CompTIA

Exam Questions N10-009

CompTIA Network+ Exam

NEW QUESTION 1
- (Exam Topic 1)
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

Answer: A

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.
References:
> Network+ N10-007 Certification Exam Objectives, Objective 2.2: Given a scenario, implement the appropriate network-based security and troubleshoot common connectivity issues.

NEW QUESTION 2
- (Exam Topic 1)
An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex. Which of the following is the MOST likely cause of this issue?

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

Answer: C

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

NEW QUESTION 3
- (Exam Topic 1)
Wireless users are reporting intermittent internet connectivity. Connectivity is restored when the users disconnect and reconnect, utilizing the web authentication process each time. The network administrator can see the devices connected to the APs at all times. Which of the following steps will MOST likely determine the cause of the issue?

A. Verify the session time-out configuration on the captive portal settings
B. Check for encryption protocol mismatch on the client’s wireless settings
C. Confirm that a valid passphrase is being used during the web authentication
D. Investigate for a client’s disassociation caused by an evil twin AP

Answer: A

Explanation:
A captive portal is a web page that requires users to authenticate before they can access the internet. If the session time-out configuration is too short, users may experience intermittent internet connectivity and have to reconnect using the web authentication process each time. The network administrator can verify the session time-out configuration on the captive portal settings and adjust it if needed. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 1.0 Network Architecture, Objective 1.8 Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 4
- (Exam Topic 1)
Which of the following is used to prioritize Internet usage per application and per user on the network?

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

Answer: A

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

NEW QUESTION 5
- (Exam Topic 1)
Which of the following would be BEST to use to detect a MAC spoofing attack?

A. Internet Control Message Protocol
B. Reverse Address Resolution Protocol
C. Dynamic Host Configuration Protocol
D. Internet Message Access Protocol

Answer: B

Explanation:
Reverse Address Resolution Protocol (RARP) is a protocol that allows a device to obtain its MAC address from its IP address. A MAC spoofing attack is an attack where a device pretends to have a different MAC address than its actual one. RARP can be used to detect a MAC spoofing attack by comparing the MAC address obtained from RARP with the MAC address obtained from other sources, such as ARP or DHCP. References: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.techopedia.com/definition/25597/reverse-address-resolution-protocol-rarp

NEW QUESTION 6
- (Exam Topic 1)
A technician is connecting multiple switches to create a large network for a new office. The switches are unmanaged Layer 2 switches with multiple connections between each pair. The network is experiencing an extreme amount of latency. Which of the following is MOST likely occurring?

A. Ethernet collisions
B. A DDoS attack
C. A broadcast storm
D. Routing loops

Answer: C

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

NEW QUESTION 7
- (Exam Topic 1)
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

Answer: A

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. References: 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

NEW QUESTION 8
- (Exam Topic 1)
A technician is installing multiple UPS units in a major retail store. The technician is required to keep track of all changes to new and old equipment. Which of the following will allow the technician to record these changes?

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

Answer: A

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

NEW QUESTION 9
- (Exam Topic 1)
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

Answer: B

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. References:
https://www.howtogeek.com/663056/how-to-use-the-nslookup-command-on-linux/

NEW QUESTION 10
- (Exam Topic 1)
Access to a datacenter should be individually recorded by a card reader even when multiple employees enter the facility at the same time. Which of the following allows the enforcement of this policy?

A. Motion detection
B. Access control vestibules
C. Smart lockers
D. Cameras

Answer: B

Explanation:
The most effective security mechanism against physical intrusions due to stolen credentials would likely be a combination of several of these options. However, of the options provided, the most effective security mechanism would probably be an access control vestibule. An access control vestibule is a secure area that is located between the outer perimeter of a facility and the inner secure area. It is designed to provide an additional layer of security by requiring that individuals pass through a series of security checks before being allowed access to the secure area. This could include biometric authentication, access card readers, and motion detection cameras.
Access control vestibules allow the enforcement of the policy that access to a datacenter should be individually recorded by a card reader even when multiple employees enter the facility at the same time. An access control vestibule is a physical security device that consists of two doors with an interlocking mechanism. Only one door can be opened at a time, and only one person can pass through each door. This prevents tailgating or piggybacking, where unauthorized persons follow authorized persons into a secure area. An access control vestibule can also be integrated with a card reader or other authentication system to record each individual’s access. References: https://www.boonedam.us/blog/what-are-access-control-vestibules

NEW QUESTION 10
- (Exam Topic 1)
A technician is installing a new fiber connection to a network device in a datacenter. The connection from the device to the switch also traverses a patch panel connection. The chain of connections is in the following order:
Device
LC/LC patch cable Patch panel
Cross-connect fiber cable Patch panel
LC/LC patch cable Switch
The connection is not working. The technician has changed both patch cables with known working patch cables. The device had been tested and was working properly before being installed. Which of the following is the MOST likely cause of the issue?

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

Answer: A

Explanation:
The most likely cause of the issue where the fiber connection from a device to a switch is not working is that the TX/RX (transmit/receive) is reversed. When connecting fiber optic cables, it is important to ensure that the TX of one device is connected to the RX of the other device and vice versa. If the TX/RX is reversed, data cannot be transmitted successfully.
References:
> CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 5: Network Operations, Objective 5.1: Given a scenario, use appropriate documentation and diagrams to manage the network.

NEW QUESTION 14
- (Exam Topic 1)
A technician is troubleshooting a wireless connectivity issue in a small office located in a high-rise building. Several APs are mounted in this office. The users report that the network connections frequently disconnect and reconnect throughout the day. Which of the following is the MOST likely cause of this issue?

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

Answer: C

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

NEW QUESTION 19
- (Exam Topic 1)
A network engineer performs the following tasks to increase server bandwidth: Connects two network cables from the server to a switch stack

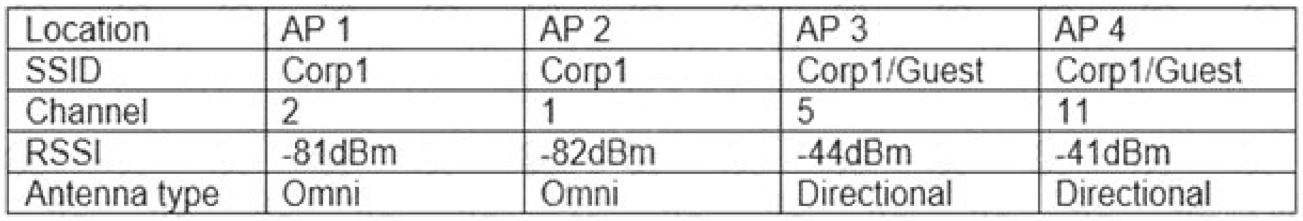
Configure LACP on the switchports
Verifies the correct configurations on the switch interfaces Which of the following needs to be configured on the server?

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

Answer: C

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

NEW QUESTION 21
- (Exam Topic 1)
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

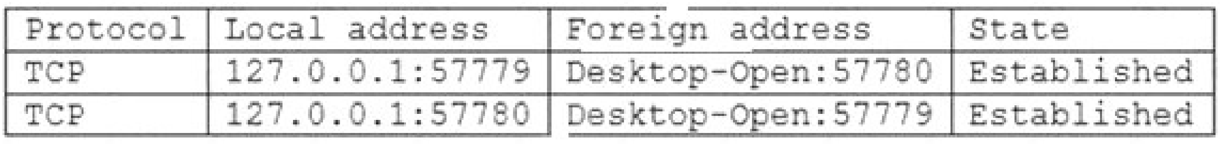
Which of the following should a wireless technician do NEXT to troubleshoot this issue?

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

Answer: A

Explanation:
Based on the site survey table, we can see that AP 2, AP 3, and AP 4 are all broadcasting on the same channel, which can cause interference and affect performance. Therefore, the next step a wireless technician should take to troubleshoot this issue is to reconfigure the channels to reduce overlap. This will help to improve network performance and eliminate any interference.
References:
- Network+ N10-007 Certification Exam Objectives, Objective 2.8: Given a scenario, troubleshoot common wireless problems and perform site surveys.

NEW QUESTION 25
- (Exam Topic 1)
Given the following information:



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

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

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

Answer: D

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

NEW QUESTION 29
- (Exam Topic 1)
A network administrator is configuring a load balancer for two systems. Which of the following must the administrator configure to ensure connectivity during a failover?

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

Answer: A

Explanation:
A virtual IP (VIP) address must be configured to ensure connectivity during a failover. A VIP address is a single IP address that is assigned to a group of servers or network devices. When one device fails, traffic is automatically rerouted to the remaining devices, and the VIP address is reassigned to the backup device, allowing clients to continue to access the service without interruption.
References:
- CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 6: Network Servers, p. 300

NEW QUESTION 33
- (Exam Topic 1)
Which of the following can be used to centrally manage credentials for various types of administrative privileges on configured network devices?

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

Answer: B

Explanation:
TACACS+ (Terminal Access Controller Access Control System Plus) can be used to centrally manage credentials for various types of administrative privileges on configured network devices. This protocol separates authentication, authorization, and accounting (AAA) functions, providing more granular control over access to network resources.
References:
- Network+ N10-007 Certification Exam Objectives, Objective 4.2: Given a scenario, implement secure network administration principles.

NEW QUESTION 34
- (Exam Topic 1)
Which of the following is used to track and document various types of known vulnerabilities?

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

Answer: A

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

NEW QUESTION 39
- (Exam Topic 1)
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

Answer: A

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. References: https://www.voip-info.org/voip-jitter/

NEW QUESTION 44
- (Exam Topic 1)
A new cabling certification is being requested every time a network technician rebuilds one end of a Cat 6 (vendor-certified) cable to create a crossover connection that is used to connect switches. Which of the following would address this issue by allowing the use of the original cable?

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

Answer: D

Explanation:
MDIX (medium-dependent interface crossover) is a feature that allows network devices to automatically detect and configure the appropriate cabling type, eliminating the need for crossover cables. By enabling

MDIX on the switches, a technician can use the original Cat 6 cable to create a crossover connection. References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 46
- (Exam Topic 1)
According to troubleshooting methodology, which of the following should the technician do NEXT after determining the most likely probable cause of an issue?

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

Answer: A

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

NEW QUESTION 47
- (Exam Topic 1)
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

Answer: A

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

NEW QUESTION 48
- (Exam Topic 1)
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.

Answer: A

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. References: 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/

NEW QUESTION 51
- (Exam Topic 1)
A technician receives feedback that some users are experiencing high amounts of jitter while using the wireless network. While troubleshooting the network, the technician uses the ping command with the IP address of the default gateway and verifies large variations in latency. The technician thinks the issue may be interference from other networks and non-802.11 devices. Which of the following tools should the technician use to troubleshoot the issue?

