the source, target, method, and impact of an attack, as well as provide recommendations for remediation. Reference:
https://www.comptia.org/blog/what-is-a-honeypot

QUESTION 74
A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

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

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

QUESTION 75
A technician is implementing a new wireless network to serve guests at a local office. The network needs to provide Internet access but disallow associated stations from communicating with each other. Which of the following would BEST accomplish this requirement?

A. Wireless client isolation
B. Port security
C. Device geofencing
D. DHCP snooping

Correct Answer: A
Section:
Explanation:
Wireless client isolation is a feature on wireless routers that limits the connectivity between wireless devices connected to the same network. It prevents them from accessing resources on other wireless or wired devices, as a security measure to reduce attacks and threats. This feature can be useful for guest and BYOD SSIDs, but it can also be disabled on the router's settings. Reference:
https://www.howtogeek.com/179089/lock-down-your-wi-fi-network-with-your-routers-wireless- isolation-option/

QUESTION 76

A company requires a disaster recovery site to have equipment ready to go in the event of a disaster at its main datacenter. The company does not have the budget to mirror all the live data to the disaster recovery site. Which of the following concepts should the company select?

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

Correct Answer: C
Section:
Explanation:
A warm site is a type of disaster recovery site that has equipment ready to go in the event of a disaster at the main datacenter, but does not have live data or applications. A warm site requires some time and effort to restore the data and services from backups, but it is less expensive than a hot site that has live data and applications. A cold site is a disaster recovery site that has no equipment or data, and requires a lot of time and money to set up after a disaster. A cloud site is a disaster recovery site that uses cloud computing resources to provide data and services, but it may have issues with bandwidth, latency, security, and cost. Reference: https://www.comptia.org/blog/what-is-a-warm-site

QUESTION 77
An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch. Which of the following command-line tools should the technician use to determine where the incident is occurring?

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

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

QUESTION 78
A technician is connecting DSL for a new customer. After installing and connecting the on-premises equipment, the technician verifies DSL synchronization. When connecting to a workstation, however, the link LEDs on the workstation and modem do not light up. Which of the following should the technician perform during troubleshooting?

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

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

QUESTION 79
Which of the following services can provide data storage, hardware options, and scalability to a third- party company that cannot afford new devices?

A. SaaS
B. IaaS
C. PaaS
D. DaaS

Correct Answer: B
Section:
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. IaaS can provide data storage, hardware options, and scalability to a third-party company that cannot afford new devices by allowing them to rent or lease the infrastructure they need from a cloud provider. The company can pay only for what they use and scale up or down as needed. Reference:
https://www.comptia.org/blog/what-is-iaas

QUESTION 80
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

Correct Answer: B
Section:
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. Reference: https://www.adobe.com/sign/esignature- resources/sign-nda.html

QUESTION 81
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

Correct Answer: C
Section:
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.
Reference: https://www.comptia.org/blog/what-is-a-site-to-site-vpn

QUESTION 82

A network requirement calls for segmenting departments into different networks. The campus network is set up with users of each department in multiple buildings. Which of the following should be configured to keep the design simple and efficient?

A. MDIX
B. Jumbo frames
C. Port tagging
D. Flow control

Correct Answer: C
Section:
Explanation:
Port tagging is a technique that involves adding a tag or identifier to the frames or packets that belong to a certain VLAN. A VLAN is a logical segment of a network that isolates traffic between different groups of devices. Port tagging allows devices on different physical ports or switches to communicate with each other as if they were on the same port or switch. Port tagging can help keep the design simple and efficient by reducing the number of physical ports and switches needed to segment departments into different networks. Reference: https://www.comptia.org/blog/what-is- port-tagging

QUESTION 83
Which of the following protocols will a security appliance that is correlating network events from multiple devices MOST likely rely on to receive event messages?

A. Syslog
B. Session Initiation Protocol
C. Secure File Transfer Protocol
D. Server Message Block

Correct Answer: A
Section:
Explanation:
Syslog is a protocol that provides a standard way for network devices and applications to send event messages to a logging server or a security appliance. Syslog messages can contain information about security incidents, errors, warnings, system status, configuration changes, and other events. A security appliance that is correlating network events from multiple devices can rely on Syslog to receive event messages from different sources and formats. Reference:
https://www.comptia.org/blog/what-is-syslog

QUESTION 84
Which of the following is MOST commonly used to address CVEs on network equipment and/or operating systems?

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

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

QUESTION 85

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.

Correct Answer: C
Section:
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. Reference: https://www.comptia.org/blog/what-is-power-level

QUESTION 86
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

Correct Answer: C
Section:
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.

QUESTION 87
A medical building offers patients Wi-Fi in the waiting room. Which of the following security features would be the BEST solution to provide secure connections and keep the medical data protected?

A. Isolating the guest network
B. Securing SNMP
C. MAC filtering
D. Disabling unneeded switchports

Correct Answer: A
Section:

QUESTION 88
A malicious user is using special software 10 perform an on-path attack. Which of the following best practices should be configured to mitigate this threat?

A. Dynamic ARP inspection
B. Role-based access
C. Control plane policing
D. MAC filtering

Correct Answer: A
Section:

QUESTION 89
A systems administrator wants to use the least amount of equipment to segment two departments that nave cables terminating in the same room. Which of the following would allow this to occur?

A. A load balancer
B. A proxy server
C. A Layer 3 switch
D. A hub
E. A Layer 7 firewall
F. The RSSI was not strong enough on the link

Correct Answer: C
Section:

QUESTION 90
Two network technicians are installing a fiber-optic link between routers. The technicians used a light meter to verify the correct fibers However, when they connect the fibers to the router interface the link does not connect. Which of the following would explain the issue? (Select TWO).

A. They used the wrong type of fiber transceiver.
B. Incorrect TX/RX polarity exists on the link
C. The connection has duplexing configuration issues.
D. Halogen light fixtures are causing interference.
E. One of the technicians installed a loopback adapter.
F. The RSSI was not strong enough on the link

Correct Answer: A, B
Section:

QUESTION 91
A network administrator is testing performance improvements by configuring channel bonding on an 802.Hac AP. Although a site survey detected the majority of the 5GHz frequency spectrum was idle, being used only by the company's WLAN and a nearby government radio system, the AP is not allowing the administrator to manually configure a large portion of the 5GHz frequency range. Which of the following would be BEST to configure for the WLAN being tested?

A. Upgrade the equipment to an AP that supports manual configuration of the ElRP power settings.
B. Switch to 802.11n. disable channel auto-selection, and enforce channel bonding on the configuration.
C. Set up the AP to perform a dynamic selection of the frequency according to regulatory requirements.
D. Deactivate the band 5GHz to avoid Interference with the government radio

Correct Answer: C
Section:

QUESTION 92
An ISP is unable to provide services to a user in a remote area through cable and DSL. Which of the following is the NEXT best solution to provide services without adding external infrastructure?

A. Fiber

B. Leased line
C. Satellite
D. Metro optical

Correct Answer: C
Section:
Explanation:
If an ISP is unable to provide services to a user in a remote area through cable and DSL, the next best solution to provide services without adding external infrastructure would likely be satellite. Satellite is a wireless communication technology that uses a network of satellites orbiting the Earth to transmit and receive data. It is well-suited for providing connectivity to remote or rural areas where other types of infrastructure may not be available or may be cost-prohibitive to install.

QUESTION 93
To comply with an industry regulation, all communication destined to a secure server should be logged and archived on a storage device. Which of the Mowing can be configured to fulfill this requirement?

A. QoS traffic classification
B. Port mirroring
C. Flow control
D. Link Aggregation Control Protocol

Correct Answer: B
Section:

QUESTION 94
A technician removes an old PC from the network and replaces it with a new PC that is unable to connect to the LAN. Which of the Mowing is MOST likely the cause of the issue?

A. Port security
B. Port tagging
C. Port aggregation
D. Port mirroring

Correct Answer: A
Section:
Explanation:
It is most likely that the issue is caused by port security, as this is a feature that can prevent new devices from connecting to the LAN. Port tagging, port aggregation, and port mirroring are all features that are used to manage traffic on the network, but they are not related to the connectivity of new devices. If the technician has configured port security on the network and the new PC does not meet the security requirements, it will not be able to connect to the LAN.

QUESTION 95
A network technician is having issues connecting an loT sensor to the internet The WLAN settings were enabled via a custom command line, and a proper IP address assignment was received on the wireless interlace. However, when trying to connect to the internet, only HTTP redirections are being received when data Is requested. Which of the following will point to the root cause of the Issue?

A. Verifying if an encryption protocol mismatch exists.
B. Verifying If a captive portal is active for the WLAN.
C. Verifying the minimum RSSI for operation in the device's documentation
D. Verifying EIRP power settings on the access point.

Correct Answer: C

Section:
Explanation:
A captive portal is a web page that is displayed to a user before they can access the internet or other network resources. This is often used in public or guest networks to present users with a login or terms and conditions page before they can access the internet. If a captive portal is active on the WLAN, it would explain why the IoT sensor is only receiving HTTP redirections when trying to connect to the internet.

QUESTION 96
A corporate client is experiencing global system outages. The IT team has identified multiple potential underlying causes throughout the enterprise Each team member has been assigned an area to trouble shoot. Which of the following approaches is being used?

A. Divide-and-conquer
B. Top-to-bottom
C. Bottom-to-top
D. Determine if anything changed

Correct Answer: A
Section:

QUESTION 97
A network administrator is troubleshooting a connectivity performance issue. As part of the troubleshooting process, the administrator performs a traceout from the client to the server, and also from the server to the client. While comparing the outputs, the administrator notes they show different hops between the hosts. Which of the following BEST explains these findings?

A. Asymmetric routing
B. A routing loop
C. A switch loop
D. An incorrect gateway

Correct Answer: C
Section:

QUESTION 98
Which of the following describes the BEST device to configure as a DHCP relay?

A. Bridge
B. Router
C. Layer 2 switch
D. Hub

Correct Answer: B
Section:
Explanation:
Normally, routers do not forward broadcast traffic. This means that each broadcast domain must be served by its own DHCP server. On a large network with multiple subnets, this would mean provisioning and configuring many DHCP servers. To avoid this scenario, a DHCP relay agent can be configured to provide forwarding of DHCP traffic between subnets. Routers that can provide this type of forwarding are described as RFC 1542 compliant. The DHCP relay intercepts broadcast DHCP frames, applies a unicast address for the appropriate DHCP server, and forwards them over the interface for the subnet containing the server. The DHCP server can identify the original IP subnet from the packet and offer a lease from the appropriate scope. The DHCP relay also performs the reverse process of directing responses from the server to the appropriate client subnet.

QUESTION 99
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

Correct Answer: B
Section:

QUESTION 100
A technician is consolidating a topology with multiple SSlDs into one unique SSiD deployment. Which of the following features will be possible after this new configuration?

A. Seamless roaming
B. Basic service set
C. WPA
D. MU-MIMO

Correct Answer: A
Section:

QUESTION 101
Which of the following network devices can perform routing between VLANs?

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

Correct Answer: B
Section:
Explanation:
https://www.practicalnetworking.net/stand-alone/routing-between- vlans/#:~:text=A%20router%20will%20perform%20the,to%20communicate%20with%20one%20anot her.

QUESTION 102
An international company is transferring its IT assets including a number of WAPs from the United States to an office in Europe for deployment. Which of the following considerations should the company research before Implementing the wireless hardware?

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

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

QUESTION 103
Network connectivity in an extensive forest reserve was achieved using fiber optics. A network fault was detected, and now the repair team needs to check the integrity of the fiber cable. Which of me following actions can reduce repair time?

A. Using a tone generator and wire map to determine the fault location
B. Using a multimeter to locate the fault point
C. Using an OTDR In one end of the optic cable to get the liber length information
D. Using a spectrum analyzer and comparing the current wavelength with a working baseline

Correct Answer: C
Section:

QUESTION 104
Which of the following would be used to enforce and schedule critical updates with supervisory approval and include backup plans in case of failure?

A. Business continuity plan
B. Onboarding and offboarding policies
C. Acceptable use policy
D. System life cycle
E. Change management

Correct Answer: A
Section:

QUESTION 105
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

Correct Answer: C
Section:

QUESTION 106
A technician is troubleshooting reports that a networked printer is unavailable. The printer's IP address is configured with a DHCP reservation, but the address cannot be pinged from the print server in the same subnet. Which of the following is MOST likely the cause of me connectivity failure?

A. Incorrect VLAN
B. DNS failure
C. DHCP scope exhaustion
D. Incorrect gateway

Correct Answer: D
Section:

QUESTION 107
An administrator would like to create a fault-tolerant ring between three switches within a Layer 2 network. Which of the following Ethernet features should the administrator employ?

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

Correct Answer: A
Section:
Explanation:
Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology in Ethernet networks by actively blocking certain links and enabling others. STP prevents loops by putting some of the links in a blocking state, effectively creating a loop-free topology. This ensures that there is only one active path between two devices, which helps prevent network loops and the associated problems (such as broadcast storms) that can result from them. STP is used to create a fault-tolerant ring between three switches within a Layer 2 network.

QUESTION 108
A systems operator is granted access to a monitoring application, configuration application, and timekeeping application. The operator is denied access to the financial and project management applications by the system's security configuration. Which of the following BEST describes the security principle in use?

A. Network access control
B. Least privilege
C. Multifactor authentication
D. Separation of duties

Correct Answer: D
Section:

QUESTION 109
Which of the following physical security methods Is the MOST effective to prevent tailgating?

A. Biometrics in an access control vestibule
B. IP cameras with motion detection
C. Smart lockers with tamper protection
D. Badge readers plus a PIN pad

Correct Answer: A
Section:
Explanation:
Biometrics is a type of authentication that uses a person’s physical characteristics, such as fingerprints, iris, or face, to verify their identity. An access control vestibule is a small room or area that separates two spaces and allows only one person to enter or exit at a time. Biometrics in an access control vestibule is the most effective physical security method to prevent tailgating, which is the unauthorized entry of a person behind another person who has legitimate access.
Reference: Network+ Study Guide Objective 5.1: Summarize the importance of physical security controls.

QUESTION 110
Which of the following is used to provide disaster recovery capabilities to spin up an critical devices using internet resources?

A. Cloud site

B. Hot site
C. Cold site
D. Warm site

Correct Answer: A
Section:

QUESTION 111
Which of the following would be used to adjust resources dynamically for a virtual web server under variable loads?

A. Elastic computing
B. Scalable networking
C. Hybrid deployment
D. Multitenant hosting

Correct Answer: B
Section:
Explanation:
A technique used to adjust resources dynamically for a virtual web server under variable loads is called auto-scaling. Auto-scaling automatically increases or decreases the number of instances of a virtual web server in response to changes in demand, ensuring that the right amount of resources are available to handle incoming traffic. This can help to improve the availability and performance of a web application, as well as reduce costs by avoiding the need to provision and maintain excess capacity.

QUESTION 112
After a critical power issue, the network team was not receiving UPS status notifications. The network team would like to be alerted on these status changes. Which of the following would be BEST to use tor these notifications?

A. Traps
B. MB
C. NetFlow
D. Syslog

Correct Answer: A
Section:

QUESTION 113
Which of the following needs to be tested to achieve a Cat 6a certification for a company's data cawing?

A. RJ11
B. LC ports
C. Patch panel
D. F-type connector

Correct Answer: D
Section:

QUESTION 114
A company's data center is hosted at its corporate office to ensure greater control over the security of sensitive dat

A. During times when there are increased workloads, some of the company's non-sensitive data is shifted to an external cloud provider. Which of the following cloud deployment models does this describe?
B. Hybrid
C. Community
D. Public
E. Private

Correct Answer: A
Section:

QUESTION 115
A network administrator wants to test the throughput of a new metro Ethernet circuit to verify that its performance matches the requirements specified m the SL

A. Which of the following would BEST help measure the throughput?
B. iPerf
C. Ping
D. NetFlow
E. Netstat

Correct Answer: A
Section:

QUESTION 116
A Wi-Fi network was recently deployed in a new, multilevel budding. Several issues are now being reported related to latency and drops in coverage. Which of the following is the FIRST step to troubleshoot the issues?

A. Perform a site survey.
B. Review the AP placement
C. Monitor channel utilization.
D. Test cable attenuation.

Correct Answer: A
Section:

QUESTION 117
A network technician needs to install security updates on several switches on me company's network. The management team wants this completed as quickly and efficiently as possible. Which of the following should the technician do to perform the updates?

A. Upload the security update onto each switch using a terminal emulator and a console cable.
B. Configure a TFTP server. SSH into each device, and perform the update.
C. Replace each old switch with new switches that have the updates already performed.
D. Connect a USB memory stick to each switch and perform the update.