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

Answer: D

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

NEW QUESTION 53
- (Exam Topic 1)
A client recently added 100 users who are using VMs. All users have since reported slow or unresponsive desktops. Reports show minimal network congestion, zero packet loss, and acceptable packet delay. Which of the following metrics will MOST accurately show the underlying performance issues? (Choose two.)

A. CPU usage
B. Memory
C. Temperature
D. Bandwidth
E. Latency
F. Jitter

Answer: AB

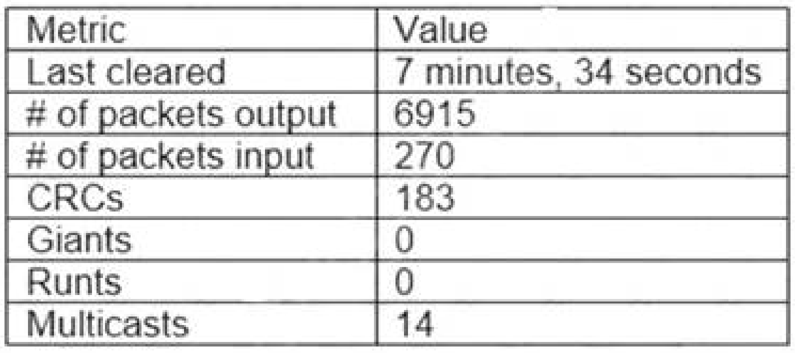
NEW QUESTION 58
- (Exam Topic 1)
Which of the following is the LARGEST MTU for a standard Ethernet frame?

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

Answer: C

Explanation:
The maximum transmission unit (MTU) is the largest size of a data packet that can be transmitted over a network. A standard Ethernet frame supports an MTU of 1500 bytes, which is the default value for most Ethernet networks. Larger MTUs are possible with jumbo frames, but they are not widely supported and may cause fragmentation or compatibility issues. References:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0),
https://en.wikipedia.org/wiki/Maximum_transmission_unit

NEW QUESTION 60
- (Exam Topic 1)
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

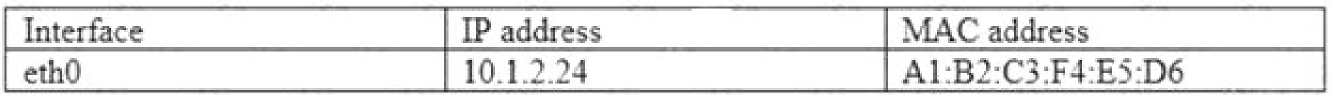
Which of the following metrics confirms there is a cabling issue?

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

Answer: C

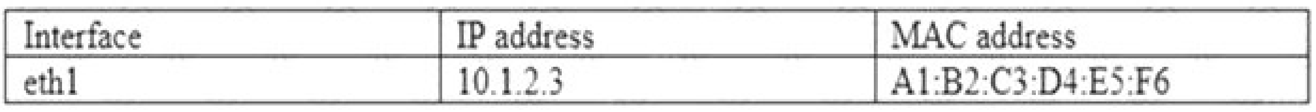
Explanation:
CRC stands for Cyclic Redundancy Check, and it is a type of error-detecting code used to detect accidental changes to raw data. If the CRC count is increasing on a particular interface, it indicates that there might be an issue with the cabling, which is causing data corruption. References: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

NEW QUESTION 64
- (Exam Topic 1)
A technician needs to configure a Linux computer for network monitoring. The technician has the following information:
Linux computer details:



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

Switch mirror port details:



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

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

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

Answer: A

Explanation:

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

NEW QUESTION 65
- (Exam Topic 1)
A company hired a technician to find all the devices connected within a network. Which of the following software tools would BEST assist the technician in completing this task?

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

Answer: A

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

NEW QUESTION 68
- (Exam Topic 1)
A network is experiencing a number of CRC errors during normal network communication. At which of the following layers of the OSI model will the administrator MOST likely start to troubleshoot?

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 4
E. Layer 5
F. Layer 6
G. Layer 7

Answer: A

Explanation:
CRC errors are cyclic redundancy check errors that occur when data is corrupted during transmission. CRC errors are usually caused by physical layer issues such as faulty cables, connectors, ports, or interference. The network administrator will most likely start to troubleshoot at layer 1 of the OSI model, which is the physical layer that deals with the transmission of bits over a medium. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 4.0 Network Troubleshooting and Tools, Objective 4.1 Given a scenario, implement network troubleshooting methodology.

NEW QUESTION 71
- (Exam Topic 1)
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

Answer: B

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

NEW QUESTION 72
- (Exam Topic 1)
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

Answer: B

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.
References:
> CompTIA Network+ Certification Study Guide

NEW QUESTION 75
- (Exam Topic 1)
Which of the following is the physical topology for an Ethernet LAN?

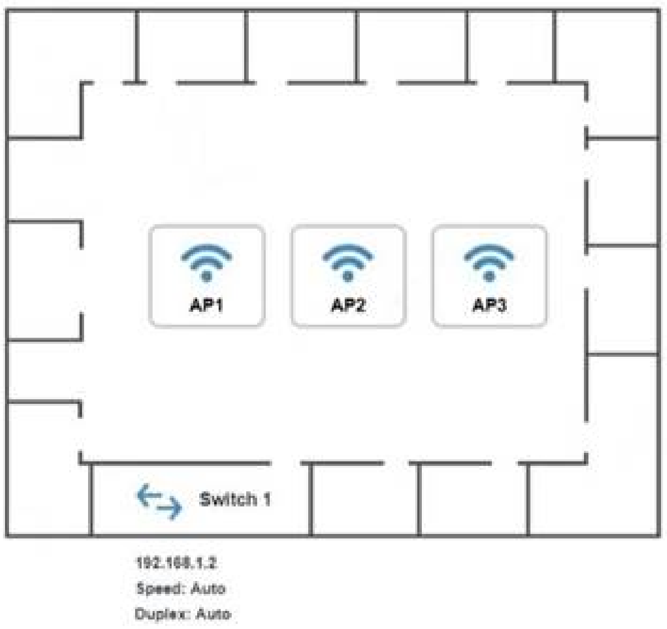
A. Bus
B. Ring
C. Mesh
D. Star

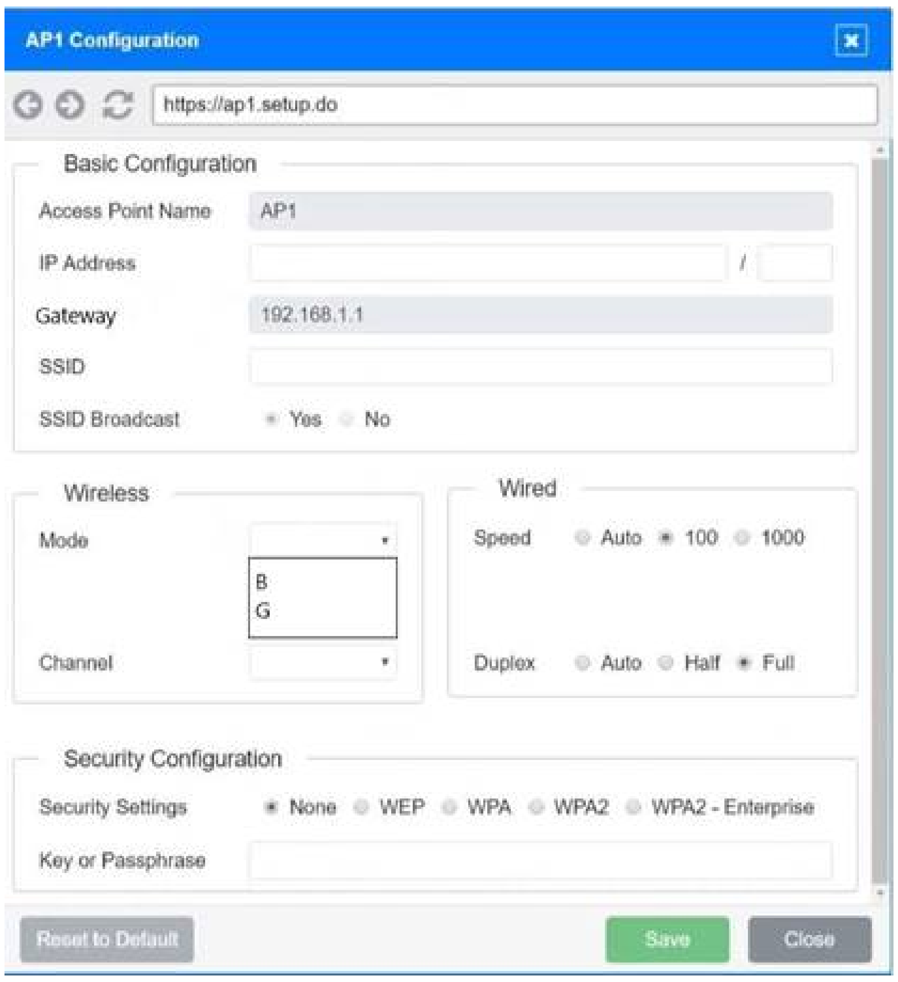
Answer: D

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

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

NEW QUESTION 76
- (Exam Topic 1)
SIMULATION
You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:
The SSIDs need to be configured as CorpNet with a key of S3cr3t! The wireless signals should not interfere with each other
The subnet the Access Points and switch are on should only support 30 devices maximum The Access Points should be configured to only support TKIP clients at a maximum speed 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.