Correct Answer: B
Section:

QUESTION 118
Which of the following fouling protocols is generally used by major ISPs for handing large-scale internet traffic?

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

Correct Answer: D
Section:

QUESTION 119
A network administrator is installing a new server in the data center. The administrator is concerned the amount of traffic generated will exceed 1GB. and higher-throughput NiCs are not available for installation. Which of the following is the BEST solution for this issue?

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

Correct Answer: A
Section:

QUESTION 120
Which of me following security controls indicates unauthorized hardware modifications?

A. Biometric authentication
B. Media device sanitization
C. Change management policy
D. Tamper-evident seals

Correct Answer: A
Section:

QUESTION 121
Which of the following topologies requires me MOST connections when designing a network?

A. Mesh
B. Star
C. Bus
D. Ring

Correct Answer: A
Section:

QUESTION 122
An administrator would like to allow Windows clients from outside me office to access workstations without using third-party software. Which or the following access methods would meet this requirement?

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

Correct Answer: A
Section:
Explanation:
To allow Windows clients from outside the office to access workstations without using third-party software, the administrator can use the Remote Desktop Protocol (RDP). RDP is a built-in feature of the Windows operating system that allows users to remotely connect to and control other Windows computers over a network connection.
To use RDP, the administrator will need to enable the Remote Desktop feature on the workstations that need to be accessed, and ensure that the appropriate firewall rules are in place to allow RDP traffic to pass through. The administrator will also need to provide the remote users with the necessary credentials to access the workstations.
Once RDP is set up and configured, the remote users can use the Remote Desktop client on their own computers to connect to the workstations and access them as if they were physically present in the office. This allows the administrator to provide remote access to the workstations without the need for any additional software or third-party tools.

QUESTION 123
Which of the following is a benefit of the spine-and-leaf network topology?

A. Increased network security
B. Stable network latency
C. Simplified network management
D. Eliminated need for inter-VLAN routing

Correct Answer: A
Section:

QUESTION 124
To access production applications and data, developers must first connect remotely to a different server From there, the developers are able to access production data Which of the following does this BEST represent?

A. A management plane
B. A proxy server
C. An out-of-band management device
D. A site-to-site VPN
E. A jump box

Correct Answer: E
Section:

QUESTION 125
A network administrator is reviewing the following metrics from a network management system regarding a switchport. The administrator suspects an issue because users are calling in regards to the switchport's performance:

Metric	Value
Uptime	201 days, 3 hours, 18 minutes
MDIX	On
CRCs	0
Giants	2508
Output queue maximum	40
Packets input	136208849
Packets output	64458087024

Based on the information in the chart above, which of the following fs the cause of these performance issues?

A. The connected device is exceeding the configured MTU.
B. The connected device is sending too many packets
C. The switchport has been up for too long
D. The connected device is receiving too many packets.
E. The switchport does not have enough CRCs

Correct Answer: A
Section:

QUESTION 126
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

Correct Answer: D
Section:

QUESTION 127
During a risk assessment which of the following should be considered when planning to mitigate high CPU utilization of a firewall?

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

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

QUESTION 128
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 tracerouute 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

Correct Answer: A
Section:
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."

QUESTION 129
A security engineer is installing a new IOS on the network. The engineer has asked a network administrator to ensure all traffic entering and leaving the router interface is available for the IDS. Which of the following should the network administrator do?

A. Install a network tap for the IDS
B. Configure ACLs to route traffic to the IDS.
C. Install an additional NIC into the IDS
D. Install a loopback adapter for the IDS.
E. Add an additional route on the router for the IDS.

Correct Answer: A
Section:
Explanation:
a network tap is a way of connecting an IDS out of band, which means it does not interfere with the normal network traffic. A network tap allows you to view a copy of the network traffic transmitted over the media being tapped.

QUESTION 130
A network technician is planning a network scope. The web server needs to be within 12.31 69.1 to 12.31.69.29. Which of the following would meet this requirement?

A. Lease time
B. Range reservation
C. DNS
D. Superscope

Correct Answer: A
Section:

QUESTION 131
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

Correct Answer: D
Section:

QUESTION 132
A network technician receives a report about a performance issue on a client PC that is connected to port 1/3 on a network switch. The technician observes the following configuration output from the switch:

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

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

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

Correct Answer: A
Section:

QUESTION 133
Which of the following must be functioning properly in order for a network administrator to create an accurate timeline during a troubleshooting process?

A. NTP
B. IP helper
C. Syslog
D. MySQL

Correct Answer: C
Section:
Explanation:

QUESTION 134
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

Correct Answer: B, C
Section:

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.

QUESTION 135
Which of the following is considered a physical security detection device?

A. Cameras
B. Biometric readers
C. Access control vestibules
D. Locking racks

Correct Answer: A
Section:

QUESTION 136
A network administrator is trying to add network redundancy for the server farm. Which of the following can the network administrator configure to BEST provide this capability?

A. VRRP
B. DNS
C. UPS
D. RPO

Correct Answer: A
Section:
Explanation:
VRRP is an open standard protocol, which is used to provide redundancy in a network. It is a network layer protocol (protocol number-112). The number of routers (group members) in a group acts as a virtual logical router which will be the default gateway of all the local hosts. If one router goes down, one of the other group members can take place for the responsibilities for forwarding the traffic.

QUESTION 137
The power company notifies a network administrator that it will be turning off the power to the building over the weekend. Which of the following is the BEST solution to prevent the servers from going down?

A. Redundant power supplies
B. Uninterruptible power supply
C. Generator
D. Power distribution unit

Correct Answer: A
Section:

QUESTION 138
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

Correct Answer: A
Section:

QUESTION 139
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

Correct Answer: C
Section:

QUESTION 140
A security engineer is trying to determine whether an internal server was accessed by hosts on the internet. The internal server was shut down during the investigation Which of the following will the engineer review to determine whether the internal server had an unauthorized access attempt?

A. The server's syslog
B. The NetFlow statistics
C. The firewall logs
D. The audit logs on the core switch

Correct Answer: A
Section:

QUESTION 141
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

Correct Answer: B
Section:

QUESTION 142
A company joins a bank's financial network and establishes a connection to the clearinghouse servers in the range 192 168.124.0/27. An IT technician then realizes the range exists within the VM pool at the data center. Which of the following is the BEST way for the technician to connect to the bank's servers?

A. NAT
B. PAT
C. CIDR
D. SLAAC

Correct Answer: A
Section:

QUESTION 143
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

Correct Answer: A
Section:

QUESTION 144
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

Correct Answer: B
Section:

QUESTION 145
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

Correct Answer: B
Section:

QUESTION 146
At which of the following OSI model layers does routing occur?

A. Data link

B. Transport
C. Physical
D. Network

Correct Answer: D
Section:

QUESTION 147
A network technician has determined the cause of a network disruption. Which of the following is the NEXT step for the technician to perform?

A. Validate the findings in a top-to-bottom approach
B. Duplicate the issue, if possible
C. Establish a plan of action to resolve the issue
D. Document the findings and actions

Correct Answer: C
Section:

QUESTION 148
A company streams video to multiple devices across a campus. When this happens, several users report a degradation of network performance. Which of the following would MOST likely address this issue?

A. Enable IGMP snooping on the switches.
B. Implement another DHCP server.
C. Reconfigure port tagging for the video traffic.
D. Change the SSID of the APs

Correct Answer: A
Section:

QUESTION 149
Which of the following can be used to store various types of devices and provide contactless delivery to users?

A. Asset tags
B. Biometrics
C. Access control vestibules
D. Smart lockers

Correct Answer: D
Section:

QUESTION 150
Which of the following connectors and terminations are required to make a Cat 6 cable that connects from a PC to a non-capable MDIX switch? (Select TWO).

A. T1A-568-A - TIA-568-B
B. TIA-568-B - TIA-568-B
C. RJ11
D. RJ45

E. F-type

Correct Answer: A, D
Section:

QUESTION 151
Users are reporting intermittent Wi-Fi connectivity in specific parts of a building. Which of the following should the network administrator check FIRST when troubleshooting this issue? (Select TWO).

A. Site survey
B. EIRP
C. AP placement
D. Captive portal
E. SSID assignment
F. AP association time

Correct Answer: A, C
Section:
Explanation:
This is a coverage issue. WAP placement and power need to be checked. Site survey should be done NEXT because it takes a while.

QUESTION 152
A network manager is configuring switches in IDFs to ensure unauthorized client computers are not connecting to a secure wired network. Which of the following is the network manager MOST likely performing?

A. Disabling unneeded switchports
B. Changing the default VLAN
C. Configuring DHCP snooping
D. Writing ACLs to prevent access to the switch

Correct Answer: C
Section:

QUESTION 153
Which of the following OSI model layers is where a technician would view UDP information?

A. Physical
B. Data link
C. Network
D. Transport

Correct Answer: D
Section:

QUESTION 154
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

Correct Answer: B
Section:

QUESTION 155
A company wants to add a local redundant data center to its network in case of failure at its primary location. Which of the following would give the LEAST amount of redundancy for the company's network?

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

Correct Answer: A
Section:

QUESTION 156
A technician was cleaning a storage closet and found a box of transceivers labeled 8Gbps. Which of the following protocols uses those transceivers?

A. Coaxial over Ethernet
B. Internet Small Computer Systems Interface
C. Fibre Channel
D. Gigabit interface converter

Correct Answer: C
Section:
Explanation:
The transceivers labeled 8Gbps are likely to be used with the Fibre Channel protocol. Fibre Channel is a high-speed networking technology that is primarily used to connect storage devices to servers in storage area networks (SANs). It is capable of transmitting data at speeds of up to 8 Gbps (gigabits per second), and uses specialized transceivers to transmit and receive data over fiber optic cables.
Coaxial over Ethernet (CoE) is a networking technology that uses coaxial cables to transmit data, and is not related to the transceivers in question. Internet Small Computer Systems Interface (iSCSI) is a protocol that allows devices to communicate over a network using the SCSI protocol, and does not typically use specialized transceivers. Gigabit interface converter (GBIC) is a type of transceiver used to transmit and receive data over fiber optic cables, but it is not capable of transmitting data at 8 Gbps.

QUESTION 157
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

Correct Answer: B
Section:
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.
Reference: Network+ Study Guide Objective 5.1: Summarize the importance of physical security controls.

QUESTION 158
During an annual review of policy documents, a company decided to adjust its recovery time frames. The company agreed that critical applications can be down for no more than six hours, and the acceptable amount of data loss is no more than two hours. Which of the following should be documented as the RPO?

A. Two hours
B. Four hours
C. Six hours
D. Eight hours

Correct Answer: A
Section:
Explanation:
" RPO designates the variable amount of data that will be lost or will have to be re-entered during network downtime. RTO designates the amount of "real time" that can pass before the disruption begins to seriously and unacceptably impede the flow of normal business operations."

QUESTION 159
A new global ISP needs to connect from central offices in North America to the United Kingdom. Which of the following would be the BEST cabling solution for this project?

A. Single-mode
B. Coaxial
C. Cat 6a
D. Twinaxial

Correct Answer: A
Section:
Explanation:
For a new global ISP to connect from central offices in North America to the United Kingdom, the best cabling solution would be single-mode fiber optic cable. Single-mode fiber optic cable is a type of cable that is used to transmit data over long distances using light signals. It is typically used in long-haul communication networks, such as those that connect different countries or continents.

QUESTION 160
Which of the following would be BEST to install to find and block any malicious users within a network?

A. IDS
B. IPS
C. SCADA
D. ICS

Correct Answer: B
Section:
Explanation:
IPS takes action itself to block the attempted intrusion or otherwise remediate the incident. IDS is designed to only provide an alert about a potential incident, which enables a security operations center (SOC) analyst to investigate the event and determine whether it requires further action.

QUESTION 161
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

Correct Answer: A
Section:
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.

QUESTION 162
A network technician is troubleshooting a new web server connectivity issue. The network technician discovers the following on the support ticket
• The server's IP address can be pinged from the client PCs,
• Access to the web resource works correctly when on the server's console.
• No clients can access the servers data via URL.
• The server does not have a firewall configured
• No ACLs are preventing connectivity from the client's network.
• All services on the server are operating normally,
which was confirmed by the server team.
Which of the following actions will resolve the issue?

A. Reset port security on the switchport connecting the server.
B. Adjust the web server's NTP settings to match the client settings.
C. Configure A records for the web server.
D. Install the correct MIB on the web server

Correct Answer: C
Section:
Explanation:
The problem is likely related to DNS resolution, as the clients are able to ping the server's IP address but not access the web resource via URL. The other answers do not address this issue. Configuring A records for the web server will ensure that clients are able to access the web resource via its domain name.

QUESTION 163
A Chief Executive Officer and a network administrator came to an agreement With a vendor to purchase new equipment for the data center A document was drafted so all parties would be Informed about the scope of the project before It started. Which of the following terms BEST describes the document used?

A. Contract
B. Project charter

C. Memorandum of understanding
D. Non-disclosure agreement

Correct Answer: B
Section:
Explanation:
The document used to inform all parties about the scope of the project before it starts is likely a project charter.
A project charter is a document that outlines the key aspects of a project, including the project's objectives, scope, stakeholders, and resources. It serves as a formal agreement between the project team and the stakeholders, and helps to define the project's goals and constraints.
A project charter typically includes information about the project's scope, including the specific deliverables that are expected and any constraints or limitations that may impact the project. It may also include details about the project team and stakeholders, the project schedule and budget, and the roles and responsibilities of each party.
By creating a project charter, the Chief Executive Officer and the network administrator can ensure that all parties involved in the project have a clear understanding of the project's goals and objectives, and can help to prevent misunderstandings or miscommunications during the project. What is in a project charter?
A project charter is a formal short document that states a project exists and provides project managers with written authority to begin work. A project charter document describes a project to create a shared understanding of its goals, objectives and resource requirements before the project is scoped out in detail.
What are the 5 elements of the project charter?
What Are the Contents of a Project Charter? A project charter should always include an overview, an outline of scope, an approximate schedule, a budget estimate, anticipated risks, and key stakeholders

QUESTION 164
A technician is trying to install a VoIP phone, but the phone is not turning on. The technician checks the cable gong from the phone to the switch, and the cable is good. Which of the following actions IS needed for this phone to work?

A. Add a POE injector
B. Enable MDIX.
C. Use a crossover cable.
D. Reconfigure the port.

Correct Answer: A
Section:

QUESTION 165
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

Correct Answer: B, E
Section:

QUESTION 166
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

Correct Answer: A
Section:

QUESTION 167
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

Correct Answer: C
Section:

QUESTION 168
A network administrator needs to configure a server to use the most accurate NTP reference available. Which of the following NTP devices should the administrator select?

A. Stratum 1
B. Stratum 2
C. Stratum 3
D. Stratum 4

Correct Answer: A
Section:
Explanation:
Stratum 1 devices are the most accurate ntp time sources accessible via a network connection. A Stratum 1 device would normally be synchronised via a Stratum 0 reference clock.
Reference: https://endruntechnologies.com/products/ntp-time-servers/stratum1

QUESTION 169
A Fortune 500 firm is deciding On the kind or data center equipment to install given its five-year budget Outlook. The Chief Information comparing equipment based on the life expectancy Of different models. Which Of the following concepts BEST represents this metric?

A. MTBF
B. MTRR
C. RPO
D. RTO

Correct Answer: A
Section:

QUESTION 170
While setting up a new workstation, a technician discovers that the network connection is only 100 full duplex (FD), although it is connected to a gigabit switch.
While reviewing the interface information in the switch CLI, the technician notes the port is operating at IOOFD but Shows many RX and TX errors. The technician moves the computer to another switchport and experiences

the same issues.
Which of the following is MOST likely the cause of the low data rate and port errors?

A. Bad switch ports
B. Duplex issues
C. Cable length
D. Incorrect pinout

Correct Answer: B
Section:

QUESTION 171
A network administrator wants to check all network connections and see the output in integer form. Which of the following commands should the administrator run on the command line?

A. netstat
B. netstat -a
C. netstat —e
D. netstat —n

Correct Answer: A
Section:

QUESTION 172
A Network engineer is investigating issues on a Layer 2 Switch. The department typically snares a Switchport during meetings for presentations, but atter the first user Shares, no Other users can connect. Which Of the following is MOST likely related to this issue?

A. Spanning Tree Protocol is enabled on the switch.
B. VLAN trunking is enabled on the switch.
C. Port security is configured on the switch.
D. Dynamic ARP inspection is configured on the switch.

Correct Answer: C
Section:

QUESTION 173
Which of the following would MOST likely utilize PoE?

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

Correct Answer: A
Section:
Explanation:
A camera is most likely to utilize PoE (Power over Ethernet). PoE is a technology that allows electrical power to be delivered over Ethernet cables. It is used to power a variety of devices, such as cameras, phones, access points, and other networking equipment.Cameras are particularly well-suited for PoE because they are often installed in locations where it is difficult or impossible to run electrical power. By using PoE, cameras can be

powered directly over the Ethernet cable, eliminating the need for separate power cables and outlets.Other devices, such as printers, hubs, and modems, are less likely to utilize PoE because they typically do not need to be powered over Ethernet. These devices are usually powered by AC (alternating current) power and are typically connected to a power outlet rather than an Ethernet cable.

QUESTION 174
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

Correct Answer: A
Section:

QUESTION 175
A network engineer needs to pass both data and telephony on an access port. Which or the following features should be configured to meet this requirement?

A. VLAN
B. VoIP
C. VIP
D. VRRP

Correct Answer: A
Section:

QUESTION 176
A technician is troubleshooting a connectivity issue with an end user. The end user can access local network shares and intranet pages but is unable to access the internet or remote resources. Which of the following needs to be reconfigured?

A. The IP address
B. The subnet mask
C. The gateway address
D. The DNS servers

Correct Answer: C
Section:

QUESTION 177
Which of the following protocols can be used to change device configurations via encrypted and authenticated sessions? (Select TWO).

A. SNMPv3
B. SSh
C. Telnet
D. IPSec
E. ESP
F. Syslog

Correct Answer: B, D
Section:

QUESTION 178
A technician wants to monitor and provide traffic segmentation across the network. The technician would like to assign each department a specific identifier. Which of the following will the technician MOST likely use?

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

Correct Answer: C
Section:
Explanation:
To monitor and provide traffic segmentation across the network, a technician may use the concept of VLANs (Virtual Local Area Networks). VLANs are a way of dividing a single physical network into multiple logical networks, each with its own unique identifier or "tag."
By assigning each department a specific VLAN identifier, the technician can segment the network traffic and ensure that the different departments' traffic is kept separate from one another. This can help to improve network security, performance, and scalability, as well as allowing for better monitoring and control of the network traffic.
To implement VLANs, the technician will need to configure VLAN tagging on the network devices, such as switches and routers, and assign each department's devices to the appropriate VLAN. The technician may also need to configure VLAN trunking to allow the different VLANs to communicate with each other.
By using VLANs, the technician can effectively monitor and segment the network traffic, providing better control and visibility into the network.

QUESTION 179
Which of the following is used to elect an STP root?

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

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

QUESTION 180
A network technician needs to ensure that all files on a company's network can be moved in a safe and protected manner without interception from someone who is not the intended recipient. Which of the following would allow the network technician to meet these requirements?

A. FTP
B. TFTP
C. SMTP
D. SFTP

Correct Answer: D
Section:

QUESTION 181
Which of the following is MOST appropriate for enforcing bandwidth limits when the performance of an application is not affected by the use of buffering but is heavily impacted by packet drops?

A. Traffic shaping
B. Traffic policing
C. Traffic marking
D. Traffic classification

Correct Answer: B
Section:
Explanation:
Traffic policing is a mechanism that monitors the traffic in any network and enforces a bandwidth limit by discarding packets that exceed a certain rate1. This can reduce congestion and ensure fair allocation of bandwidth among different applications or users. However, discarding packets can also affect the performance and quality of some applications, especially those that are sensitive to packet loss, such as voice or video.
Traffic shaping is a congestion control mechanism that delays packets that exceed a certain rate instead of discarding them1. This can smooth out traffic bursts and avoid packet loss, but it also introduces latency and jitter. Traffic shaping can be beneficial for applications that can tolerate some delay but not packet loss, such as file transfers or streaming. Traffic marking is a mechanism that assigns different priority levels to packets based on their type, source, destination, or other criteria2. This can help to differentiate between different classes of service and apply different policies or treatments to them. However, traffic marking does not enforce bandwidth limits by itself; it only provides information for other mechanisms to act upon. Traffic classification is a process that identifies and categorizes packets based on their characteristics, such as protocol, port number, payload, or behavior. This can help to distinguish between different types of traffic and apply appropriate policies or actions to them. However, traffic classification does not enforce bandwidth limits by itself; it only provides input for other mechanisms to use.

QUESTION 182
Which of the following documents would be used to define uptime commitments from a provider, along with details on measurement and enforcement?

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

Correct Answer: B
Section:
Explanation:
A service level agreement (SLA) is a document that is used to define uptime commitments from a provider, along with details on measurement and enforcement. An SLA is a contract between a service provider and a customer that outlines the level of service that the provider is committed to providing and the terms under which that service will be delivered.

QUESTION 183
A company ranis out a largo event space and includes wireless internet access for each tenant. Tenants reserve a two-hour window from the company each week, which includes a tenant-specific SSID However, all users share the company's network hardware.

Wireless encryption	WPA2
Captive portal	Disabled
AP isolation	Enabled
Subnet mask	255.255.255.0
DNS server	10.0.0.1
Default gateway	10.1.10.1
DHCP scope begin	10.1.10.10
DHCP scope end	10.1.10.150
DHCP lease time	24 hours

The network support team is receiving complaints from tenants that some users are unable to connect to the wireless network Upon investigation, the support teams discovers a pattern indicating that after a tenant with a particularly large attendance ends its sessions, tenants throughout the day are unable to connect.

The following settings are common lo all network configurations:
Which of the following actions would MOST likely reduce this Issue? (Select TWO).

A. Change to WPA encryption
B. Change the DNS server to 10.1.10.1.
C. Change the default gateway to 10.0.0.1.
D. Change the DHCP scope end to 10.1.10.250
E. Disable AP isolation
F. Change the subnet mask lo 255.255.255.192.
G. Reduce the DHCP lease time to four hours.

Correct Answer: D, G
Section:

QUESTION 184
Which of the following would be increased by adding encryption to data communication across the network?

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

Correct Answer: D
Section:
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.
Reference: Network+ Study Guide Objective 4.1: Summarize the purposes of physical security devices. Subobjective: Encryption.

QUESTION 185
Which of the following uses the link-state routing algorithm and operates within a single autonomous system?

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

Correct Answer: B
Section:
Explanation:
OSPF uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks

QUESTION 186
A large metropolitan city is looking to standardize the ability tor 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

Correct Answer: B
Section:

QUESTION 187
A customer wants to log in t o a vendor's server using a web browser on a laptop. Which of the following would require the LEAST configuration to allow encrypted access to the server?

A. Secure Sockets Layer
B. Site-to-site VPN
C. Remote desktop gateway
D. Client-to-site VPN

Correct Answer: A
Section:
Explanation:
SSL is a widely used protocol for establishing secure, encrypted connections between devices over the Internet. It is typically used to secure communication between web browsers and servers, and can be easily enabled on a server by installing an SSL certificate.

QUESTION 188
Which of the following would be the MOST likely attack used to bypass an access control vestibule?

A. Tailgating
B. Phishing
C. Evil twin
D. Brute-force

Correct Answer: A
Section:
Explanation:
Tailgating is when someone follows an authorized person into a restricted area without having the proper credentials. This is usually done by pretending to be with the authorized person, or by offering assistance. Tailgating is a social engineering attack and does not require any technical skill.

QUESTION 189
A network administrator received a report staling a critical vulnerability was detected on an application that is exposed to the internet. Which of the following Is the appropriate NEXT step?

A. Check for the existence of a known exploit in order to assess the risk
B. Immediately shut down the vulnerable application server.
C. Install a network access control agent on the server.
D. Deploy a new server to host the application.

Correct Answer: A
Section:

Explanation:
The appropriate next step in this situation would be to check for the existence of a known exploit in order to assess the risk. This is important because it will help the network administrator determine the severity of the vulnerability and the potential impact it could have on the organization. Once the network administrator has assessed the risk, they can then take appropriate action to address the vulnerability. This might include patching the application, deploying a new server to host the application, or implementing other security measures to mitigate the risk. It is generally not advisable to immediately shut down the vulnerable application server, as this could disrupt business operations and cause significant downtime. Similarly, installing a network access control agent on the server may not be the most effective solution, as it would not address the underlying vulnerability.

QUESTION 190
While waking from the parking lot lo an access-controlled door an employee sees an authorized user open the door. Then the employee notices that another person catches the door before It closes and goes inside Which of the following attacks Is taking place?

A. Tailgating
B. Pipgybacking
C. Shoulder surfing
D. Phisning

Correct Answer: A
Section:
Explanation:
The difference between piggybacking and tailgaiting is that with piggybacking, the person is willfully and intentionally letting you in. In this particular case, the person caught the door before it closed, so it is tailgating.
Tailgating is a physical security attack that occurs when an unauthorized person follows an authorized person through a secured door or gate without their knowledge or consent. Tailgating can allow an attacker to bypass access control mechanisms and gain entry to restricted areas or resources. Tailgating can also pose a safety risk for the authorized person and other occupants of the facility. Piggybacking is a physical security attack that occurs when an unauthorized person follows an authorized person through a secured door or gate with their knowledge or consent. Piggybacking can also allow an attacker to bypass access control mechanisms and gain entry to restricted areas or resources. Piggybacking can also violate security policies and compromise the accountability of the authorized person.
Shoulder surfing is a physical security attack that occurs when an unauthorized person observes or records an authorized person's confidential information, such as passwords, PINs, or credit card numbers. Shoulder surfing can allow an attacker to steal credentials and access sensitive data or systems. Shoulder surfing can also violate privacy and confidentiality rights of the authorized person. Phishing is a cyber security attack that occurs when an unauthorized person sends fraudulent emails or messages that appear to come from legitimate sources, such as banks, companies, or government agencies. Phishing can trick recipients into clicking on malicious links, opening malicious attachments, or providing personal or financial information. Phishing can allow an attacker to install malware, steal credentials, or perform identity theft. Phishing does not involve physical access to secured doors or gates.

QUESTION 191
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

Correct Answer: A
Section:
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.

QUESTION 192
A network engineer needs to create a subnet that has the capacity for five VLANs. with the following number of clients lo be allowed on each:

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

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

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

Correct Answer: B
Section:

QUESTION 193
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

Correct Answer: A
Section:

QUESTION 194
Which of the following bandwidth management techniques uses buffers al 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

Correct Answer: D
Section:

QUESTION 195
A network administrator is getting reports of some internal users who cannot connect to network resources. The users slate they were able to connect last week, but not today. No changes have been configured on the network devices or server during the last few weeks. Which of the following is the MOST likely cause of the issue?

A. The client DHCP scope is fully utilized
B. The wired network is experiencing electrical interference
C. The captive portal is down and needs to be restarted
D. SNMP traps are being received

E. The packet counter on the router interface is high.

Correct Answer: A
Section:

QUESTION 196
A technician is investigating packet loss to a device that has varying data bursts throughout the day. Which of the following will the technician MOST likely configure to resolve the issue?

A. Flow control
B. Jumbo frames
C. Duplex
D. Port mirroring

Correct Answer: A
Section:
Explanation:
Ethernet flow control is a mechanism for temporarily stopping the transmission of data on Ethernet family computer networks. The goal of this mechanism is to avoid packet loss in the presence of network congestion.
Flow control is a mechanism that allows a device to regulate the amount of data it receives from another device, ensuring that the receiving device is not overwhelmed with data. If the device experiencing packet loss is receiving large bursts of data at times when it is not able to process it quickly enough, configuring flow control could help prevent packets from being lost.
"In theory, flow control can help with situations like a host that can't keep up with the flow of traffic. It enables the host to send an Ethernet PAUSE frame, which asks the switch to hold up for some amount of time so the host can catch its breath. If the switch can, it'll buffer transmissions until the pause expires, and then start sending again. If the host catches up early, it can send another PAUSE frame with a delay of zero to ask the switch to resume. In practice, flow control can cause latency trouble for modern real-time applications such as VoIP, and the same needs are usually met by QoS"

QUESTION 197
A network administrator needs to provide evidence to confirm that recent network outages were caused by increased traffic generated by a recently released application. Which of the following actions will BEST support the administrator's response?

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

Correct Answer: C
Section:

QUESTION 198
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

Correct Answer: C
Section:

QUESTION 199
A network security engineer locates an unapproved wireless bridge connected to the corporate LAN that is broadcasting a hidden SSID, providing unauthenticated access to internal resources. Which of the following types of

attacks BEST describes this finding?

A. Rogue access point Most Voted
B. Evil twin
C. ARP spoofing
D. VLAN hopping

Correct Answer: A
Section:
Explanation:
A rogue access point is an illegitimate access point plugged into a network to create a bypass from outside into the legitimate network. By contrast, an evil twin is a copy of a legitimate access point.

QUESTION 200
Which of the following is an example of on-demand scalable hardware that is typically housed in the vendor's data center?

A. DaaS
B. IaaS
C. PaaS
D. SaaS

Correct Answer: B
Section:

QUESTION 201
A network device needs to discover a server that can provide it with an IPv4 address. Which of the following does the device need to send the request to?

A. Default gateway
B. Broadcast address
C. Unicast address
D. Link local address

Correct Answer: B
Section:
Explanation:
The DHCP client sends broadcast request packets to the network; the DHCP servers respond with broadcast packets that offer IP parameters, such as an IP address for the client. After the client chooses the IP parameters, communication between the client and server is by unicast packets. "When a DHCP client boots up, it automatically sends out a DHCP Discover UDP datagram to the broadcast address, 255.255.255.255. This DHCP Discover message asks “Are there any DHCP servers out there?” The client can’t send unicast traffic yet, as it doesn’t have a valid IP address that can be used."

QUESTION 202
Which of the following is a valid and cost-effective solution to connect a fiber cable into a network switch without available SFP ports?

A. Use a media converter and a UTP cable
B. Install an additional transceiver module and use GBICs
C. Change the type of connector from SC to F-type
D. Use a loopback adapter to make the connection

Correct Answer: A

Section:

QUESTION 203
Which of the following would be BEST suited for a long cable run with a 40Gbps bandwidth?

A. Cat 5e
B. Cat 6a
C. Cat 7
D. Cat 8

Correct Answer: C
Section:
Explanation:
Cat 7 is a type of twisted-pair copper cable that supports up to 40 Gbps bandwidth and up to 100 meters cable length. Cat 7 is suitable for long cable runs that require high-speed data transmission. Cat 7 has better shielding and crosstalk prevention than lower categories of cables.
Reference: Network+ Study Guide Objective 1.5: Compare and contrast network cabling types, features and their purposes.

QUESTION 204
Which of the following would enable a network technician to implement dynamic routing?

A. An IPS
B. A bridge
C. A Layer 3 switch
D. A hub

Correct Answer: C
Section:

QUESTION 205
A WAN technician reviews activity and identifies newly installed hardware that is causing outages over an eight-hour period. Which of the following should be considered FIRST?

A. Network performance baselines
B. VLAN assignments
C. Routing table
D. Device configuration review

Correct Answer: D
Section:

QUESTION 206
A network technician recently installed 35 additional workstations. After installation, some users are unable to access network resources. Many of the original workstations that are experiencing the network access issue were offline when the new workstations were turned on. Which of the following is the MOST likely cause of this issue?

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

Correct Answer: B
Section:

QUESTION 207
A network administrator is investigating a network event that is causing all communication to stop. The network administrator is unable to use SSH to connect to the switch but is able to gain access using the serial console port. While monitoring port statistics, the administrator sees the following:

Total Rx (bps)	23,041,464	Total Tx (bps)	621,032
Unicast Rx (Pkts/sec)	102,465	Unicast Tx (Pkts/sec)	66
B/Mcast Rx (Pkts/sec)	21,456.465	B/Mcast Tx (Pkts/sec)	7
Utilization Rx	2.3%	Utilization Tx	0.06%

Which of the following is MOST likely causing the network outage?

A. Duplicate IP address
B. High collisions
C. Asynchronous route
D. Switch loop

Correct Answer: B
Section:

QUESTION 208
A network administrator has received calls every day for the past few weeks from three users who cannot access the network. The administrator asks all the users to reboot their PCs, but the same users still cannot access the system. The following day, three different users report the same issue, and the administrator asks them all to reboot their PCs; however, this does not fix the issue. Which of the following is MOST likely occurring?

A. Incorrect firewall settings
B. Inappropriate VLAN assignment
C. Hardware failure
D. Overloaded CAM table in switch
E. DHCP scope exhaustion

Correct Answer: E
Section:

QUESTION 209
An administrator wants to increase the availability of a server that is connected to the office network. Which of the following allows for multiple NICs to share a single IP address and offers maximum performance while providing fault tolerance in the event of a NIC failure?