AP1 Configuration

https://ap1.setup.do

Basic Configuration

Access Point Name	AP1
IP Address	/
Gateway	192.168.1.1
SSID	
SSID Broadcast	● Yes ○ No

Wireless

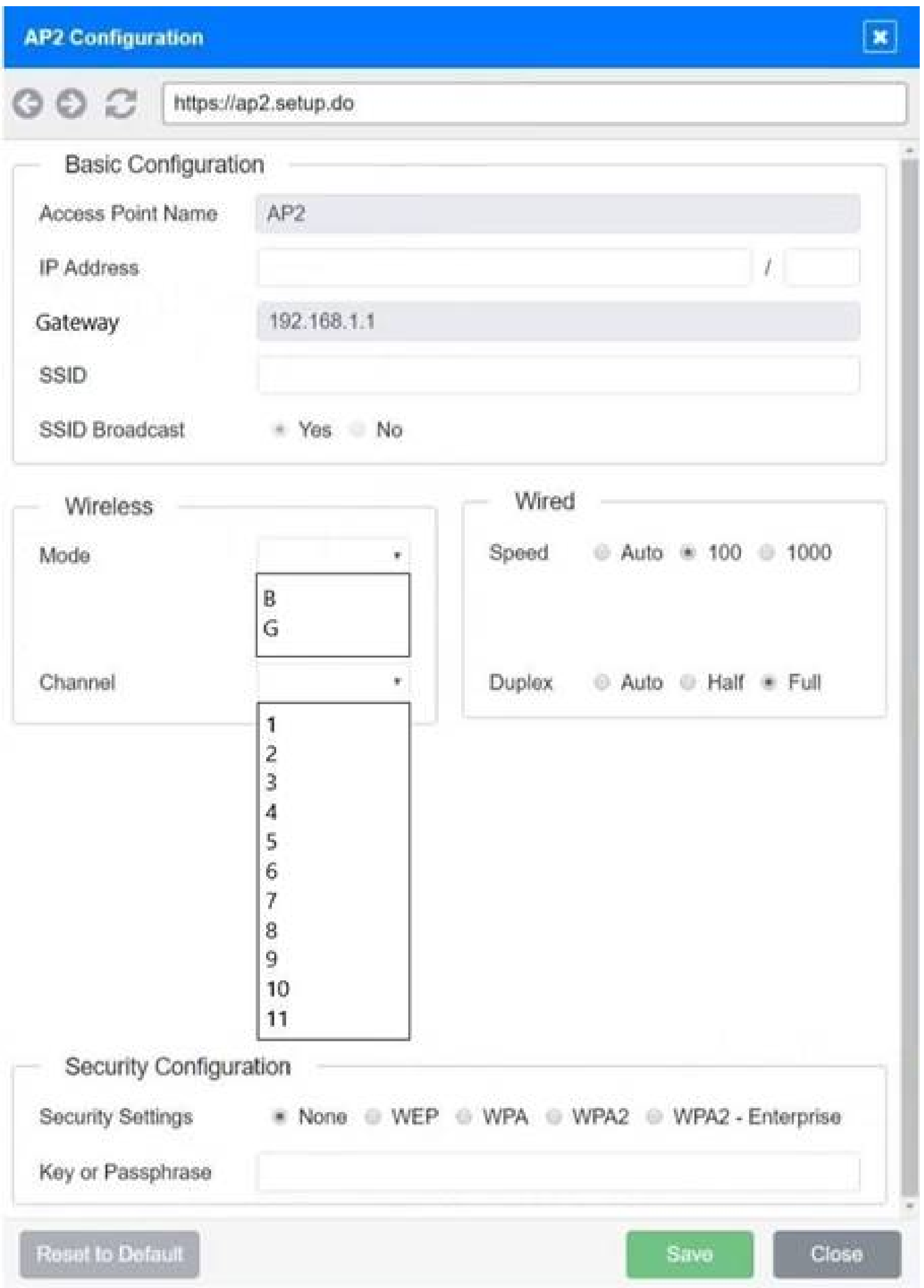
Mode: B / G
Channel:

Wired

Speed: ○ Auto ● 100 ○ 1000
Duplex: ○ Auto ○ Half ● Full

Security Configuration

Security Settings: ● None ○ WEP ○ WPA ○ WPA2 ○ WPA2 - Enterprise
Key or Passphrase:



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

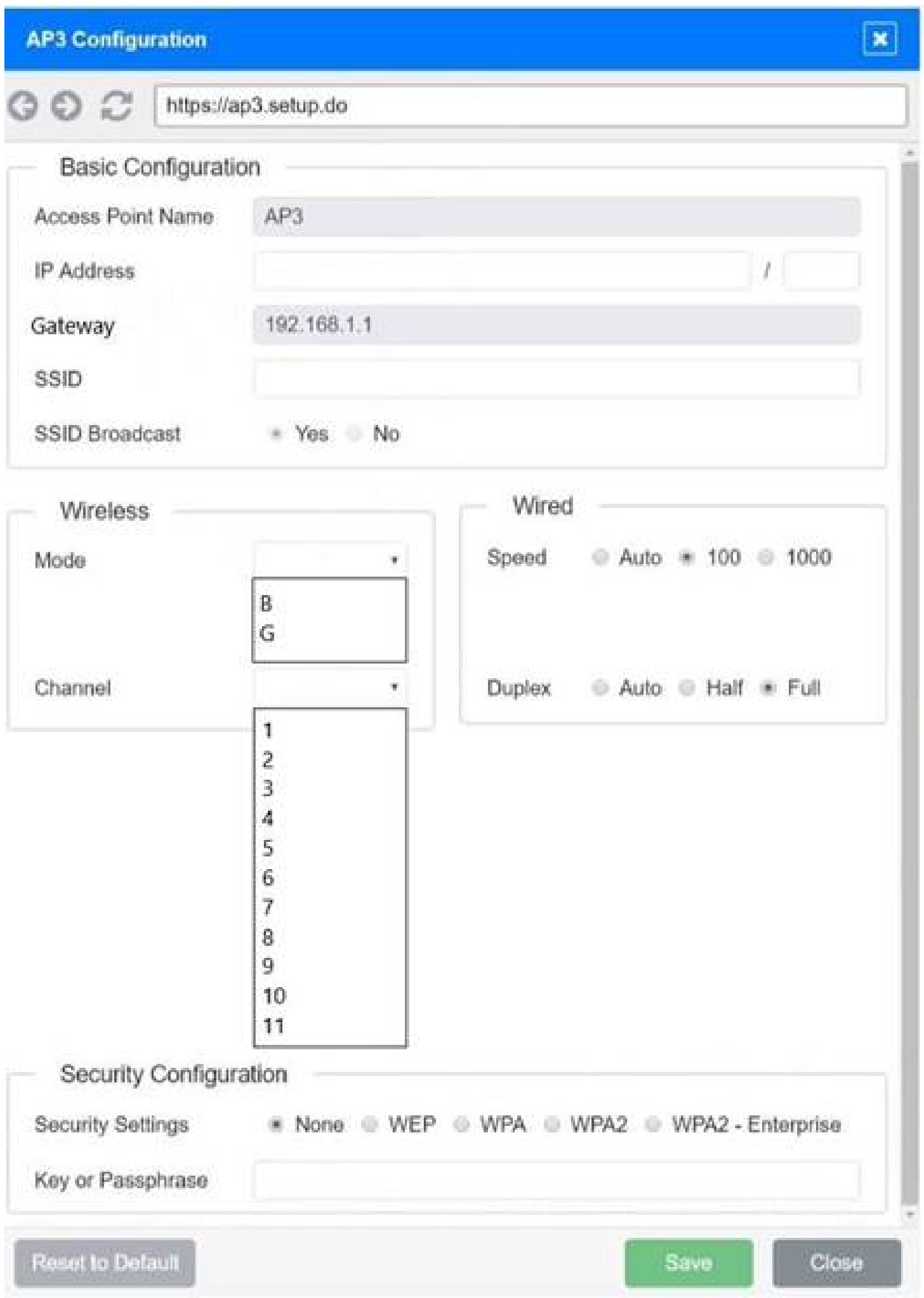
Speed: ○ Auto ● 100 ○ 1000

Duplex: ○ Auto ○ Half ● Full

Security Configuration

Security Settings: ● None ○ WEP ○ WPA ○ WPA2 ○ WPA2 - Enterprise

Key or Passphrase:



AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name: AP3

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast: ● Yes ○ No

Wireless

Mode: B, G

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

Wired

Speed: ○ Auto ● 100 ○ 1000

Duplex: ○ Auto ○ Half ● Full

Security Configuration

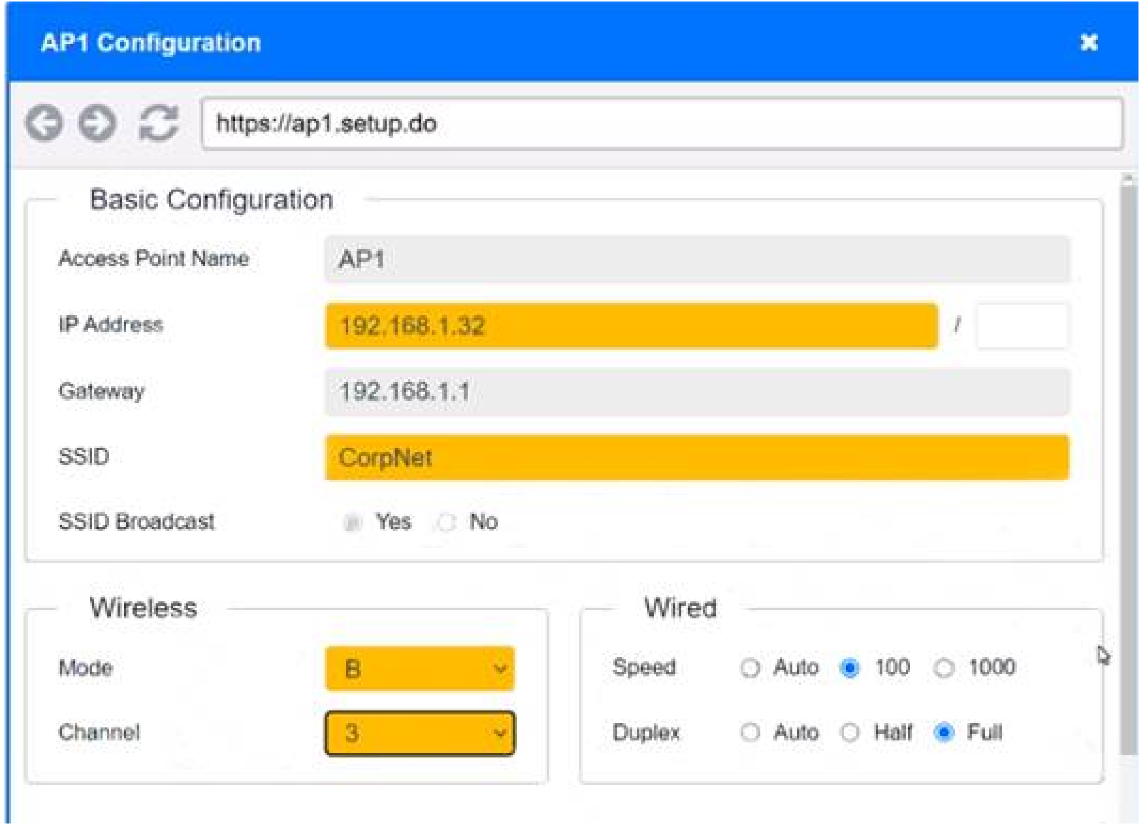
Security Settings: ● None ○ WEP ○ WPA ○ WPA2 ○ WPA2 - Enterprise