A. Multipathing
B. Spanning Tree Protocol

C. First Hop Redundancy Protocol
D. Elasticity

Correct Answer: A
Section:
Explanation:
Reference: https://docs.oracle.com/cd/E19455-01/806-6547/6jffv7oma/index.html

QUESTION 210
A Wi-Fi network was originally configured to be able to handle interference from a microwave oven. The microwave oven was recently removed from the office. Now the network administrator wants to optimize the system to maximize the range of the signal. The main sources of signal degradation are the numerous cubicles and wooden walls between the WAP and the intended destination. Which of the following actions should the administrator take?

A. Implement CDMA.
B. Change from omni to directional.
C. Change the SSID.
D. Change the frequency.

Correct Answer: D
Section:
Explanation:
- the microwave was already removed from the office
- the signal is OK now
- Notice that the question mentions "numerous cubicles and wooden walls" - meaning the signal now won't have the interference as before
- KEY POINT: the admin wants to "maximize the range of the signal:"
Manually change the frequency to 2.4 GHz for more reliable speeds and range. While 5 GHz gives you a stronger signal, it doesn't travel through walls or ceilings as well, so it doesn't give you the best range.
"Microwave ovens: Older microwave ovens, which might not have sufficient shielding, can emit relatively high-powered signals in the 2.4GHz band, resulting in significant interference with WLAN devices operating in the 2.4GHz band."

QUESTION 211
A company has wireless APS that were deployed with 802.11g. A network engineer has noticed more frequent reports of wireless performance issues during the lunch hour in comparison to the rest of the day. The engineer thinks bandwidth consumption will increase while users are on their breaks, but network utilization logs do not show increased bandwidth numbers. Which Of the following would MOST likely resolve this issue?

A. Adding more wireless APS
B. Increasing power settings to expand coverage
C. Configuring the APS to be compatible with 802.1la
D. Changing the wireless channel used

Correct Answer: C
Section:
Explanation:
802.11g is an older wireless standard that operates in the 2.4 GHz frequency band and has a maximum data rate of 54 Mbps. 802.11a is a newer wireless standard that operates in the 5 GHz frequency band and has a maximum data rate of 54 Mbps. By configuring the APS to be compatible with 802.11a, the network engineer can reduce interference and congestion in the 2.4 GHz band and improve wireless performance.
Reference: Network+ Study Guide Objective 2.5: Implement network troubleshooting methodologies

QUESTION 212
A network is secured and is only accessible via TLS and IPSec VPNs. Which of the following would need to be present to allow a user to access network resources on a laptop without logging in to the VPN application?

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

Correct Answer: A
Section:
Explanation:
A site-to-site VPN is a type of VPN that connects two or more networks over the Internet using a secure tunnel. A site-to-site VPN allows users to access network resources on a laptop without logging in to the VPN application, as long as the laptop is connected to one of the networks in the VPN. A site-to-site VPN is transparent to the users and does not require any additional software or configuration on the client devices.
Reference: Network+ Study Guide Objective 3.4: Explain the purposes and use cases for VPNs.

QUESTION 213
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

Correct Answer: A
Section:
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.
Reference: Network+ Study Guide Objective 3.1: Explain the purposes and use cases for advanced networking devices.

QUESTION 214
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

Correct Answer: A
Section:
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.
Reference: Network+ Study Guide Objective 2.2: Explain the concepts and characteristics of routing and switching.

QUESTION 215
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

Correct Answer: C
Section:
Explanation:

QUESTION 216
An engineer is using a tool to run an ICMP sweep of a network to find devices that are online. When reviewing the results, the engineer notices a number of workstations that are currently verified as being online are not listed in the report.
The tool was configured to scan using the following information:
Network address: 172.28.16.0
CIDR: /22
The engineer collected the following information from the client workstation:
IP address: 172.28.17.206
Subnet mask: 255.255.252.0
Which of the following MOST likely explains why the tool is failing to detect some workstations?

A. The scanned network range is incorrect.
B. The subnet mask on the client is misconfigured.
C. The workstation has a firewall enabled.
D. The tool is unable to scan remote networks.

Correct Answer: C
Section:
Explanation:
A firewall is a device or software that filters and controls the incoming and outgoing network traffic based on predefined rules. A firewall can block ICMP packets, which are used for ping and other diagnostic tools. If the workstation has a firewall enabled, it may not respond to the ICMP sweep and appear as offline. The engineer should check the firewall settings on the workstation and allow ICMP traffic if needed.
Reference: Network+ Study Guide Objective 4.1: Given a scenario, use the appropriate tool.

QUESTION 217
A technician is equipped with a tablet, a smartphone, and a laptop to troubleshoot a switch with the help of support over the phone. However, the technician is having issues interconnecting all these tools in troubleshooting the switch. Which Of the following should the technician use to gain connectivity?

A. PAN
B. WAN
C. LAN
D. MAN

Correct Answer: A
Section:
Explanation:
A PAN stands for Personal Area Network and it is a type of network that connects devices within a small range, such as a few meters. A PAN can use wireless technologies such as Bluetooth or Wi-Fi to interconnect devices such as tablets, smartphones, and laptops. A technician can use a PAN to gain connectivity among these tools and troubleshoot the switch.
Reference: Network+ Study Guide Objective 1.2: Explain devices, applications, protocols and services at their appropriate OSI layers.

QUESTION 218
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. lla
B. 802.11b
C. 802. 11g
D. 802.11 n

Correct Answer: D
Section:
Explanation:
802.11n 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.
Reference: Network+ Study Guide Objective 1.6: Explain the functions of network services.

QUESTION 219
Which of the following documents is MOST likely to be associated with identifying and documenting critical applications?

A. Software development life-cycle policy
B. User acceptance testing plan
C. Change management policy
D. Business continuity plan

Correct Answer: D
Section:
Explanation:
A business continuity plan (BCP) is a document that outlines the procedures and strategies to ensure the continuity of critical business functions in the event of a disaster or disruption. A BCP is most likely to be associated with identifying and documenting critical applications that are essential for the organization's operations and recovery. A BCP also defines the roles and responsibilities of the staff, the backup and restore processes, the communication channels, and the testing and maintenance schedules.
Reference: Network+ Study Guide Objective 5.2: Explain disaster recovery and business continuity concepts.

QUESTION 220
A company is opening a new building on the other side of its campus. The distance from the closest building to the new building is 1,804ft (550m). The company needs to connect the networking equipment in the new building to the Other buildings on the campus without using a repeater. Which Of the following transceivers should the company use?

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

Correct Answer: B
Section:
Explanation:
10GBASE-LR is a standard for 10 Gbps Ethernet over single-mode fiber optic cable. It can support a maximum distance of 6.2 miles (10 km), which is much longer than the distance between the buildings. 10GBASE-SW, 10GBASE-LX4, and 10GBASE-SR are all standards for 10 Gbps Ethernet over multimode fiber optic cable, which have shorter maximum distances ranging from 984ft (300m) to 1,312ft (400m).
Reference: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.5:
Compare and contrast network cabling types, standards and speeds.

QUESTION 221
An IT technician installs five old switches in a network. In addition to the low port rates on these switches, they also have improper network configurations. After three hours, the network becomes overwhelmed by continuous traffic and eventually shuts down. Which Of the following is causing the issue?

A. Broadcast storm
B. Collisions
C. IP settings
D. Routing loops

Correct Answer: A
Section:
Explanation:
A broadcast storm is a situation where a network is flooded with broadcast packets, which are sent to all devices on the network. This can consume bandwidth, cause congestion, and degrade performance. A broadcast storm can be caused by improper network configurations, such as loops or misconfigured switches. In this scenario, the old switches may have created loops or failed to filter broadcast packets, resulting in a broadcast storm that overwhelmed the network.
Reference: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.4:
Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

QUESTION 222
At which of the following OSI model layers does a MAC filter list for a wireless infrastructure operate?

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

Correct Answer: D
Section:
Explanation:
A MAC filter list is a security feature that allows or denies access to a wireless network based on the MAC address of the device. A MAC address is a unique identifier assigned to a network interface card (NIC) at the physical layer of the OSI model. However, MAC filtering operates at the data link layer of the OSI model, where MAC addresses are used to encapsulate and deliver data frames between devices on the same network segment.
Reference: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.1:
Given a scenario, install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.

QUESTION 223
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

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

QUESTION 224
A network administrator notices excessive wireless traffic occurring on an access point after normal business hours. The access point is located on an exterior wall. Which of the following should the administrator do to limit wireless access outside the building?

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

Correct Answer: C
Section:
Explanation:
A directional antenna is a type of antenna that radiates or receives radio waves in a specific direction. This can help limit wireless access outside the building by focusing the signal towards the intended area and reducing the signal strength in other directions. A private VLAN is a feature that isolates network devices within a VLAN. Disabling roaming on the WAP prevents wireless clients from switching to another WAP when the signal is weak. Stopping broadcasting of the SSID hides the network name from wireless clients, but does not prevent them from connecting if they know the SSID.
Reference: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.1:
Given a scenario, install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.

QUESTION 225
A store owner would like to have secure wireless access available for both business equipment and patron use. Which of the following features should be configured to allow different wireless access through the same equipment?

A. MIMO
B. TKIP
C. LTE
D. SSID

Correct Answer: D
Section:
Explanation:
SSID stands for Service Set Identifier and is the name of a wireless network. A wireless access point (WAP) can support multiple SSIDs, which allows different wireless access through the same equipment. For example, the store owner can create one SSID for business equipment and another SSID for patron use, and assign different security settings and bandwidth limits for each SSID. MIMO stands for Multiple Input Multiple Output and is a technology that uses multiple antennas to improve wireless performance. TKIP stands for Temporal Key Integrity Protocol and is an encryption method for wireless networks. LTE stands for Long Term Evolution and is a cellular network technology.
Reference: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.1:
Given a scenario, install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.

QUESTION 226
A network administrator is troubleshooting a client's device that cannot connect to the network. A physical inspection of the switch shows the RJ45 is connected. The NIC shows no activity lights. The network administrator moves the device to another location and connects to the network without issues. Which Of the following tools would be the BEST option for the network administrator to use to further troubleshoot?

A. Tone generator
B. Multimeter

C. Optical time-domain reflectometer
D. Cable tester

Correct Answer: D
Section:
Explanation:
A cable tester is a tool that can verify the integrity and functionality of a network cable. It can measure the electrical characteristics of the cable, such as resistance, capacitance, and impedance, and detect any faults or defects, such as shorts, opens, or crosstalk. A cable tester can help the network administrator troubleshoot the problem by determining if the cable is faulty or not. A tone generator is a tool that can send an audible signal through a cable to help locate and identify it. A multimeter is a tool that can measure voltage, current, and resistance of electrical circuits. An optical time-domain reflectometer (OTDR) is a tool that can test the quality and length of fiber optic cables.
Reference: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.3:
Given a scenario, use the appropriate tool to support wired or wireless networks.

QUESTION 227
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

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

QUESTION 228
An IT technician is working on a support ticket regarding an unreachable web-site. The technician has utilized the ping command to the website, but the site is still unreachable. Which of the following tools should the technician use NEXT?

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

Correct Answer: B
Section:
Explanation:
tracert is a command-line tool that can trace the route of a packet from the source to the destination. It can show the number of hops, the IP address and hostname of each router, and the round-trip time for each hop. tracert can help the technician troubleshoot the unreachable website by identifying where the packet is dropped or delayed along the path. ipconfig is a command-line tool that can display and configure the IP settings of a network interface. arp is a command-line tool that can display and manipulate the Address Resolution Protocol (ARP) cache, which maps IP addresses to MAC addresses. netstat is a command-line tool that can display network connections, routing tables, and statistics.

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

QUESTION 229
A security vendor needs to add a note to the DNS to validate the ownership of a company domain before services begin. Which of the following records did the security company MOST likely ask the company to configure?

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

Correct Answer: A
Section:
Explanation:
TXT stands for Text and is a type of DNS record that can store arbitrary text data associated with a domain name. TXT records can be used for various purposes, such as verifying the ownership of a domain, providing information about a domain, or implementing security mechanisms such as SPF (Sender Policy Framework) or DKIM (DomainKeys Identified Mail). In this scenario, the security company most likely asked the company to configure a TXT record with a specific value that can prove the ownership of the domain. AAAA stands for IPv6 Address and is a type of DNS record that maps a domain name to an IPv6 address. CNAME stands for Canonical Name and is a type of DNS record that maps an alias name to another name. SRV stands for Service and is a type of DNS record that specifies the location of a service on a network.
Reference: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.8:
Explain the purposes and use cases for advanced networking devices.

QUESTION 230
Many IP security cameras use RTSP to control media playback. Which of the following default transport layer port numbers does RTSP use?

A. 445
B. 554
C. 587
D. 5060

Correct Answer: B
Section:
Explanation:
RTSP stands for Real Time Streaming Protocol and is an application-level network protocol designed for controlling media playback on streaming media servers. RTSP uses the default transport layer port number 554 for both TCP and UDP1. Port 445 is used for SMB (Server Message Block), a protocol for file and printer sharing. Port 587 is used for SMTP (Simple Mail Transfer Protocol), a protocol for sending email messages. Port 5060 is used for SIP (Session Initiation Protocol), a protocol for initiating and managing multimedia sessions.
Reference: 1 Real Time Streaming Protocol - Wikipedia
(https://en.wikipedia.org/wiki/Real_Time_Streaming_Protocol)

QUESTION 231
An IT technician needs to increase bandwidth to a server. The server has multiple gigabit ports. Which of the following can be used to accomplish this without replacing hardware?

A. STP
B. 802. IQ
C. Duplex
D. LACP

Correct Answer: D
Section:

Explanation:
LACP stands for Link Aggregation Control Protocol and is a protocol that allows multiple physical ports to be combined into a single logical port. This can increase bandwidth, redundancy, and load balancing for a server. LACP is part of the IEEE 802.3ad standard for link aggregation. STP stands for Spanning Tree Protocol and is a protocol that prevents loops in a network by blocking redundant links. 802.1Q is a standard for VLAN (Virtual Local Area Network) tagging, which allows multiple logical networks to share the same physical infrastructure. Duplex is a mode of communication that determines how data is transmitted and received on a link. Full duplex allows simultaneous transmission and reception, while half duplex allows only one direction at a time.
Reference: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.5:
Compare and contrast network cabling types, standards and speeds.

QUESTION 232
Which of the following protocols uses Dijkstra's algorithm to calculate the LOWEST cost between routers?

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

Correct Answer: B
Section:
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 network1. 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.
Reference: 1 Dijkstra's algorithm - Wikipedia (https://en.wikipedia.org/wiki/Dijkstra%27s_algorithm)

QUESTION 233
A PC and a network server have no network connectivity, and a help desk technician is attempting to resolve the issue. The technician plans to run a constant ping command from a Windows workstation while testing various possible reasons for the connectivity issue. Which of the following should the technician use?

A. ping —w
B. ping -i
C. ping —s
D. ping —t

Correct Answer: D
Section:
Explanation:
ping -t is an option for the ping command in Windows that allows the user to send continuous ping requests to a target until stopped by pressing Ctrl-C. This can help the technician run a constant ping command while testing various possible reasons for the connectivity issue. ping -w is an option for the ping command in Windows that allows the user to specify a timeout value in milliseconds for each ping request. ping -i is an option for the ping command in Linux that allows the user to specify the time interval in seconds between each ping request. ping -s is an option for the ping command in Linux that allows the user to specify the size of the data payload in bytes for each ping request.
Reference: How to Use the Ping Command in Windows - Lifewire (https://www.lifewire.com/ping- command-2618099)

QUESTION 234
A switch is connected to another switch. Incompatible hardware causes a surge in traffic on both switches. Which of the following configurations will cause traffic to pause, allowing the switches to drain buffers?

A. Speed

B. Flow control
C. 802.1Q
D. Duplex

Correct Answer: B
Section:
Explanation:
Flow control is a mechanism that allows a network device to regulate the amount of traffic it can receive or send. Flow control can help prevent congestion and buffer overflow by sending pause frames or signals to the sender when the receiver's buffer is full or nearly full. Flow control can cause traffic to pause, allowing the switches to drain buffers and resume normal operation. Speed is a parameter that determines the data transfer rate of a network link. 802.1Q is a standard for VLAN (Virtual Local Area Network) tagging, which allows multiple logical networks to share the same physical infrastructure. Duplex is a mode of communication that determines how data is transmitted and received on a link. Full duplex allows simultaneous transmission and reception, while half duplex allows only one direction at a time.
Reference: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.5:
Compare and contrast network cabling types, standards and speeds.