Key or Passphrase:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
On the first exhibit, the layout should be as follows



AP1 Configuration

https://ap1.setup.do

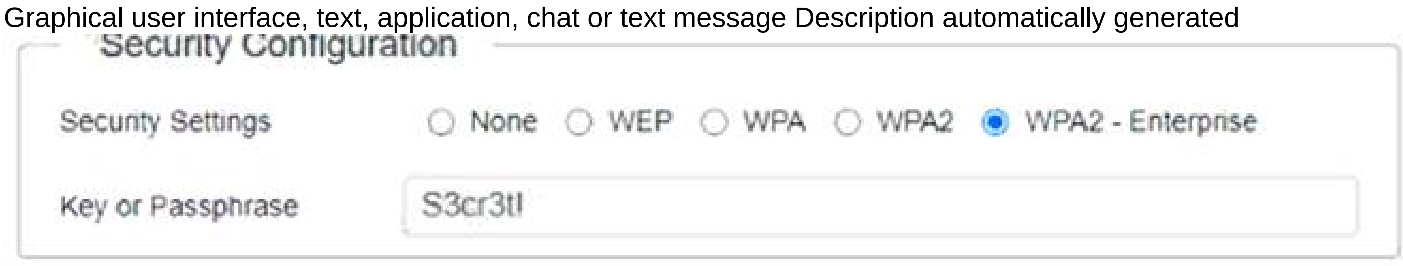
Basic Configuration

Access Point Name: AP1
IP Address: 192.168.1.32 /
Gateway: 192.168.1.1
SSID: CorpNet
SSID Broadcast: ● Yes ○ No

Wireless
Mode: B
Channel: 3

Wired
Speed: ○ Auto ● 100 ○ 1000
Duplex: ○ Auto ○ Half ● Full

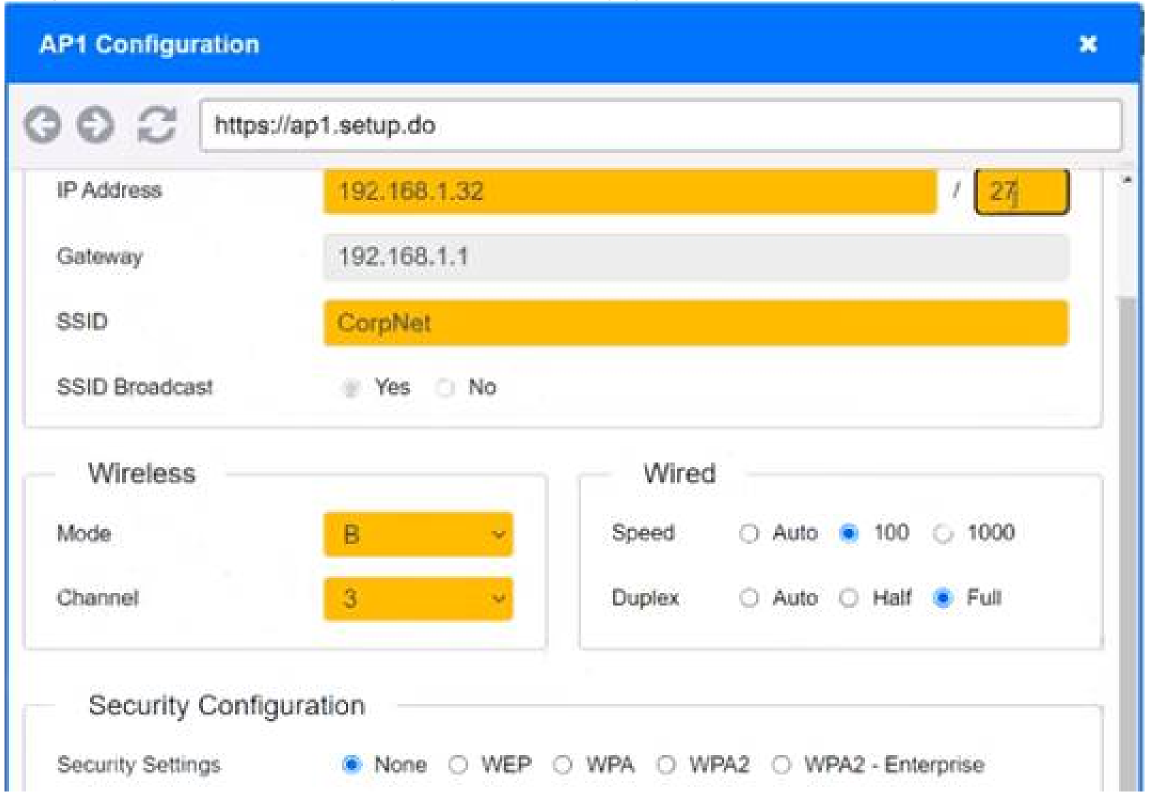
Graphical user interface, text, application, chat or text message Description automatically generated



Security Configuration

Security Settings: ○ None ○ WEP ○ WPA ○ WPA2 ● WPA2 - Enterprise
Key or Passphrase: S3cr3t!

Graphical user interface Description automatically generated



AP1 Configuration

https://ap1.setup.do

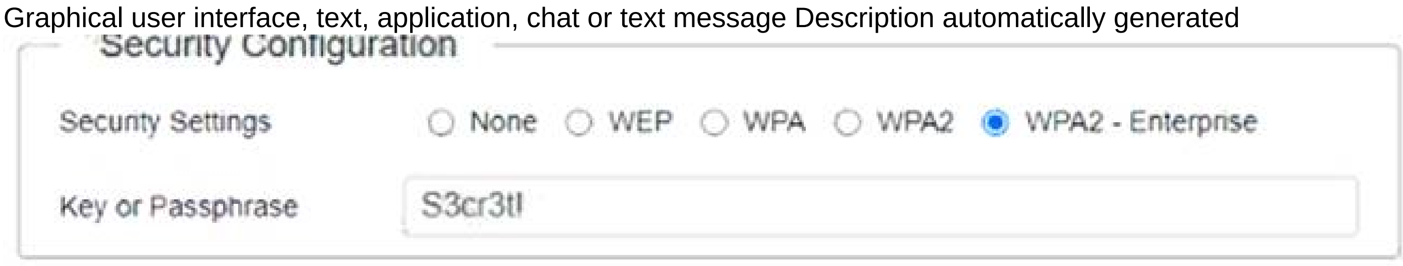
IP Address: 192.168.1.32 / 27
Gateway: 192.168.1.1
SSID: CorpNet
SSID Broadcast: ● Yes ○ No

Wireless
Mode: B
Channel: 3

Wired
Speed: ○ Auto ● 100 ○ 1000
Duplex: ○ Auto ○ Half ● Full

Security Configuration
Security Settings: ● None ○ WEP ○ WPA ○ WPA2 ○ WPA2 - Enterprise

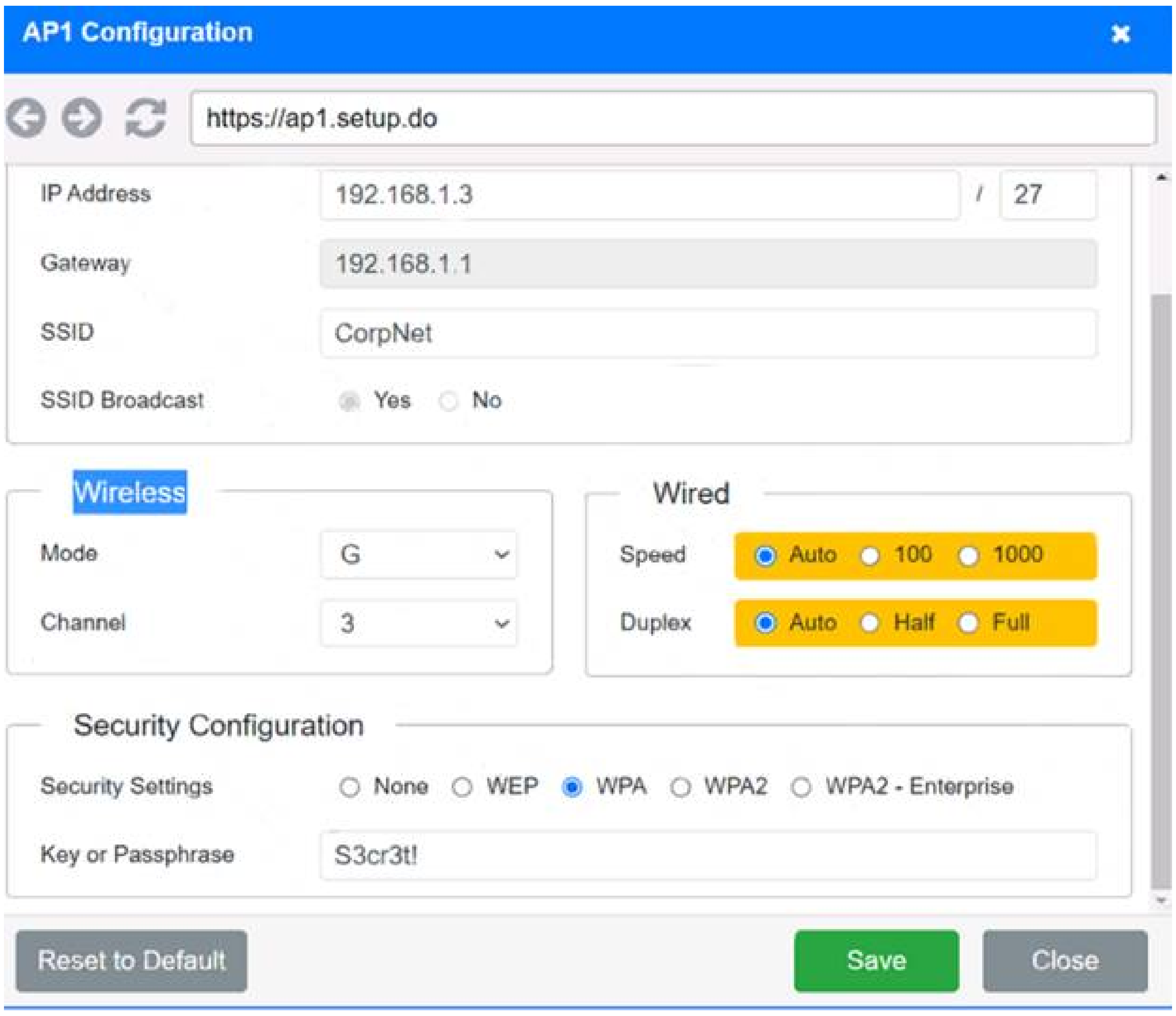
Graphical user interface, text, application, chat or text message Description automatically generated



Security Configuration

Security Settings: ○ None ○ WEP ○ WPA ○ WPA2 ● WPA2 - Enterprise
Key or Passphrase: S3cr3t!