QUESTION 235
Classification using labels according to information sensitivity and impact in case of unauthorized access or leakage is a mandatory component of:

A. an acceptable use policy.
B. a memorandum of understanding.
C. data loss prevention,
D. a non-disclosure agreement.

Correct Answer: C
Section:
Explanation:
Data loss prevention (DLP) is a set of tools and processes that aim to prevent unauthorized access or leakage of sensitive information. One of the components of DLP is data classification, which involves labeling data according to its information sensitivity and impact in case of unauthorized disclosure. Data classification helps to identify and protect the most critical and confidential data and apply appropriate security controls and policies.
Reference: Network+ Study Guide Objective 5.1: Explain the importance of policies, processes and procedures for IT governance. Subobjective: Data loss prevention.

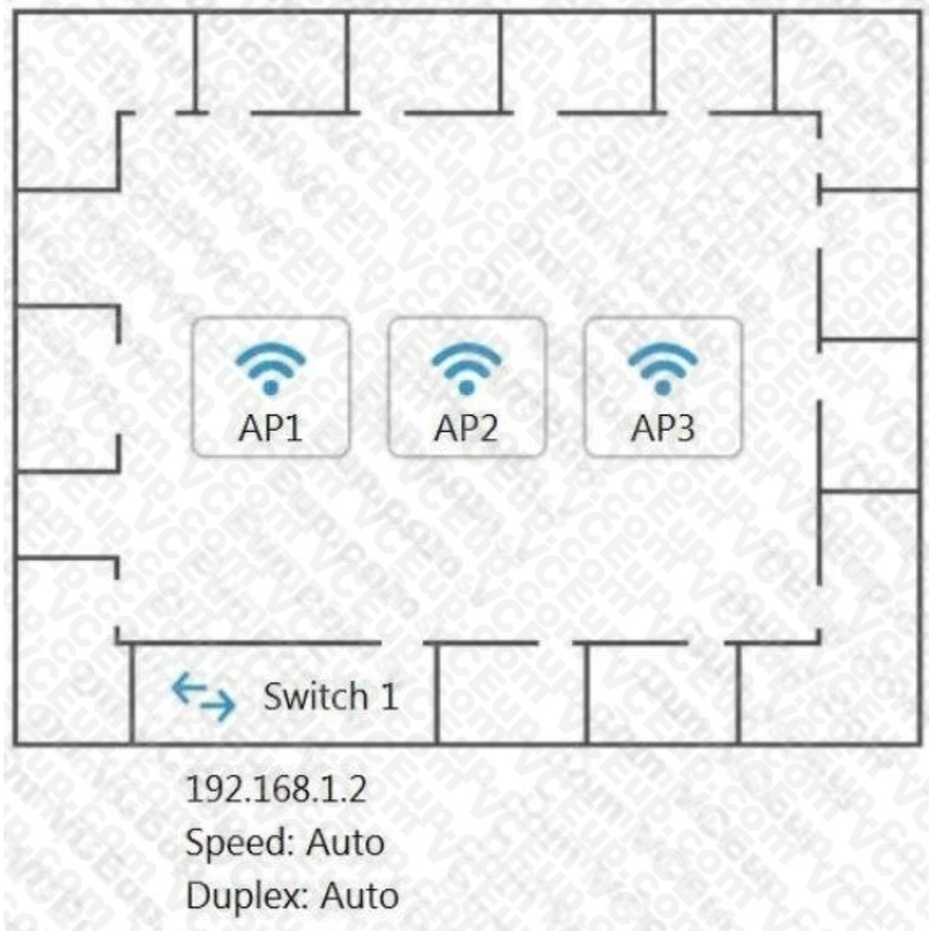
QUESTION 236
A network technician needs to select an AP that will support at least 1.3Gbps and 5GHz only. Which of the following wireless standards must the AP support to meet the requirements?

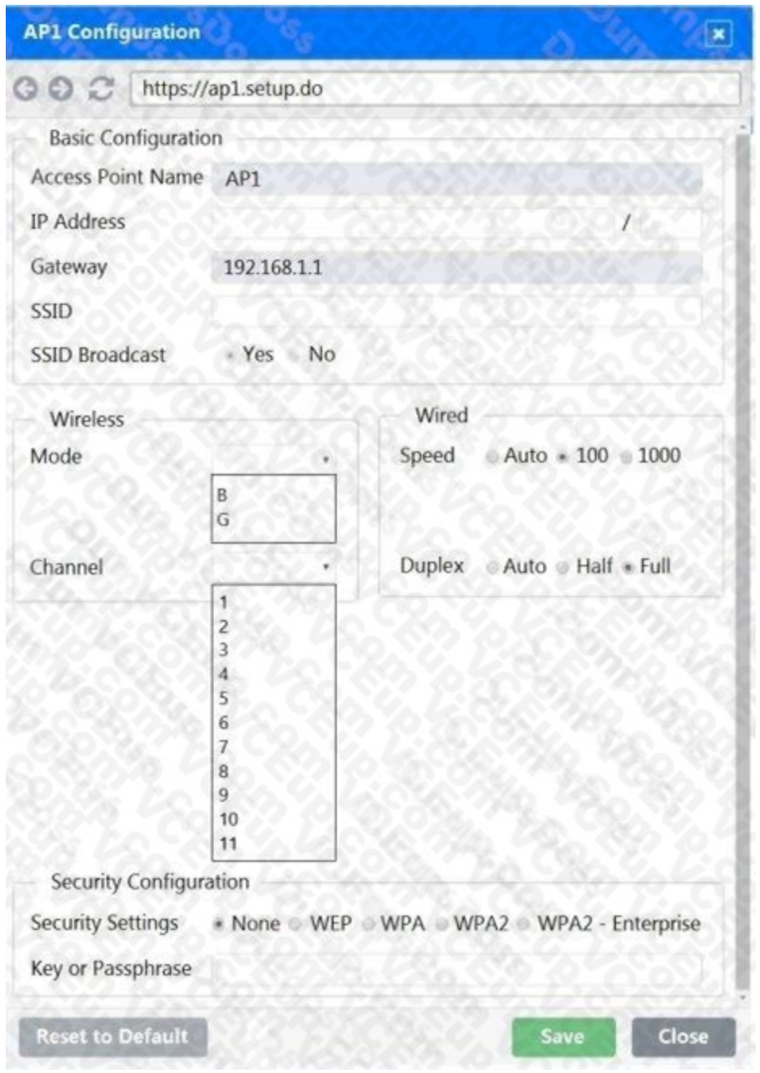
A. B
B. AC
C. AX
D. N
E. G

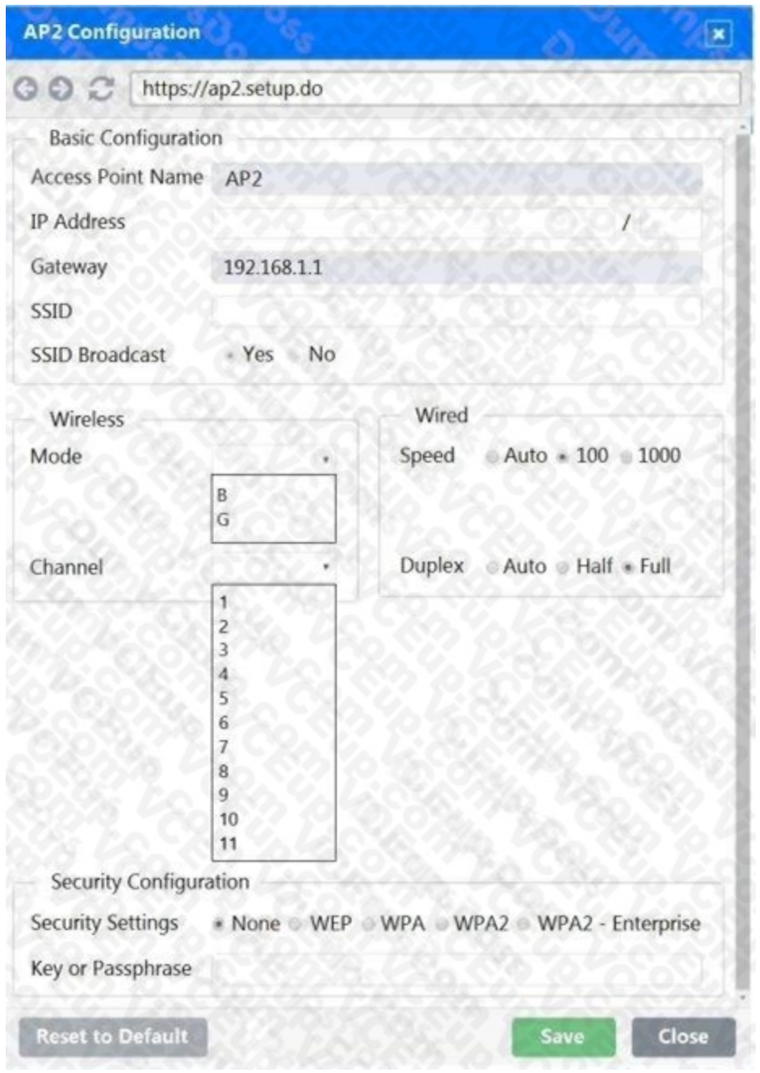
Correct Answer: B
Section:
Explanation:
Wireless AC is a wireless standard that supports up to 1.3Gbps data rate and operates in the 5GHz frequency band only. Wireless AC is also backward compatible with wireless A and N devices that use the 5GHz band. Wireless AC is suitable for high-performance applications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

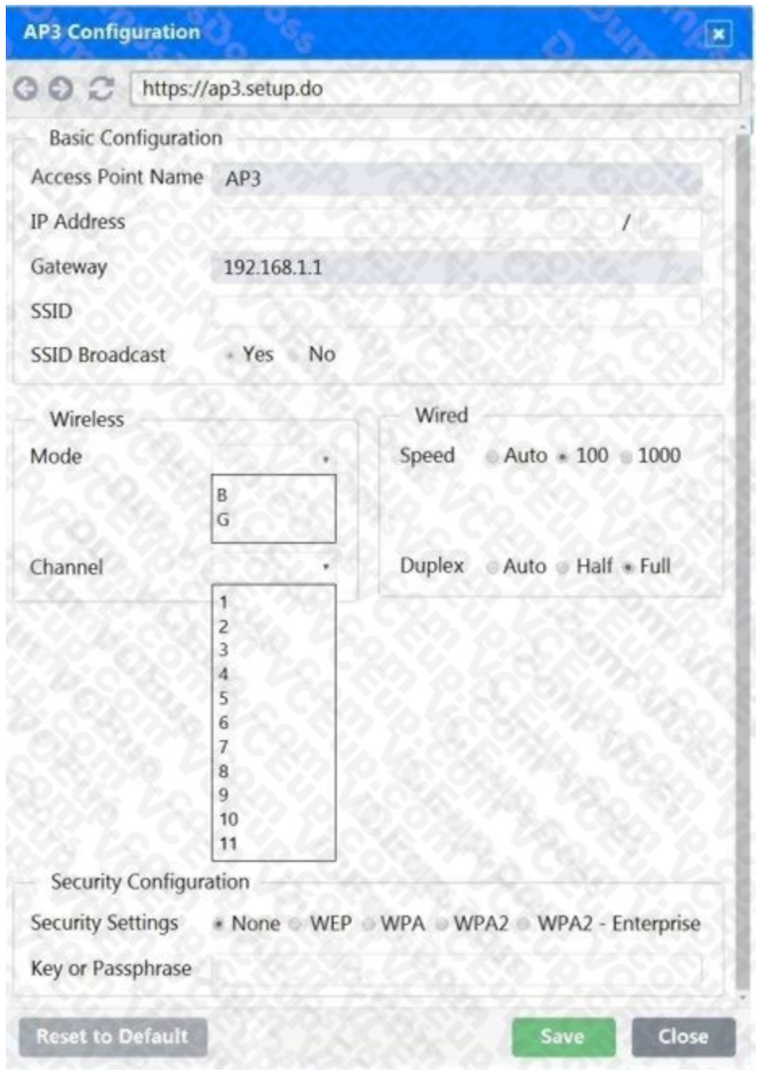
QUESTION 237
SIMULATION
You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:
The SSIDs need to be configured as CorpNet with a key of S3cr3t!

The wireless signals should not interfere with each other
The subnet the Access Points and switch are on should only support 30 devices maximum The Access Points should be configured to only support TKIP clients at a maximum speed INSTRUCTONS Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.






AP2 Configuration
https://ap2.setup.do
Basic Configuration
Access Point Name
AP2
IP Address
/
Gateway
192.168.1.1
SSID
SSID Broadcast
Yes
No
Wireless
Mode
B
G
Channel
1
2
3
4
5
6
7
8
9
10
11
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise
Key or Passphrase
Reset to Default
Save
Close



A. See explanation below.

Correct Answer: A
Section:
Explanation:
On the first exhibit, the layout should be as follows