Graphical user interface Description automatically generated



AP1 Configuration

https://ap1.setup.do

IP Address 192.168.1.3 / 27

Gateway 192.168.1.1

SSID CorpNet

SSID Broadcast ● Yes ○ No

Wireless

Mode G

Channel 3

Wired

Speed ● Auto ○ 100 ○ 1000

Duplex ● Auto ○ Half ○ Full

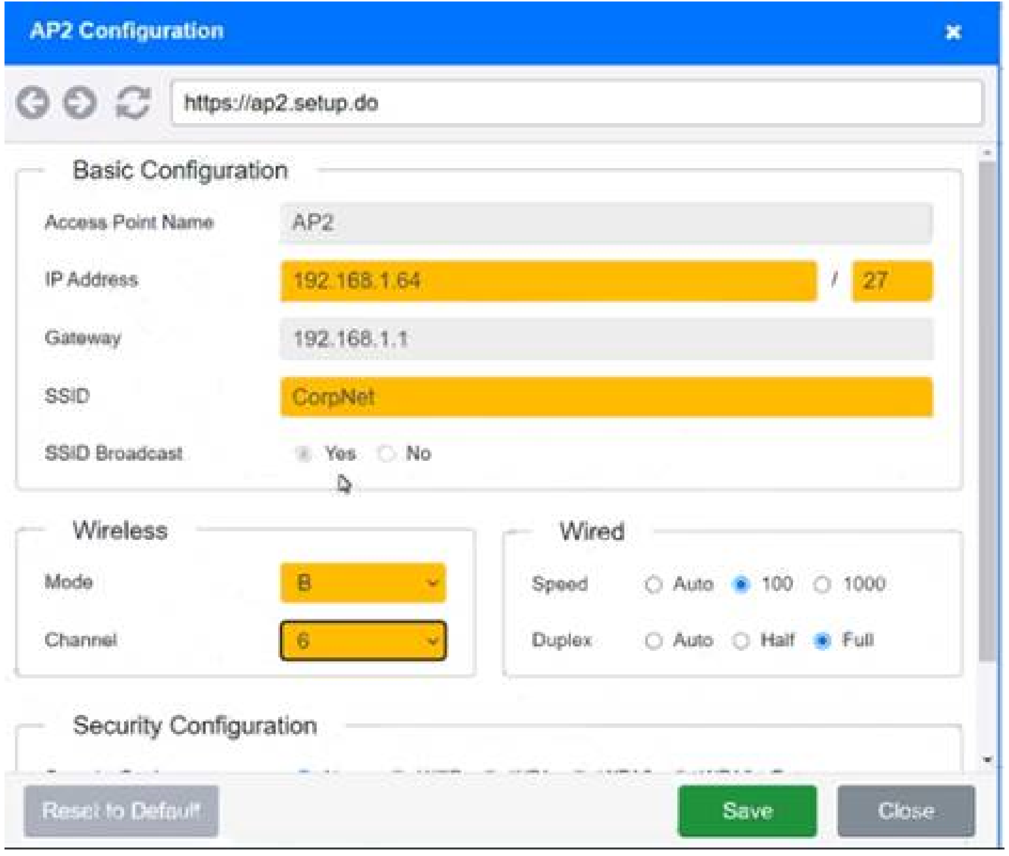
Security Configuration

Security Settings ○ None ○ WEP ● WPA ○ WPA2 ○ WPA2 - Enterprise

Key or Passphrase S3cr3t!

Exhibit 2 as follows Access Point Name AP2

Graphical user interface Description automatically generated



AP2 Configuration

https://ap2.setup.do

Basic Configuration

Access Point Name AP2

IP Address 192.168.1.64 / 27

Gateway 192.168.1.1

SSID CorpNet

SSID Broadcast ● Yes ○ No

Wireless

Mode B

Channel 6

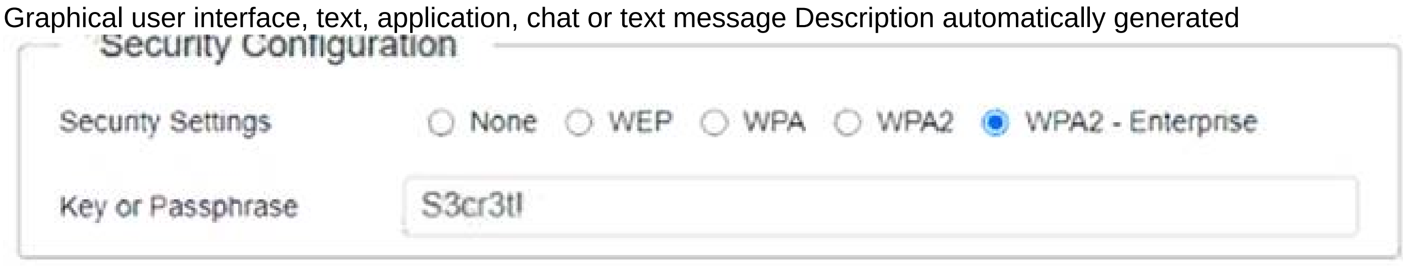
Wired

Speed ○ Auto ● 100 ○ 1000

Duplex ○ Auto ○ Half ● Full

Security Configuration

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

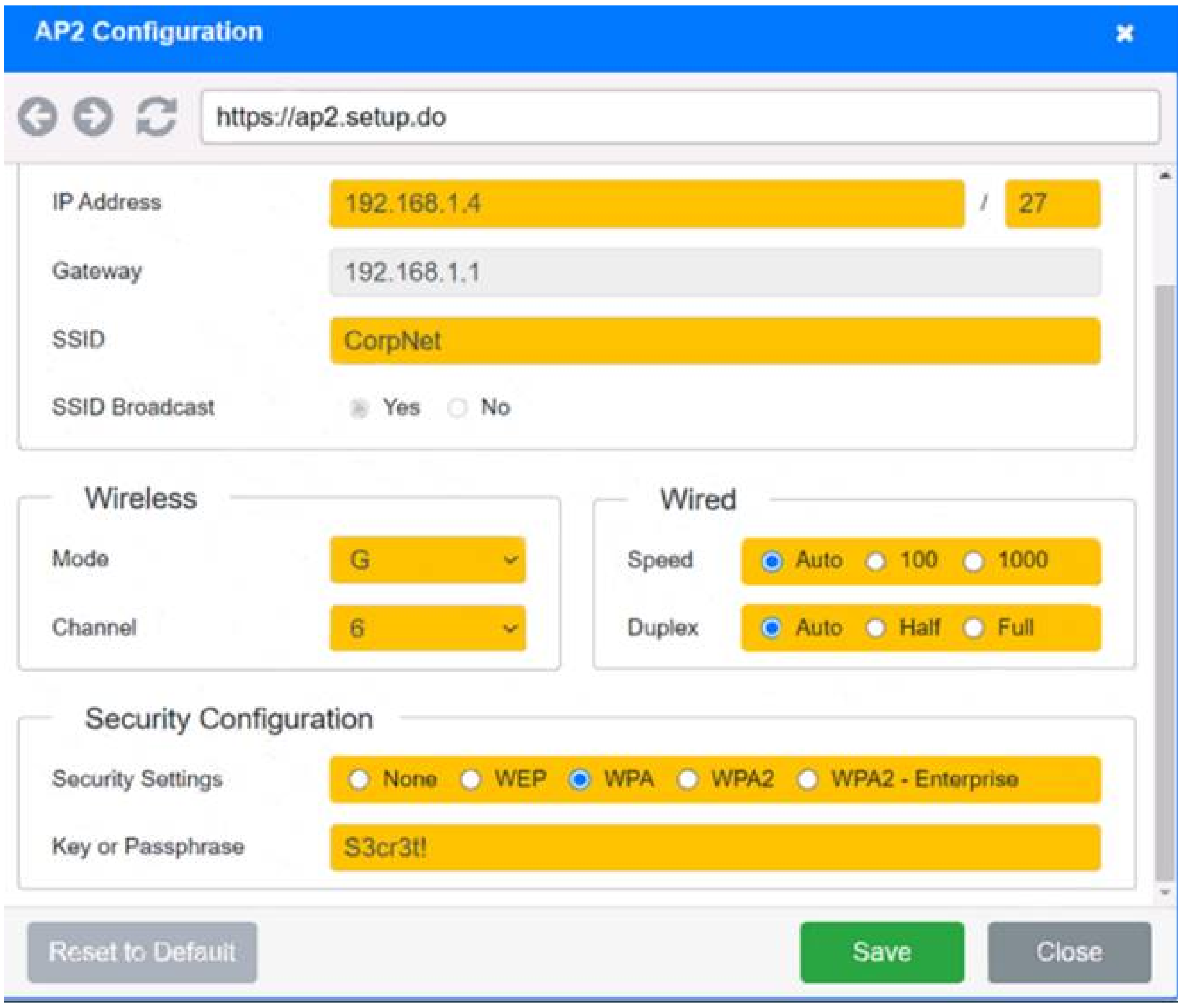


Security Configuration

Security Settings ○ None ○ WEP ○ WPA ○ WPA2 ● WPA2 - Enterprise

Key or Passphrase S3cr3t!

Graphical user interface Description automatically generated



AP2 Configuration

https://ap2.setup.do

IP Address: 192.168.1.4 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ● Yes ○ No

Wireless

Mode: G

Channel: 6

Wired

Speed: ● Auto ○ 100 ○ 1000

Duplex: ● Auto ○ Half ○ Full

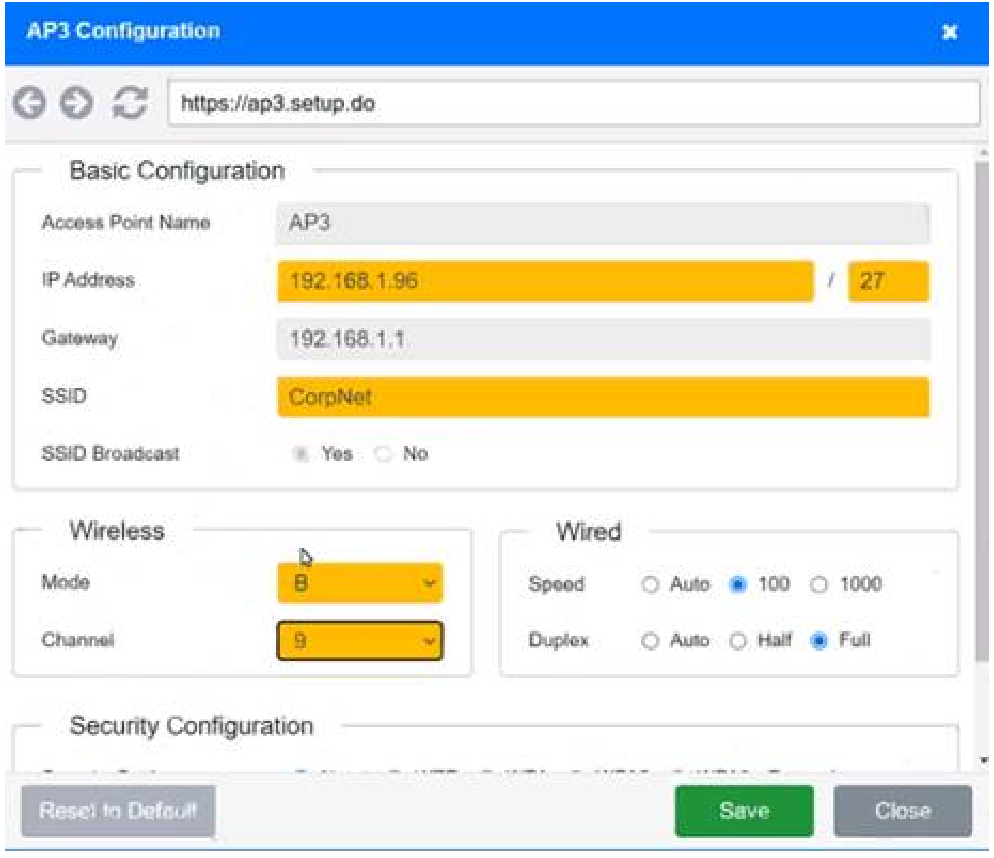
Security Configuration

Security Settings: ○ None ○ WEP ● WPA ○ WPA2 ○ WPA2 - Enterprise

Key or Passphrase: S3cr3t!

Exhibit 3 as follows Access Point Name AP3

Graphical user interface Description automatically generated



AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name: AP3

IP Address: 192.168.1.96 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ● Yes ○ No

Wireless

Mode: B

Channel: 9

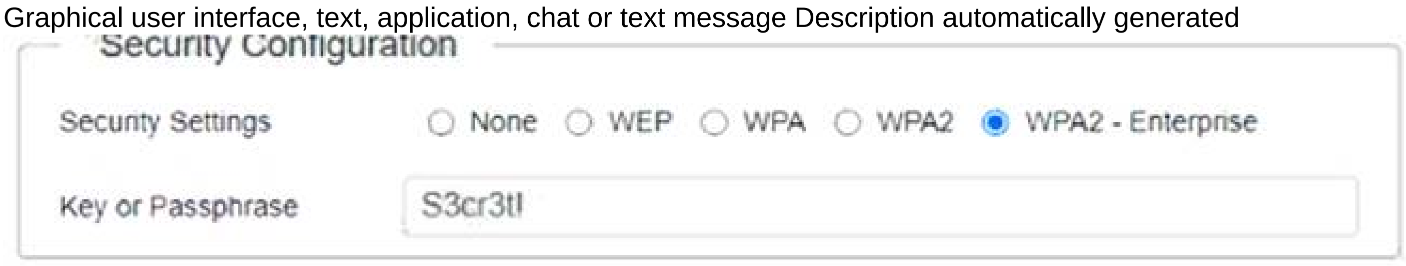
Wired

Speed: ○ Auto ● 100 ○ 1000

Duplex: ○ Auto ○ Half ● Full

Security Configuration

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

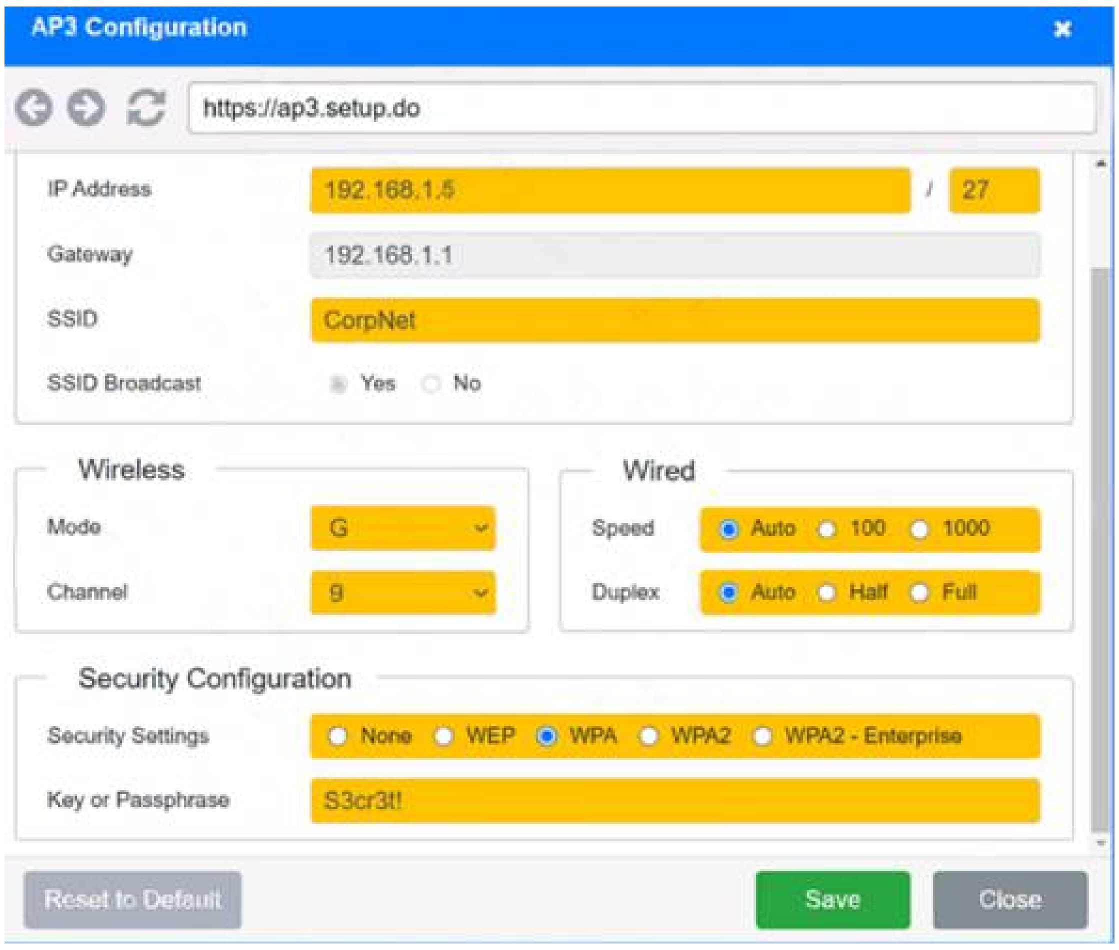


Security Configuration

Security Settings: ○ None ○ WEP ○ WPA ○ WPA2 ● WPA2 - Enterprise

Key or Passphrase: S3cr3t!

Graphical user interface Description automatically generated



IP Address 192.168.1.5 / 27

Gateway 192.168.1.1

SSID CorpNet

SSID Broadcast ● Yes ○ No

Mode G

Channel 9

Speed ● Auto ○ 100 ○ 1000

Duplex ● Auto ○ Half ○ Full

Security Settings ○ None ○ WEP ● WPA ○ WPA2 ○ WPA2 - Enterprise

Key or Passphrase S3cr3t!

NEW QUESTION 79
- (Exam Topic 1)
Which of the following routing protocols is used to exchange route information between public autonomous systems?

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

Answer: B

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

NEW QUESTION 84
- (Exam Topic 1)
A network administrator walks into a datacenter and notices an unknown person is following closely. The administrator stops and directs the person to the security desk. Which of the following attacks did the network administrator prevent?

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

Answer: B

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

NEW QUESTION 86
- (Exam Topic 1)
An IT organization needs to optimize speeds for global content distribution and wants to reduce latency in high-density user locations. Which of the following technologies BEST meets the organization's requirements?

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

Answer: D

Explanation:

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

NEW QUESTION 90
- (Exam Topic 1)
Client devices cannot enter a network, and the network administrator determines the DHCP scope is exhausted. The administrator wants to avoid creating a new DHCP pool. Which of the following can the administrator perform to resolve the issue?

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

Answer: D

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

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

NEW QUESTION 95
- (Exam Topic 1)
Which of the following is MOST likely to generate significant East-West traffic in a datacenter?

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

Answer: B

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

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

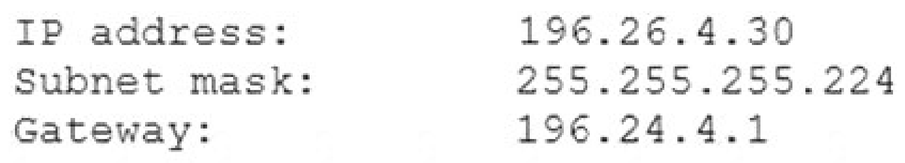
NEW QUESTION 97
- (Exam Topic 1)
Which of the following BEST describes a network appliance that warns of unapproved devices that are accessing the network?