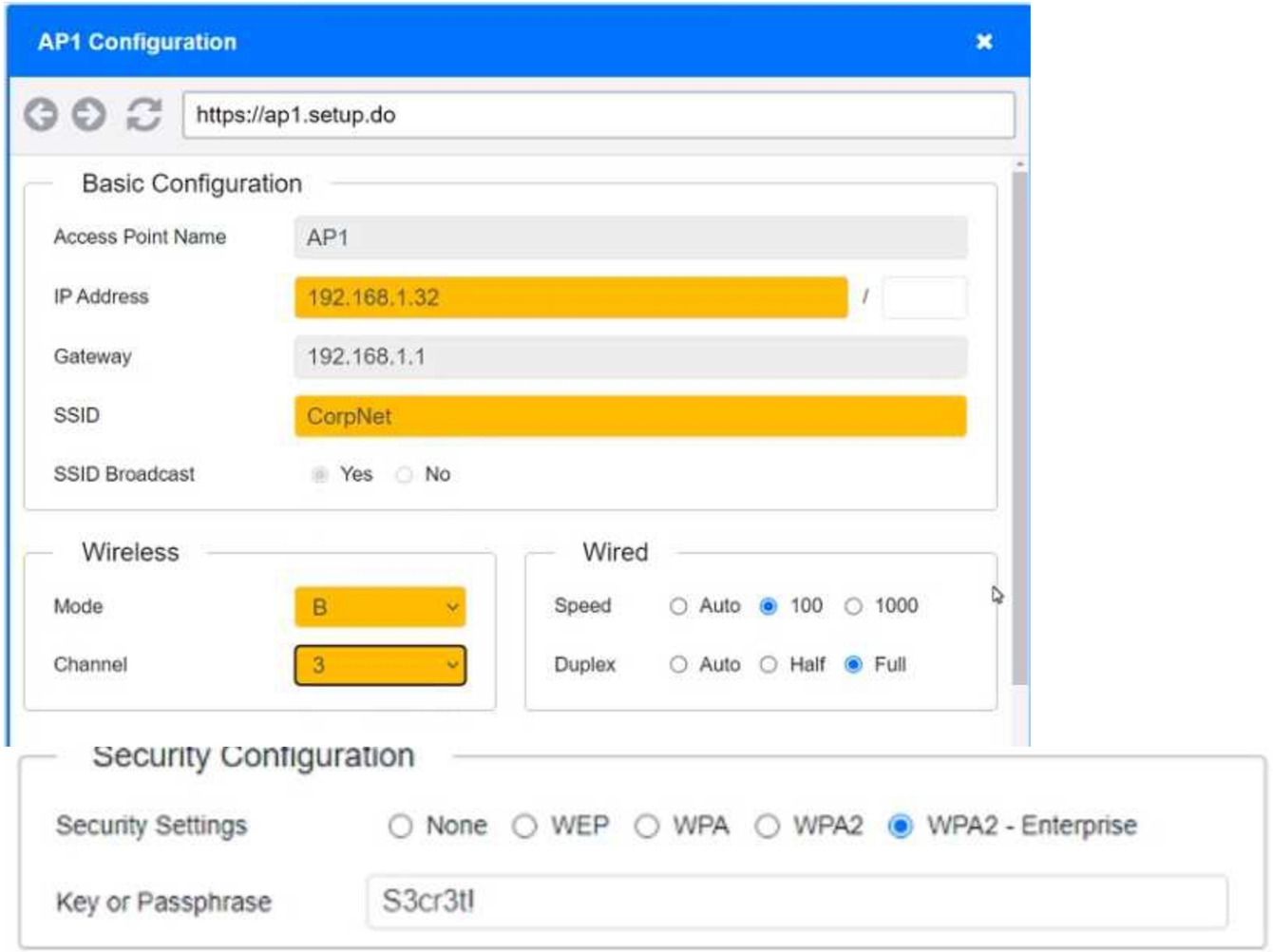


Exhibit 2 as follows
Access Point Name AP2

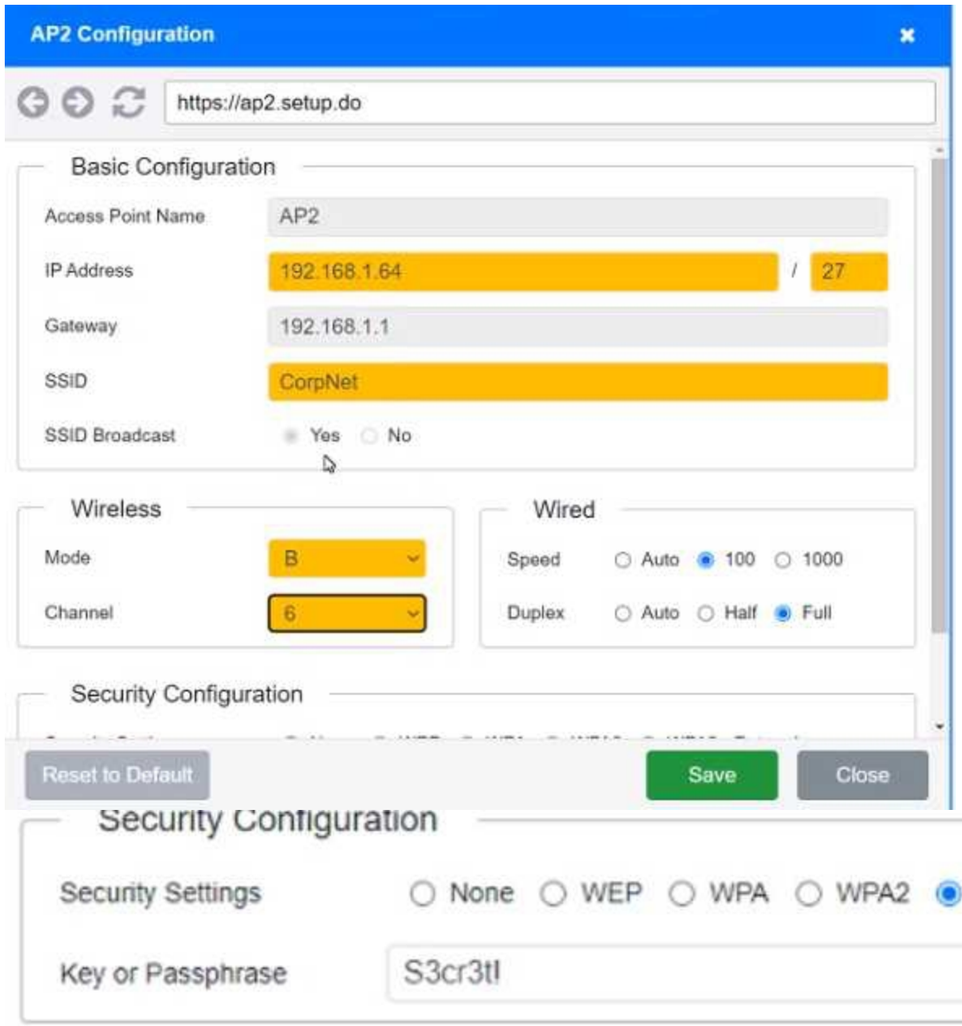
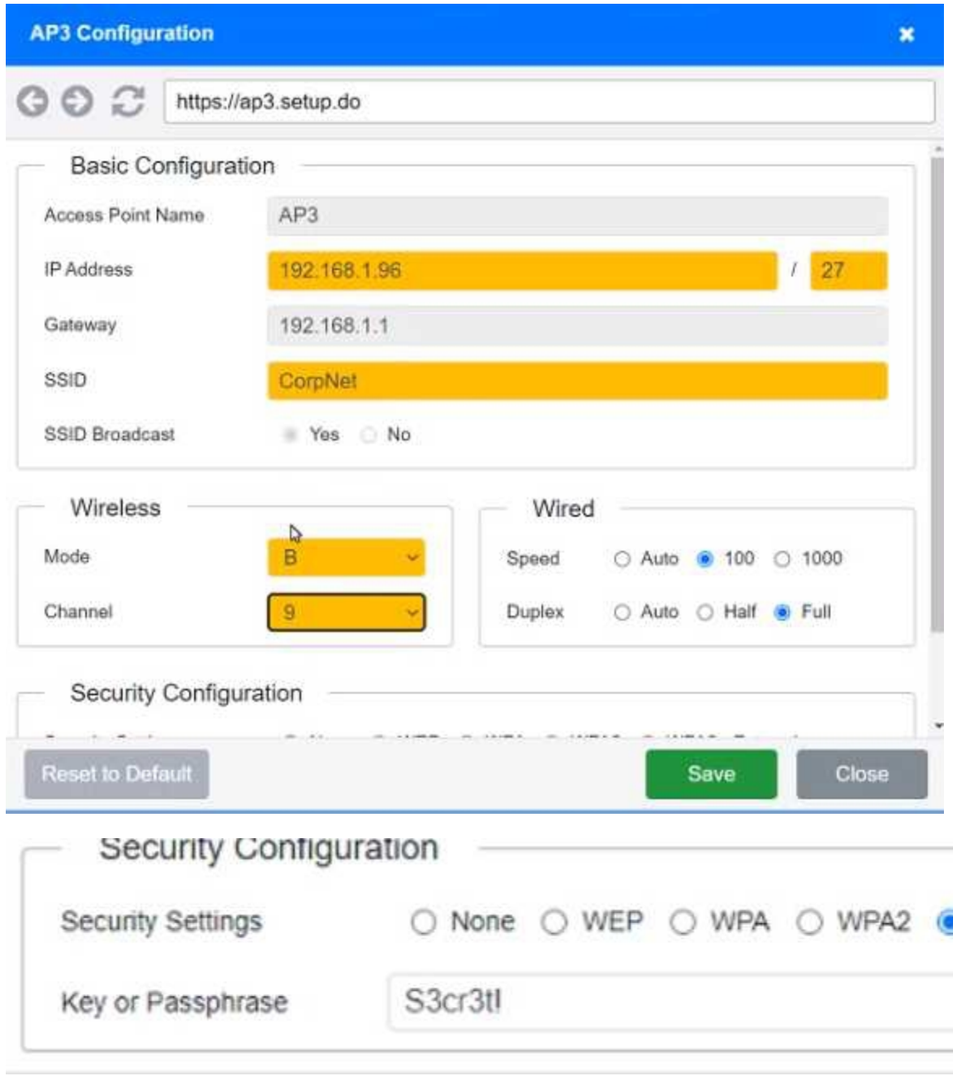
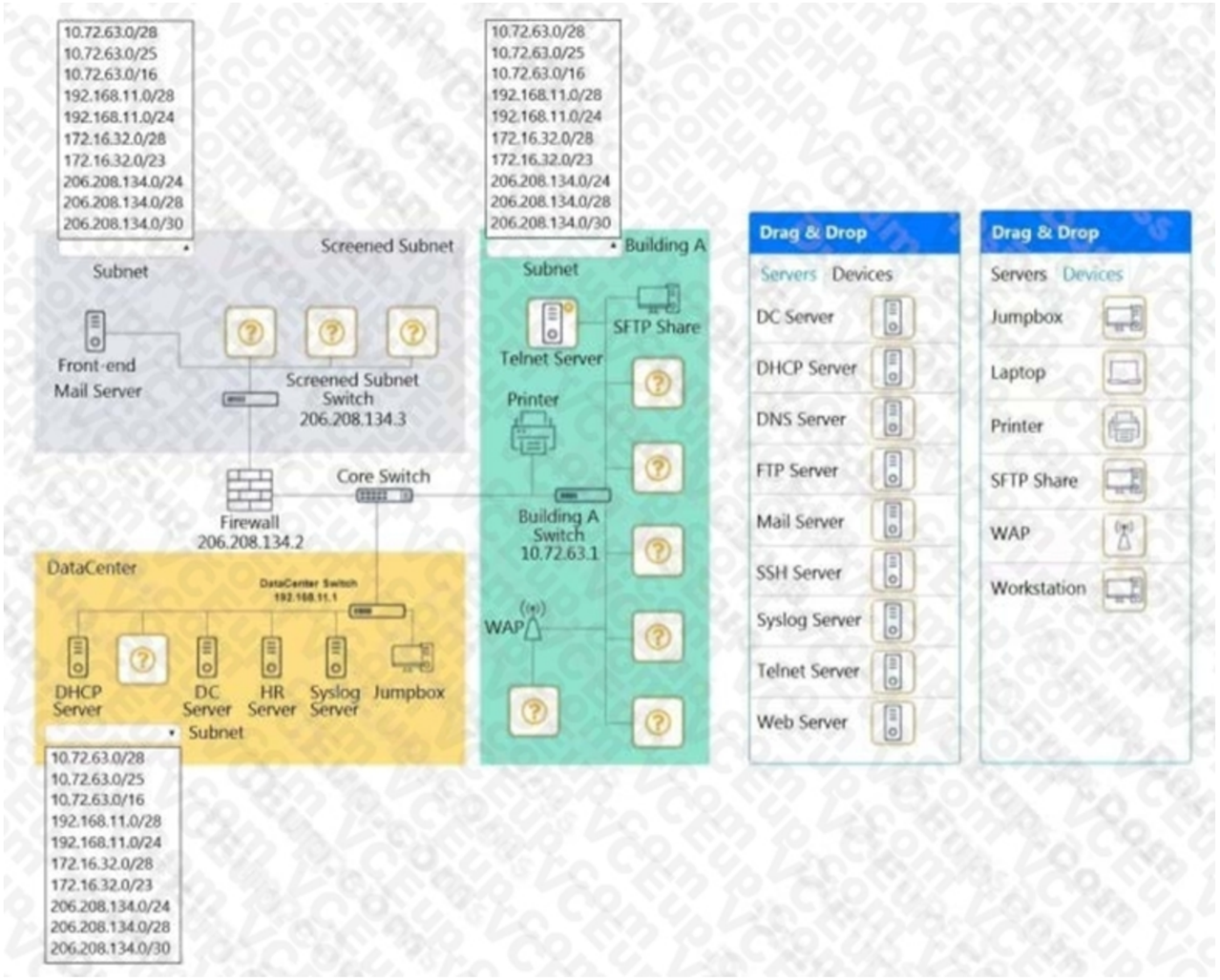


Exhibit 3 as follows
Access Point Name AP3

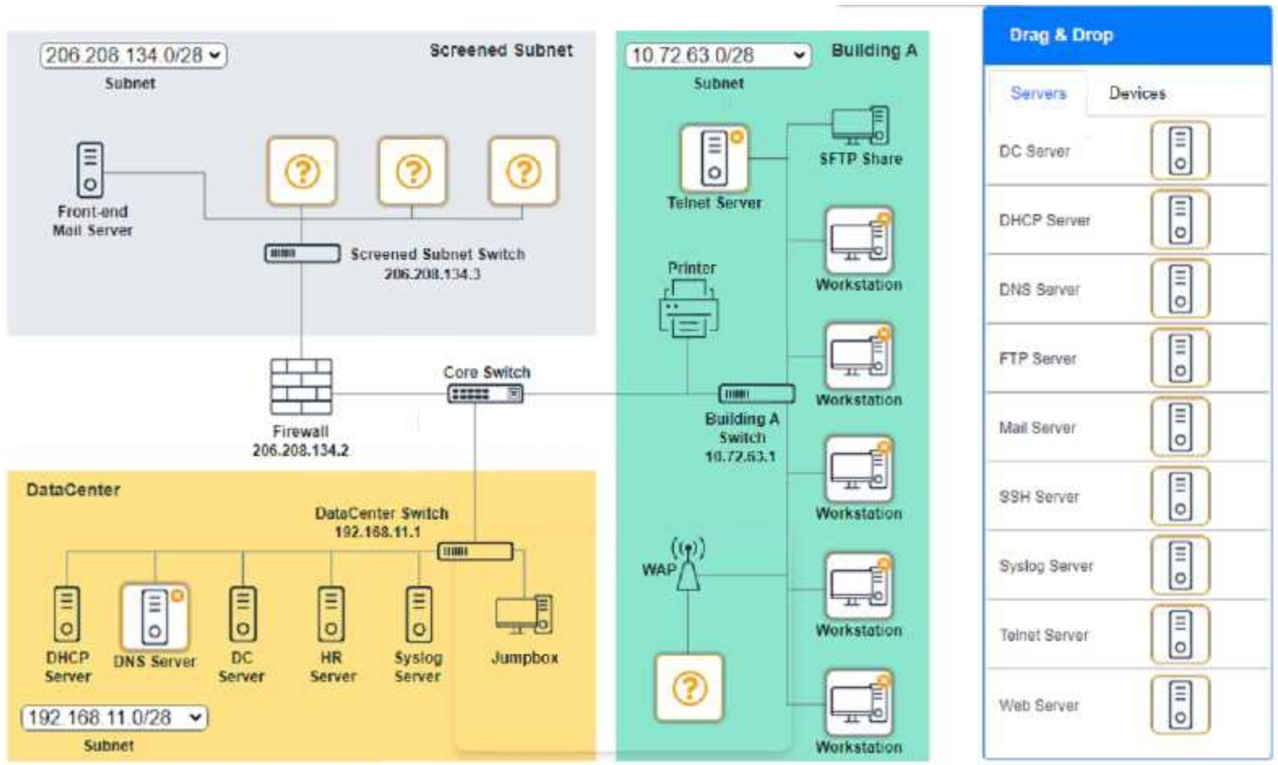


QUESTION 238
SIMULATION
You are tasked with verifying the following requirements are met in order to ensure network security.
Requirements:
Datacenter
- Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage - Provide a dedicated server to resolve 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.



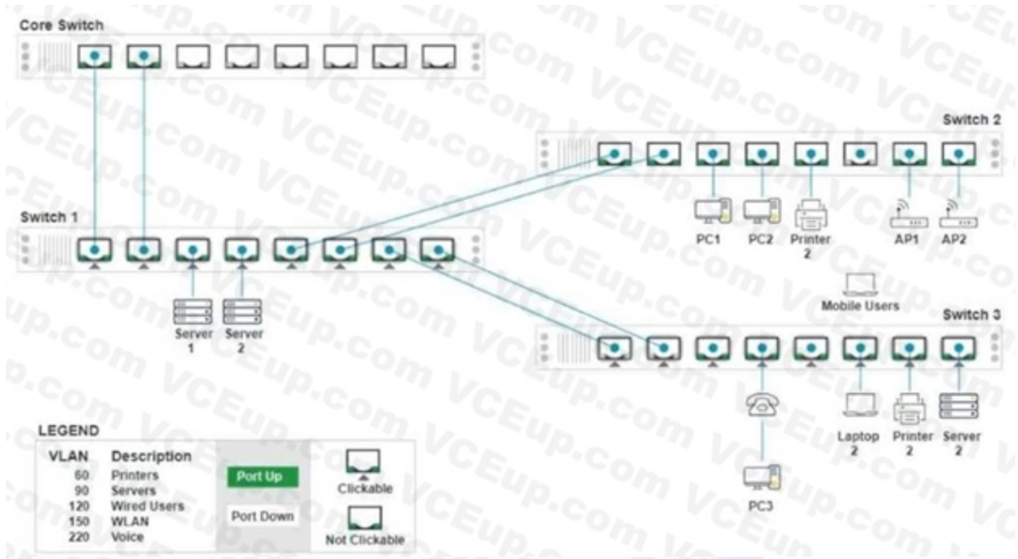
A. See explanation below.