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

Answer: D

Explanation:
IDS stands for intrusion detection system, which is a network appliance that monitors network traffic and alerts administrators of any suspicious or malicious activity. An IDS can warn of unapproved devices that are accessing the network by detecting anomalies, signatures, or behaviors that indicate unauthorized access attempts or attacks. References:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.cisco.com/c/en/us/products/security/what-is-an-intrusion-detection-system-ids.html

NEW QUESTION 99
- (Exam Topic 1)
A branch of a company recently switched to a new ISP. The network engineer was given a new IP range to assign. The ISP assigned 196.26.4.0/26, and the branch gateway router now has the following configurations on the interface that peers to the ISP:



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

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

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

Answer: C

Explanation:
The IP address configured on the router interface is 196.26.4.1/26, which belongs to the IP range assigned by the ISP (196.26.4.0/26). However, this IP address is

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

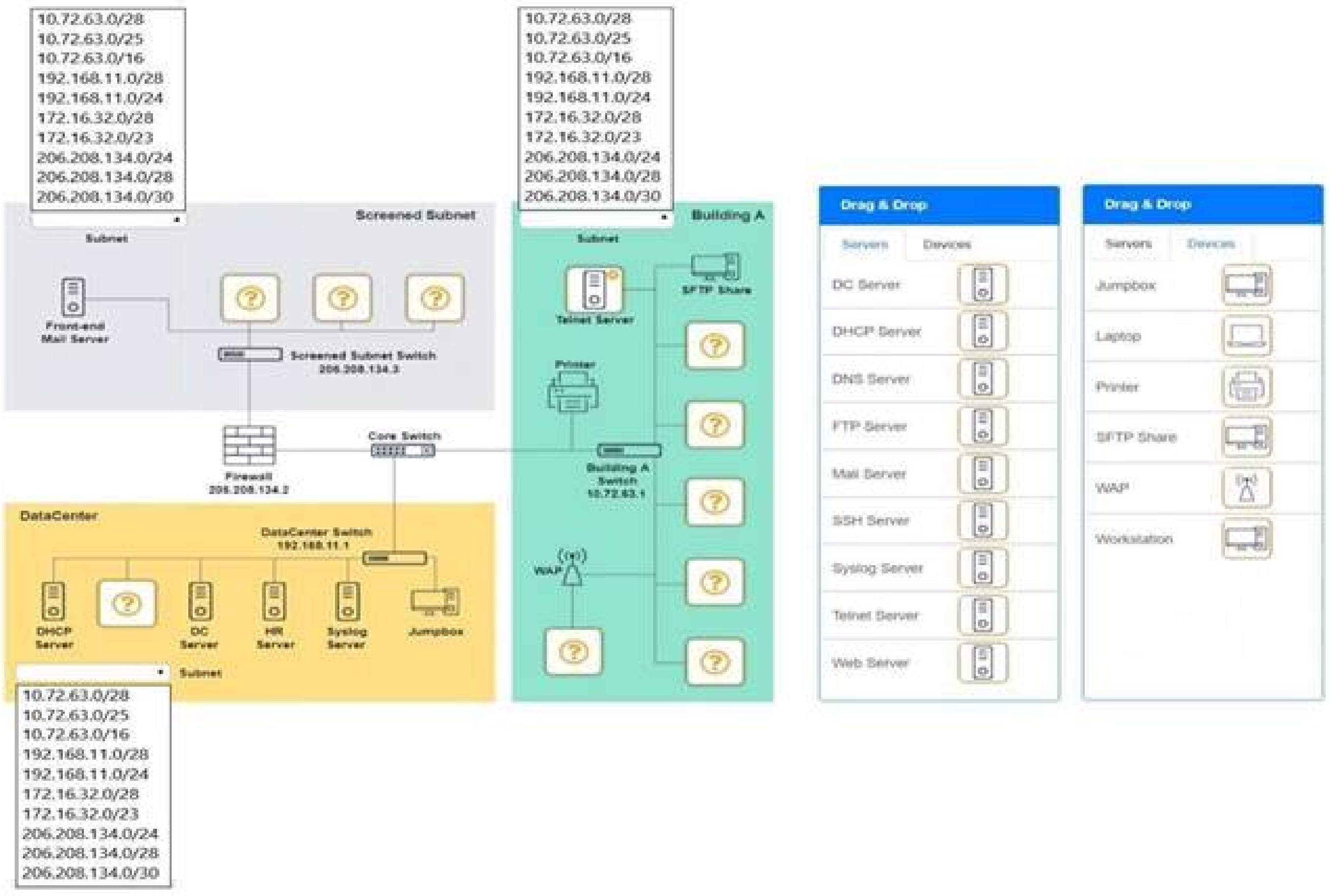
NEW QUESTION 104
- (Exam Topic 1)
A network technician needs to ensure outside users are unable to telnet into any of the servers at the datacenter. Which of the following ports should be blocked when checking firewall configuration?

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

Answer: B

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

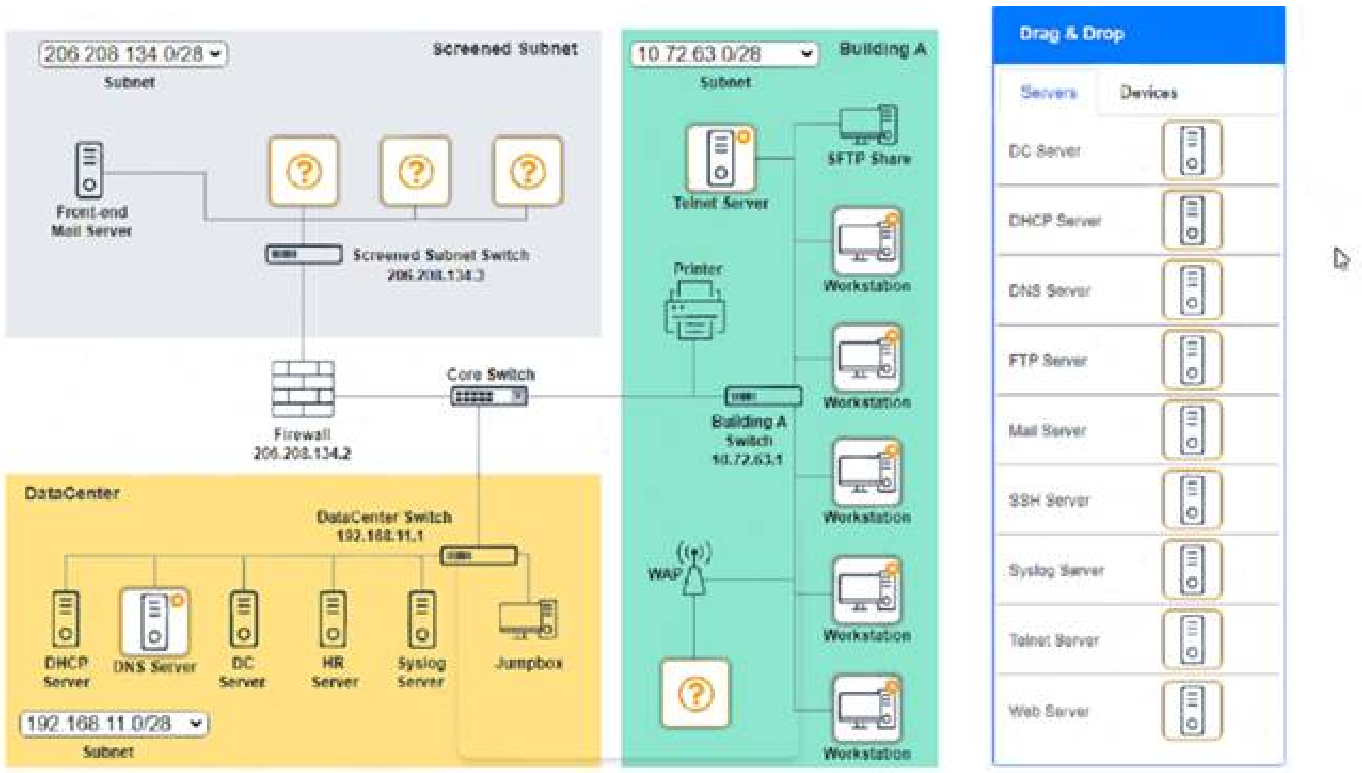
NEW QUESTION 109
- (Exam Topic 1)
You are tasked with verifying the following requirements are met in order to ensure network security. Requirements:
Datacenter
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic Building A
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
Provide devices to support 5 additional different office users
Add an additional mobile user
Replace the Telnet server with a more secure solution Screened subnet
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
Provide a server to handle external 80/443 traffic Provide a server to handle port 20/21 traffic INSTRUCTIONS
Drag and drop objects onto the appropriate locations. Objects can be used multiple times and not all placeholders need to be filled.
Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Screened Subnet devices – Web server, FTP server
Building A devices – SSH server top left, workstations on all 5 on the right, laptop on bottom left DataCenter devices – DNS server.



NEW QUESTION 110
- (Exam Topic 1)
Which of the following connector types would have the MOST flexibility?

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

Answer: A

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. References: https://www.fs.com/what-is-sfp-transceiver-aid-11.html

NEW QUESTION 113
- (Exam Topic 1)
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

Answer: C

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. References: 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.

NEW QUESTION 114
- (Exam Topic 1)
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

Answer: A

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. References: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-roam-faq.html

NEW QUESTION 119
- (Exam Topic 1)

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

Answer: B

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. References: Network+ Certification Study Guide, Chapter 8: Network Troubleshooting

NEW QUESTION 124
- (Exam Topic 1)
The following configuration is applied to a DHCP server connected to a VPN concentrator:

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

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

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

Answer: A

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

NEW QUESTION 125
- (Exam Topic 1)
A network technician is manually configuring the network settings for a new device and is told the network block is 192.168.0.0/20. Which of the following subnets should the technician use?

A. 255.255.128.0
B. 255.255.192.0
C. 255.255.240.0
D. 255.255.248.0

Answer: C

Explanation:
A subnet mask is a binary number that indicates which bits of an IP address belong to the network portion and which bits belong to the host portion. A slash notation (/n) indicates how many bits are used for the network portion. A /20 notation means that 20 bits are used for the network portion and 12 bits are used for the host portion. To convert /20 to a dotted decimal notation, we need to write 20 ones followed by 12 zeros in binary and then divide them into four octets separated by dots. This gives us 11111111.11111111.11110000.00000000 or 255.255.240.0 in decimal. References: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.techopedia.com/definition/950/subnet-mask

NEW QUESTION 130
- (Exam Topic 2)
A network engineer is designing a new secure wireless network. The engineer has been given the following requirements:
* 1 Must not use plaintext passwords
* 2 Must be certificate based
* 3. Must be vendor neutral
Which of the following methods should the engineer select?

A. TWP-RC4
B. CCMP-AES
C. EAP-TLS
D. WPA2

Answer: C

Explanation:
EAP-TLS is the method that should be selected to meet the requirements for designing a new secure wireless network. EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) is an authentication protocol that uses X.509 digital certificates for both clients and servers. It provides strong security and mutual authentication by using TLS encryption and public key cryptography. It does not use plaintext passwords or shared secrets that can be compromised or guessed. It is also an open standard that is vendor neutral and supported by most wireless devices1. References: https://www.securew2.com/blog/what-is-eap-tls
1

NEW QUESTION 131
- (Exam Topic 2)
A network technician needs to correlate security events to analyze a suspected intrusion. Which of the following should the technician use?

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

Answer: D

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

NEW QUESTION 136
- (Exam Topic 2)
A business is using the local cable company to provide Internet access. Which of the following types of cabling will the cable company MOST likely use from the demarcation point back to the central office?

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

Answer: C

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

NEW QUESTION 139
- (Exam Topic 2)
A network technician is observing the behavior of an unmanaged switch when a new device is added to the network and transmits data. Which of the following BEST describes how the switch processes this information?