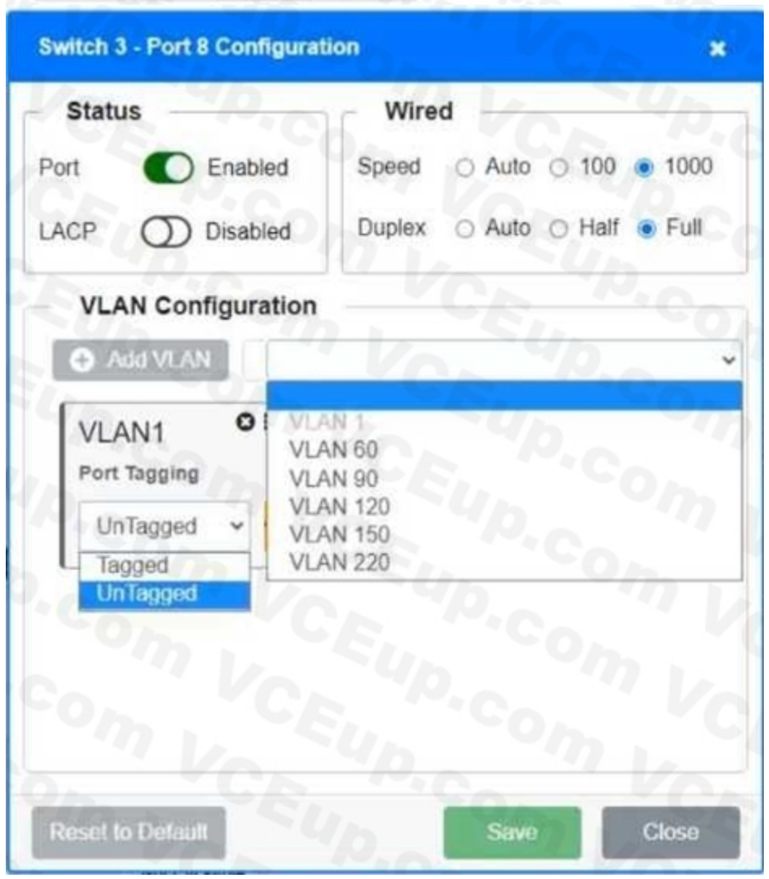
Correct Answer: A
Section:
Explanation:

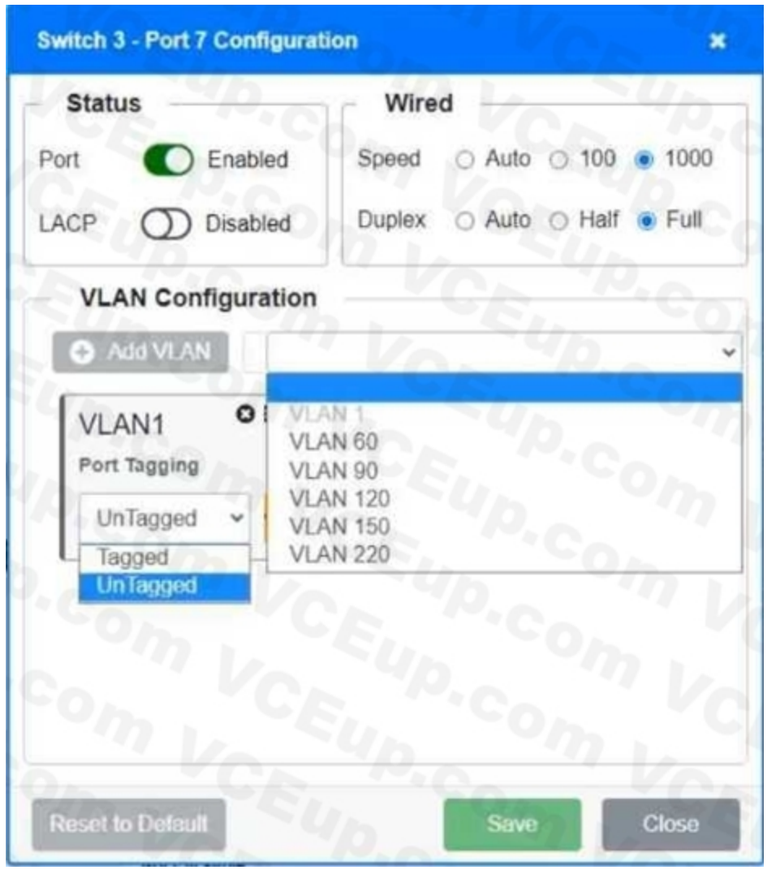


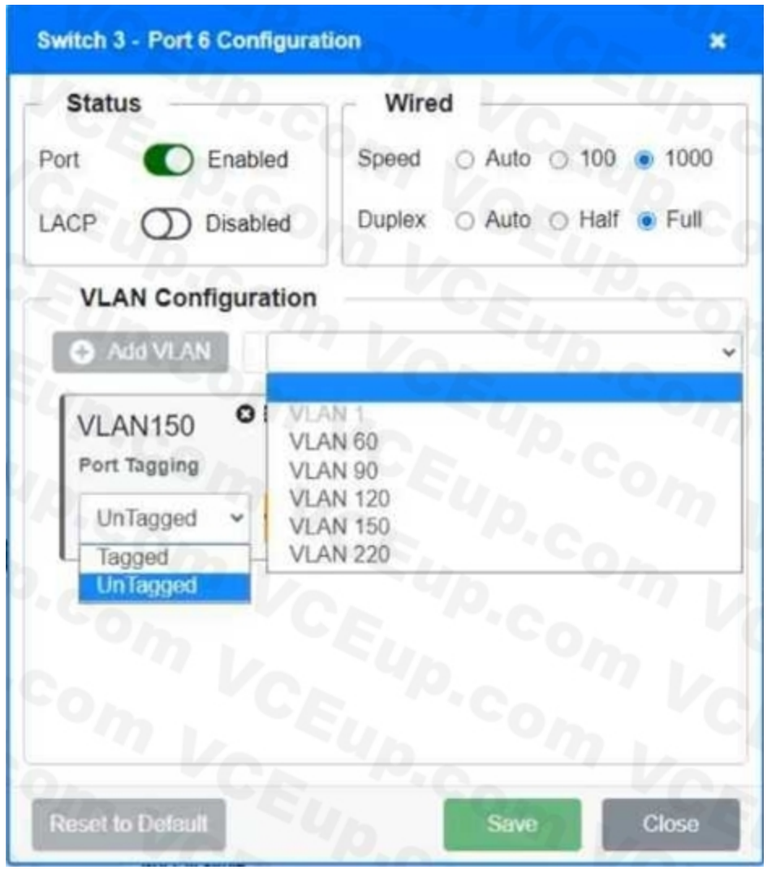
Top left subnet – 206.208.134.0/28
Top right subnet – 10.72.63.0/28
Bottom subnet – 192.168.11.0/28
Screened Subnet devices – Web server, FTP server
Building A devices – SSH server top left, workstations on all 5 on the right, laptop on bottom left DataCenter devices – DNS server.

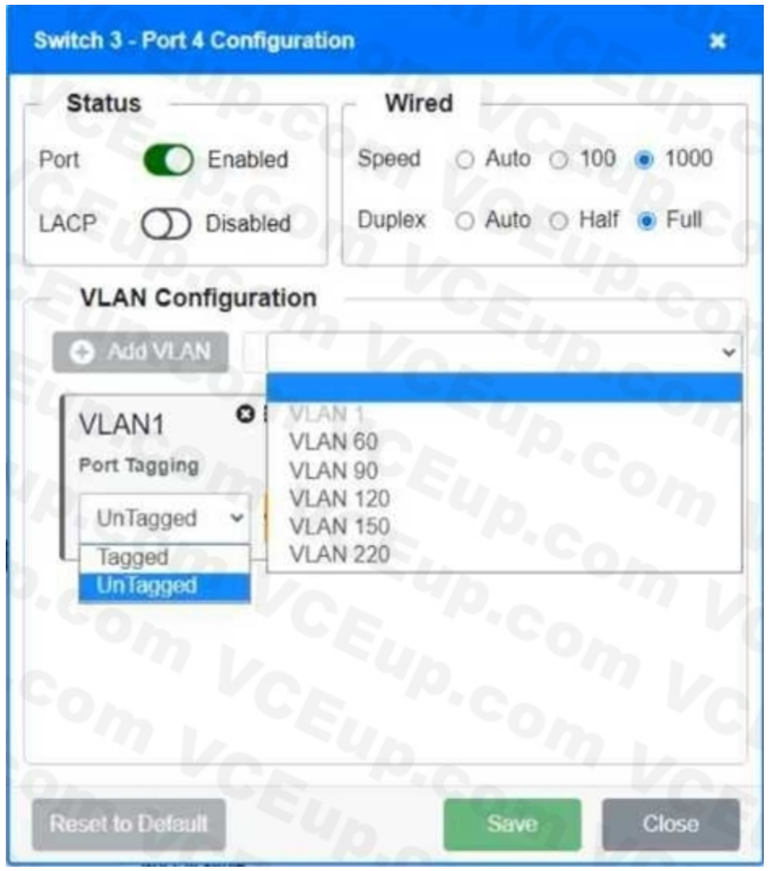
QUESTION 239
SIMULATION
A network technician replaced a switch and needs to reconfigure it to allow the connected devices to connect to the correct networks.
INSTRUCTIONS
Click on the appropriate port(s) on Switch 1 and Switch 3 to verify or reconfigure the correct settings:
•bullet Ensure each device accesses only its correctly associated network
•bullet Disable all unused switch ports
•bullet Require fault-tolerant connections between the switches
•bullet Only make necessary changes to complete the above requirements
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

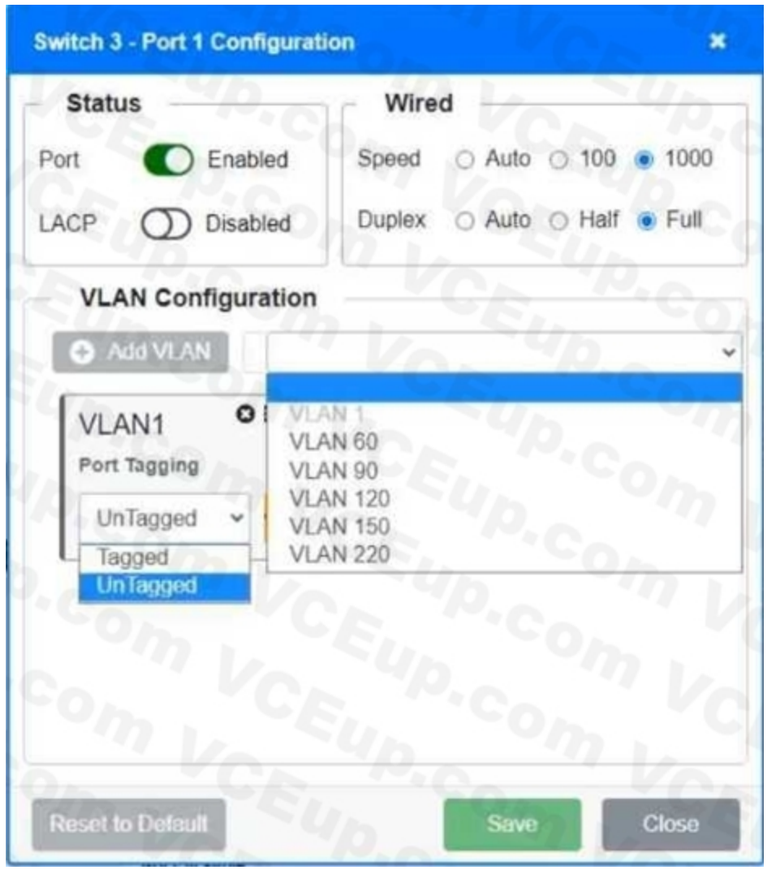

Core Switch
Switch 1
Switch 2
Switch 3
PC1
PC2
Printer 2
AP1
AP2
Mobile Users
Server 1
Server 2
Laptop 2
Printer 2
Server 2
PC3
LEGEND
VLAN
Description
60 Printers
90 Servers
120 Wired Users
150 WLAN
220 Voice
Port Up
Port Down
Clickable
Not Clickable


Switch 3 - Port 8 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close


Switch 3 - Port 7 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close


Switch 3 - Port 6 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN150
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close


Switch 3 - Port 4 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close


Switch 3 - Port 1 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close


Switch 1 - Port 7 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save
Close


Switch 1 - Port 8 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save
Close


Switch 1 - Port 6 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
Reset to Default
Save
Close


Switch 1 - Port 2 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save
Close


Switch 1 - Port 1 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save
Close


Switch 1 - Port 5 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
Reset to Default
Save
Close


Switch 1 - Port 3 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN90
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close

A. See the explanation for this solution

B.

C.

D.

Correct Answer: A
Section:
Explanation:
Explanation:
Switch 1 and Switch 2 is the only two switches that can be configured. Only switches linked together with there switch ports needs to be "tagged" and "LACP" needs to be enabled. The other ports must be untagged with no LACP enabled. You only need to assign the correct vlan via each port. 'Speed and Duplex' needs to be Speed=1000 and Duplex=Full, with is by default.
https://resources.infosecinstitute.com/topic/what-are-tagged-and-untagged-ports/

QUESTION 240
An administrator would like to have two servers at different geographical locations provide fault tolerance and high performance while appearing as one URL to users. Which of the following should the administrator implement?

A. Load balancing
B. Multipathing

C. NIC teaming
D. Warm site

Correct Answer: A
Section:
Explanation:
Load balancing is a technique that can be used to provide fault tolerance and high performance while appearing as one URL to users. It is achieved by distributing the workload across multiple servers, which are usually located in different geographical locations. This allows for high performance and fault tolerance, as if one server fails, the other will take its place. Additionally, the multiple servers appear as one URL to the users, eliminating the need for the users to switch between servers.

QUESTION 241
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

Correct Answer: A
Section:

QUESTION 242
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.

Correct Answer: A
Section:
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."

QUESTION 243
An engineer was asked to update an MX record for an upcoming project. Which of the following server types is MOST likely to be in scope for the project?

A. Email
B. Web
C. File
D. Database

Correct Answer: A
Section:
Explanation:
An MX record is a type of DNS record that specifies the mail server responsible for accepting email messages on behalf of a domain name. Therefore, an engineer who needs to update an MX record is most likely working on an email server project

QUESTION 244
A technician is tasked with setting up a mail server and a DNS server. The mail port should be secured and have the ability to transfer large files. Which of the following ports should be opened? (Select TWO).

A. 22
B. 53
C. 110
D. 389
E. 995
F. 3389

Correct Answer: B, E
Section:
Explanation:
Port 53 is used for DNS, which is a service that translates domain names into IP addresses. Port 995 is used for POP3S, which is a protocol for receiving email messages securely. POP3S supports large file transfers and encryption. Therefore, these two ports should be opened for the mail server and the
DNS server project

QUESTION 245
A network technician is investigating a trouble ticket for a user who does not have network connectivity. All patch cables between the wall jacks and computers in the building were upgraded over the weekend from Cat 5 to Cat 6. The newly installed cable is crimped with a TIA/EIA 568A on one end and a TIA/EIA 568B on the other end.
Which of the following should the technician do to MOST likely fix the issue?

A. Ensure the switchport has PoE enabled.
B. Crimp the cable as a straight-through cable.
C. Ensure the switchport has STP enabled.
D. Crimp the cable as a rollover cable.

Correct Answer: B
Section:
Explanation:
A straight-through cable is a type of twisted pair cable that has the same wiring standard (TIA/EIA 568A or 568B) on both ends. This is the most common type of cable used for connecting devices of different types, such as a computer and a switch. A cable that has different wiring standards on each end (TIA/EIA 568A on one end and 568B on the other) is called a crossover cable, which is used for connecting devices of the same type, such as two computers or two switches. Therefore, the technician should crimp the cable as a straight-through cable to fix the issue.

QUESTION 246
Which of the following should be used to manage outside cables that need to be routed to various multimode uplinks?

A. Fiber distribution panel
B. 110 punchdown block
C. PDU
D. TIA/EIA-568A patch bay
E. Cat 6 patch panel

Correct Answer: A
Section:
Explanation:
A fiber distribution panel is a device that provides a central location for connecting and managing fiber optic cables and optical modules. It can support various types and speeds of fiber optic links, including multimode uplinks. Therefore, a fiber distribution panel should be used to manage outside cables that need to be routed to various multimode uplinks.

QUESTION 247
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

Correct Answer: B
Section:
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.

QUESTION 248
A technician is investigating why a PC cannot reach a file server with the IP address 192.168.8.129.
Given the following TCP/IP network configuration:

Link-local IPv6 address	fe80::28e4:a7cc:a55e:4bea
IPv4 address	192.168.8.105
Subnet mask	255.255.255.128
Default gateway	192.168.8.1

Which of the following configurations on the PC is incorrect?

A. Subnet mask
B. IPv4 address
C. Default gateway
D. IPv6 address

Correct Answer: C
Section:
Explanation:
The default gateway is the IP address of the router that connects the PC to other networks. The default gateway should be on the same subnet as the PC's IPv4 address. However, in this case, the default gateway is 192.168.9.1, which is on a different subnet than the PC's IPv4 address of 192.168.8.15. Therefore, the default gateway configuration on the PC is incorrect and prevents the PC from reaching the file server on another subnet.

QUESTION 249
A network technician is configuring a wireless access point and wants to only allow company-owned devices to associate with the network. The access point uses PSKs,

and a network authentication system does not exist on the network. Which of the following should the technician implement?

A. Captive portal
B. Guest network isolation
C. MAC filtering
D. Geofencing

Correct Answer: C
Section:
Explanation:
MAC filtering is a method of allowing only company-owned devices to associate with the network by using their MAC addresses as identifiers. A MAC address is a unique identifier assigned to each network interface card (NIC) by the manufacturer. MAC filtering can be configured on the wireless access point to allow or deny access based on the MAC address of the device. This way, only devices with known MAC addresses can connect to the network. Reference: https://www.comptia.org/training/books/network-n10-008-study-guide (page 323)

QUESTION 250
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

Correct Answer: A
Section:
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. Reference: https://www.comptia.org/training/books/network-n10-008study-guide
(page 405)

QUESTION 251
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

Correct Answer: A
Section:
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 nonproprietary standard that supports up to Category 6 cabling and can be used for voice or data applications. Reference: https://www.comptia.org/training/books/network-n10-008-study-guide
(page 64)

QUESTION 252
A network administrator is implementing process changes based on recommendations following a recent penetration test. The testers used a method to gain access to the network that involved exploiting a publicly available and fixed remote code execution vulnerability in the VPN appliance.
Which of the following should the administrator do to BEST prevent this from happening again?

A. Change default passwords on internet-facing hardware.

B. Implement robust ACLs with explicit deny-all entries.
C. Create private VLANs for management plane traffic.
D. Routinely upgrade all network equipment firmware.

Correct Answer: D
Section:
Explanation:
Firmware is the software that runs on network equipment such as routers, switches, and VPN appliances. Firmware updates often contain bug fixes, security patches, and performance improvements that can prevent or mitigate vulnerabilities and attacks. By routinely upgrading all network equipment firmware, a network administrator can ensure that the network devices are running the latest and most secure versions of firmware and avoid exploiting known and fixed remote code execution vulnerabilities in the VPN appliance. Reference:
https://www.comptia.org/training/books/network-n10-008-study-guide (page 462)

QUESTION 253
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

Correct Answer: C
Section:
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. Reference:
https://www.comptia.org/training/books/network-n10-008-study-guide (page 199)

QUESTION 254
A network administrator needs to monitor traffic on a specific port on a switch. Which of the following should the administrator configure to accomplish the task?

A. Port security
B. Port tagging
C. Port mirroring
D. Media access control

Correct Answer: C
Section:
Explanation:
Port mirroring is a feature that allows a network technician to monitor traffic on a specific port on a switch by copying all the traffic from that port to another port where a monitoring device is connected. Port mirroring can be used for troubleshooting, analysis, or security purposes, such as detecting network anomalies, performance issues, or malicious activities. Reference:
https://www.comptia.org/training/books/network-n10-008-study-guide (page 156)

QUESTION 255
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

Correct Answer: B

Section:

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

QUESTION 256

A company is undergoing expansion but does not have sufficient rack space in its data center. Which of the following would be BEST to allow the company to host its new equipment without a major investment in facilities?

A. Using a colocation service

B. Using available rack space in branch offices

C. Using a flat network topology

D. Reorganizing the network rack and installing top-of-rack switching

Correct Answer: A

Section:

Explanation:

A colocation service is a service that provides rack space, power, cooling, security, and connectivity for a company's network equipment in a data center. A colocation service can be used when a company does not have sufficient rack space in its own data center and does not want to invest in building or expanding its own facilities. By using a colocation service, a company can host its new equipment in a professional and reliable environment without a major investment in facilities. Reference: https://www.comptia.org/training/books/network-n10-008-study-guide (page 414)

QUESTION 257

In which of the following components do routing protocols belong in a software-defined network?

A. Infrastructure layer

B. Control layer

C. Application layer

D. Management plane

Correct Answer: B

Section:

Explanation:

A software-defined network (SDN) is a network architecture that decouples the control plane from the data plane and centralizes the network intelligence in a software controller. The control plane is the part of the network that makes decisions about how to route traffic, while the data plane is the part of the network that forwards traffic based on the control plane's instructions. The control layer is the layer in an SDN that contains the controller and the routing protocols that communicate with the
network devices. The control layer is responsible for managing and configuring the network devices and providing them with the necessary information to forward traffic. Reference: https://www.comptia.org/training/books/network-n10-008-study-guide (page 378)

QUESTION 258

A company, which is located in a coastal town, retrofitted an office building for a new data center.
The underground fiber optics were brought in and connected to the switches in the basement network MDF. A server data center was built on the fifth floor with the two rooms vertically connected by fiber optics. Which of the following types of environmental sensors is MOST needed?

A. Temperature sensor in the network MDF

B. Water sensor in the network MDF

C. Temperature sensor in the data center

D. Water sensor in the data center

Correct Answer: B

Section:

Explanation:
A water sensor is a type of environmental sensor that detects the presence of water or moisture in an area. A water sensor is most needed in a network main distribution frame (MDF) that is located in a basement near underground fiber-optic cables. A network MDF is a central point where all the network connections converge and where network equipment such as switches and routers are located. If water leaks into the basement and damages the fiber-optic cables or the network equipment, it can cause network outages, performance degradation, or data loss. A water sensor can alert the network administrator of any water intrusion and help prevent or minimize the damage.
Reference: https://www.comptia.org/training/books/network-n10-008-study-guide (page 446)

QUESTION 259
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.

Correct Answer: B
Section:
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. Reference:
https://www.comptia.org/training/books/network-n10-008-study-guide (page 308)

QUESTION 260
Which of the following would be BEST suited for use at the access layer in a three-tier architecture system?

A. Router
B. Multilayer switch
C. Layer 2 switch
D. Access point

Correct Answer: C
Section:
Explanation:
A layer 2 switch is a device that forwards traffic based on MAC addresses within a single network segment or VLAN. A layer 2 switch is best suited for use at the access layer in a three-tier architecture system. The access layer is the layer that connects end devices such as computers, printers, and phones to the network. A layer 2 switch can provide fast and efficient switching for end devices without adding complexity or overhead to the network. Reference:
https://www.comptia.org/training/books/network-n10-008-study-guide (page 139)

QUESTION 261
A public, wireless ISP mounts its access points on top of traffic signal poles. Fiber-optic cables are installed from a fiber switch through the ground and up the pole to a fiber-copper media converter, and then connected to the AP. In one location, the switchport is showing sporadic link loss to the attached AP. A similar link loss is not seen at the AP interface. The fiber-optic cable is moved to another unused switchport with a similar result. Which of the following steps should the assigned technician complete NEXT?

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

Correct Answer: B
Section:
Explanation:

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

QUESTION 262
A company wants to implement a disaster recovery site for non-critical applications, which can tolerate a short period of downtime. Which of the following types of sites should the company implement to achieve this goal?

A. Hot
B. Cold
C. warm
D. Passive

Correct Answer: C
Section:
Explanation:
The type of site that the company should implement for non-critical applications that can tolerate a short period of downtime is a warm site. A warm site is a disaster recovery site that has some pre-installed equipment and software, but not as much as a hot site, which is fully operational and ready to take over the primary site's functions in case of a disaster. A warm site requires some time and effort to activate and synchronize with the primary site, but not as much as a cold site, which has no equipment or software installed and requires a lot of configuration and testing. A passive site is not a common term for a disaster recovery site, but it could refer to a site that only receives backups from the primary site and does not actively participate in the network operations. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 347; The Official CompTIA Network+ Student Guide (Exam N10-008), page 13-10.

QUESTION 263
A technician needs to allow a device to maintain the same IP address lease based on the physical address of a network card. Which of the following should the technician use?

A. MAC address reservation
B. Static IP address
C. Custom DNS server entry
D. IP address exclusion

Correct Answer: A
Section:
Explanation:
MAC address reservation is the technique that allows a device to maintain the same IP address lease based on the physical address of a network card. MAC address reservation is a feature of DHCP that allows network administrators to assign specific IP addresses to specific devices based on their MAC addresses. A MAC address is a unique identifier that is assigned to each network interface card (NIC) by its manufacturer. A MAC address reservation can ensure that a device always receives the same IP address from the DHCP server, regardless of its location or connection time. This can be useful for devices that need consistent network access or configuration, such as servers, printers, or cameras. Reference: [CompTIA Network+ Certification Exam Objectives], How to Reserve IP Addresses with DHCP Server

QUESTION 264
Which of the following can be used to aggregate logs from different devices and would make analysis less difficult?

A. Syslog
B. SIEM
C. Event logs
D. NetFlow

Correct Answer: B
Section:
Explanation:
SIEM stands for Security Information and Event Management, and it is a system that collects, normalizes, and analyzes log data from different sources in a centralized platform. SIEM can help identify security incidents,

monitor network performance, and generate reports and alerts.SIEM can make log analysis less difficult by providing a unified view of the log data, correlating events across different devices, and applying rules and filters to detect anomalies and patterns12.

QUESTION 265
A network technician is responding to an issue with a local company. To which of the following documents should the network technician refer to determine the scope of the issue?

A. MTTR
B. MOU
C. NDA
D. SLA

Correct Answer: D
Section:
Explanation:
SLA stands for Service Level Agreement, and it is a contract that defines the expectations and responsibilities between a service provider and a customer. SLA can specify the quality, availability, and performance metrics of the service, as well as the penalties for non-compliance and the procedures for resolving issues.SLA can help the network technician determine the scope of the issue by providing the baseline and target values for the service, the escalation process and contacts, and the service credits or remedies for the customer45.
CompTIA Network+ N10-008 Cert Guide - Chapter 15: Network Troubleshooting Methodology35: What is a Service Level Agreement (SLA)? | ITIL | AXELOS

QUESTION 266
An engineer is troubleshooting poor performance on the network that occurs during work hours. Which of the following should the engineer do to improve performance?

A. Replace the patch cables.
B. Create link aggregation.
C. Create separation rules on the firewall.
D. Create subinterfaces on the existing port.

Correct Answer: B
Section:
Explanation:
Link aggregation is a technique that allows multiple network interfaces to act as a single logical interface, increasing the bandwidth and redundancy of the network connection. Link aggregation can improve the performance of the network by balancing the traffic load across multiple links and providing failover in case one link fails. Link aggregation is also known as port trunking, port channeling, or NIC teaming.

QUESTION 267
A client utilizes mobile tablets to view high-resolution images and videos via Wi-Fi within a corporate office building. The previous administrator installed multiple high-density APs with Wi-Fi 5, providing maximum coverage, but the measured performance is still below expected levels. Which of the following would provide the best solution?

A. Channel bonding
B. EIRP power settings
C. Antenna polarization
D. A directional antenna

Correct Answer: A
Section:
Explanation:
Channel bonding is a technique that allows two or more adjacent channels to be combined into a wider channel, increasing the data rate and throughput of the wireless network. Channel bonding can improve the performance of the Wi-Fi network by utilizing more of the available spectrum and reducing interference from other devices. Channel bonding is supported by Wi-Fi 5 (802.11ac) and Wi-Fi 6 (802.11ax) standards.

QUESTION 268
A user reports that the internet seems slow on a workstation, but no other users have reported any issues. The server team confirms the servers are functioning normally. A technician suspects something specific to the user's computer is overutilizing bandwidth. Which of the following commands should the technician use to further investigate the issue?

A. nmap
B. tcpdump
C. netstat
D. nslookup

Correct Answer: C
Section:
Explanation:
netstat is a command-line tool that displays network connections, routing tables, interface statistics, and more. It can help the technician identify which processes or applications are using the network bandwidth on the user's computer. netstat can also show the current bandwidth usage in bytes per second for each network interface.
Reference
netstat - Wikipediaprovides an overview of the netstat tool and its features.
How to get current bandwidth usage from command line using built-in Linux tools? - Super Userexplains how to use netstat and other tools to monitor bandwidth usage on Linux systems.
Get network utilization from command line - Super Usershows how to use typeperf and other tools to monitor bandwidth usage on Windows systems.

QUESTION 269
A network technician is installing a wireless network in an office building. After performing a site survey, the technician determines the area is very saturated on the 2.4GHz and the 5GHz bands. Which of the following wireless standards should the network technician implement?

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

Correct Answer: B
Section:
Explanation:
802.11 ax is the latest wireless standard that operates in both the 2.4GHz and the 5GHz bands. It offers higher throughput, lower latency, and improved efficiency compared to previous standards. It also uses technologies such as OFDMA and MU-MIMO to reduce interference and increase capacity in dense environments. Therefore, 802.11 ax is the best choice for a wireless network in an office building with high saturation on both bands.
Reference
Part 3 of current page talks about the benefits of 802.11 ax and how it improves network performance in congested areas1.
CompTIA Network+ N10-008 Exam Cramcovers the wireless standards and their characteristics in Chapter 5. It also provides practice questions and explanations for the exam.

QUESTION 270
An application is not working. When the log files are reviewed, the application continuously tries to reach the following destination:

Destination
::1/128

Which of the following is most likely associated with this IP address?

A. APIPA
B. Default gateway

C. Link local
D. Loopback

Correct Answer: D
Section:
Explanation:
The IP address ::1/128 is the loopback address of the local host in IPv6, which is the equivalent of the 127.0.0.1 in IPv4. The loopback address is a virtual interface that loops all traffic back to itself, the local host. The loopback address is used for testing and troubleshooting purposes, such as checking the connectivity and configuration of the network stack. If an application tries to reach the loopback address, it means that it is not communicating with any external network or server, but only with itself.
The other options are not correct because they are not associated with the IP address ::1/128. They are:
APIPA. APIPA stands for Automatic Private IP Addressing, which is a feature that allows a device to assign itself a private IPv4 address in the range of 169.254.0.0/16 when no DHCP server is available. APIPA does not apply to IPv6 addresses, and it is not related to the loopback address.
Default gateway. The default gateway is the IP address of the router or device that connects a local network to other networks. The default gateway is usually the first or last usable IP address in a subnet, and it is not the same as the loopback address.
Link local. Link local addresses are IPv6 addresses that are used for communication within a single network segment or link. Link local addresses have the prefix fe80::/10, and they are not routable or reachable from other networks. Link local addresses are not the same as the loopback address.
Reference 1:Loopback Address - ::1/128 - ipUpTime.net 2:Network+ (Plus) Certification | CompTIA IT Certifications 3:Reserved IP addresses - Wikipedia

QUESTION 271
A technician is setting up DNS records on local servers for the company's cloud DNS to enable access by hostname. Which of the following records should be used?

A. A
B. MX
C. CNAME
D. NS

Correct Answer: A
Section:
Explanation:
An A record, also known as an address record, is a type of DNS record that maps a hostname to an IPv4 address. An A record is used to resolve a domain name to an IP address, so that clients can connect to the server or service by using the domain name instead of the IP address. For example, an A record can map www.example.com to 192.0.2.1.
An A record is the most common type of DNS record for cloud DNS, as it allows the company to use a custom domain name for their cloud services, such as web hosting, email, or storage. An A record can also be used to create subdomains, such as blog.example.com or mail.example.com, that point to different IP addresses or servers.
The other options are not correct because they are not the best type of DNS record for cloud DNS. They are:
MX. MX stands for mail exchange, and it is a type of DNS record that specifies the mail servers that are responsible for receiving and delivering email messages for a domain name. MX records are used for email services, but they are not sufficient for cloud DNS, as they do not map a hostname to an IP address.
CNAME. CNAME stands for canonical name, and it is a type of DNS record that specifies an alias name for another domain name. CNAME records are used to create multiple names for the same IP address or server, such as www.example.com and example.com. CNAME records are useful for cloud DNS, but they are not the best type, as they depend on another A record to resolve the IP address.
NS. NS stands for name server, and it is a type of DNS record that delegates a DNS zone to an authoritative server. NS records are used to specify which DNS servers are responsible for answering queries for a domain name or a subdomain. NS records are essential for cloud DNS, but they are not the best type, as they do not map a hostname to an IP address.
Reference 1:DNS records overview | Google Cloud 2:Network+ (Plus) Certification | CompTIA IT Certifications 3:ClouDNS: What is a DNS record?

QUESTION 272
Which of the following is the first step to troubleshoot a network issue?

A. Identify the problem.
B. Document the findings.
C. Establish a theory of probable cause.

D. Test the theory to determine the cause.

Correct Answer: A
Section:
Explanation:
According to the CompTIA Network+ N10-008 Cert Guide, the first step in the troubleshooting process is to identify the problem.This involves gathering information, understanding the symptoms, and clarifying the exact nature of the issue before proceeding to other steps like establishing theories or testing them1.