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

Answer: C

Explanation:
The switch processes the data by flooding it out of every port, except the one on which it came in. Flooding is a process where a switch sends a data frame to all ports except the source port when it does not have an entry for the destination MAC address in its MAC address table. Flooding allows the switch to learn the MAC addresses of the devices connected to its ports and update its MAC address table accordingly. Flooding also ensures that the data frame reaches its intended destination, even if the switch does not know its location. References: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10556-16.html

NEW QUESTION 143
- (Exam Topic 2)
A network technician is reviewing an upcoming project's requirements to implement IaaS. Which of the following should the technician consider?

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

Answer: D

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

NEW QUESTION 148
- (Exam Topic 2)
A corporation has a critical system that would cause unrecoverable damage to the brand if it was taken offline. Which of the following disaster recovery solutions should the corporation implement?

A. Full backups
B. Load balancing

C. Hot site
D. Snapshots

Answer: C

Explanation:
A hot site is the disaster recovery solution that the corporation should implement for its critical system that would cause unrecoverable damage to the brand if it was taken offline. A hot site is a fully operational backup site that can take over the primary site’s functions in case of a disaster or disruption. A hot site has all the necessary hardware, software, data, network connections, and personnel to resume normal operations with minimal downtime. A hot site is suitable for systems that require high availability and cannot afford any data loss or interruption. References: https://www.enterprisestorageforum.com/management/disaster-recovery-site/ 1

NEW QUESTION 150
- (Exam Topic 2)
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

Answer: A

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.
References:
https://www.comptia.org/blog/what-is-a-honeypot

NEW QUESTION 155
- (Exam Topic 2)
A lab environment hosts Internet-facing web servers and other experimental machines, which technicians use for various tasks A technician installs software on one of the web servers to allow communication to the company's file server, but it is unable to connect to it Other machines in the building are able to retrieve files from the file server. Which of the following is the MOST likely reason the web server cannot retrieve the files, and what should be done to resolve the problem?

A. The lab environment's IDS is blocking the network traffic 1 he technician can whitelist the new application in the IDS
B. The lab environment is located in the DM2, and traffic to the LAN zone is denied by defaul
C. The technician can move the computer to another zone or request an exception from the administrator.
D. The lab environment has lost connectivity to the company router, and the switch needs to be rebooted.The technician can get the key to the wiring closet and manually restart the switch
E. The lab environment is currently set up with hubs instead of switches, and the requests are getting bounced back The technician can submit a request for upgraded equipment to management.

Answer: B

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

NEW QUESTION 157
- (Exam Topic 2)
Two remote offices need to be connected securely over an untrustworthy MAN. Each office needs to access network shares at the other site. Which of the following will BEST provide this functionality?

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

Answer: C

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

NEW QUESTION 160
- (Exam Topic 2)
A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the AP utilize?

A. Omni

B. Directional
C. Yagi
D. Parabolic

Answer: A

Explanation:
An omni antenna should be used by the AP to provide service in a radius surrounding a radio. An omni antenna is a type of antenna that has a 360-degree horizontal radiation pattern. It can provide wireless coverage in all directions from the antenna with varying degrees of vertical coverage. It is suitable for indoor environments where users are located around the AP1. References: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html 1

NEW QUESTION 164
- (Exam Topic 2)
An organization wants to implement a method of centrally managing logins to network services. Which of the following protocols should the organization use to allow for authentication, authorization and auditing?

A. MS-CHAP
B. RADIUS
C. LDAPS
D. RSTP

Answer: B

Explanation:
RADIUS (Remote Authentication Dial-In User Service) is a protocol that should be used by the organization to allow for authentication, authorization, and auditing of network services. RADIUS is an AAA (Authentication, Authorization, and Accounting) protocol that manages network access by verifying user credentials, granting access permissions, and logging user activities. RADIUS uses a client-server model where a RADIUS client (such as a router, switch, or VPN server) sends user information to a RADIUS server (such as an authentication server) for verification and authorization. The RADIUS server can also send accounting information to another server for billing or reporting purposes. References:
https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838

NEW QUESTION 166
- (Exam Topic 2)
A network technician has multimode fiber optic cable available in an existing IDF. Which of the following Ethernet standards should the technician use to connect the network switch to the existing fiber?

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

Answer: C

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

NEW QUESTION 168
- (Exam Topic 2)
A user reports a weak signal when walking 20ft (61 m) away from the WAP in one direction, but a strong signal when walking 20ft in the opposite direction The technician has reviewed the configuration and confirmed the channel type is correct There is no jitter or latency on the connection Which of the following would be the MOST likely cause of the issue?

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

Answer: A

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

NEW QUESTION 171
- (Exam Topic 2)
Which of the following is a system that is installed directly on a server's hardware and abstracts the hardware from any guest machines?

A. Storage array
B. Type 1 hypervisor
C. Virtual machine
D. Guest QS

Answer: B

Explanation:
A type 1 hypervisor is a system that is installed directly on a server's hardware and abstracts the hardware from any guest machines. A hypervisor is a software layer that enables virtualization by creating and managing virtual machines (VMs) on a physical host. A type 1 hypervisor, also known as a bare-metal hypervisor or a native hypervisor, runs directly on the host's hardware without requiring an underlying operating system (OS). It provides better performance and security than a type 2 hypervisor, which runs on top of an existing OS and relies on it for hardware access. References:
https://www.vmware.com/topics/glossary/content/hypervisor

NEW QUESTION 172
- (Exam Topic 2)
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

Answer: A

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. References:
https://www.comptia.org/blog/what-is-syslog

NEW QUESTION 175
- (Exam Topic 2)
A local firm has hired a consulting company to clean up its IT infrastructure. The consulting company notices remote printing is accomplished by port forwarding via publicly accessible IPs through the firm's firewall Which of the following would be the MOST appropriate way to enable secure remote printing?

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

Answer: B

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

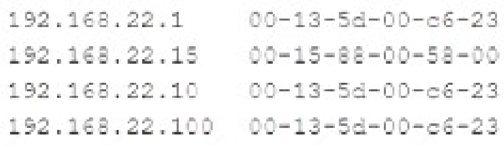
NEW QUESTION 178
- (Exam Topic 2)
A network technician is investigating an issue with a desktop that is not connecting to the network. The desktop was connecting successfully the previous day, and no changes were made to the environment. The technician locates the switchport where the device is connected and observes the LED status light on the switchport is not lit even though the desktop is turned on Other devices that arc plugged into the switch are connecting to the network successfully Which of the following is MOST likely the cause of the desktop not connecting?

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

Answer: D

Explanation:
A damaged cable is most likely the cause of the desktop not connecting to the network. A damaged cable can cause physical layer issues such as loss of signal, attenuation, interference, or crosstalk. These issues can prevent the desktop from establishing a link with the switch and result in the LED status light on the switchport being off. Other possible causes of physical layer issues are faulty connectors, ports, or transceivers. References:
https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/14119-37.html

NEW QUESTION 181
- (Exam Topic 2)
Given the following output:



```
192.168.22.1     00-13-5d-00-c6-23
192.168.22.15    00-15-88-00-58-00
192.168.22.10    00-13-5d-00-c6-23
192.168.22.100   00-13-5d-00-c6-23
```

Which of the following attacks is this MOST likely an example of?

A. ARP poisoning
B. VLAN hopping

C. Rogue access point
D. Amplified DoS

Answer: A

Explanation:
The output is most likely an example of an ARP poisoning attack. ARP poisoning, also known as ARP spoofing, is a type of attack that exploits the ARP protocol to associate a malicious device's MAC address with a legitimate IP address on a local area network. This allows the attacker to intercept, modify, or redirect network traffic between two devices without their knowledge. The output shows that there are multiple entries for the same IP address (192.168.1.1) with different MAC addresses in the ARP cache of the device. This indicates that an attacker has sent fake ARP replies to trick the device into believing that its MAC address is associated with the IP address of another device (such as the default gateway). References: https://www.cisco.com/c/en/us/about/security-center/arp-spoofing.html

NEW QUESTION 182
- (Exam Topic 2)
A network administrator decided to use SLAAC in an extensive IPv6 deployment to alleviate IP address management. The devices were properly connected into the LAN but autoconfiguration of the IP address did not occur as expected. Which of the following should the network administrator verify?

A. The network gateway is configured to send router advertisements.
B. A DHCP server is present on the same broadcast domain as the clients.
C. The devices support dual stack on the network layer.
D. The local gateway supports anycast routing.

Answer: A

Explanation:
SLAAC (Stateless Address Autoconfiguration) is a method for IPv6 devices to automatically configure their IP addresses based on the network prefix advertised by a router. The router sends periodic router advertisements (RAs) that contain the network prefix and other parameters for the devices to use. If the network gateway is not configured to send RAs, then SLAAC will not work. A DHCP server is not needed for SLAAC, as the devices generate their own addresses without relying on a server. Dual stack and anycast routing are not related to SLAAC.

NEW QUESTION 186
- (Exam Topic 2)
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

Answer: C

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. References: https://www.comptia.org/blog/what-is-tacacs

NEW QUESTION 189
- (Exam Topic 2)
A firewall administrator is implementing a rule that directs HTTP traffic to an internal server listening on a non-standard socket Which of the following types of rules is the administrator implementing?

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

Answer: B

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

NEW QUESTION 191
- (Exam Topic 2)
A network technician is configuring a new firewall for a company with the necessary access requirements to be allowed through the firewall. Which of the following would normally be applied as the LAST rule in the firewall?

A. Secure SNMP
B. Port security
C. Implicit deny

D. DHCP snooping

Answer: C

Explanation:
Implicit deny is a firewall rule that blocks all traffic that is not explicitly allowed by other rules. Implicit deny is usually applied as the last rule in the firewall to ensure that only the necessary access requirements are allowed through the firewall and that any unwanted or malicious traffic is rejected. Implicit deny can also provide a default security policy and a baseline for auditing and logging purposes.
Secure SNMP is a protocol that allows network devices to send event messages to a centralized server or console for logging and analysis. Secure SNMP can be used to monitor and manage the status, performance, and configuration of network devices. Secure SNMP can also help to detect and respond to potential problems or faults on the network. However, secure SNMP is not a firewall rule; it is a network management protocol.
Port security is a feature that allows a switch to restrict the devices that can connect to a specific port based on their MAC addresses. Port security can help to prevent unauthorized access, spoofing, or MAC flooding attacks on the switch. However, port security is not a firewall rule; it is a switch feature.
DHCP snooping is a feature that allows a switch to filter DHCP messages and prevent rogue DHCP servers from assigning IP addresses to devices on the network. DHCP snooping can help to prevent IP address conflicts, spoofing, or denial-of-service attacks on the network. However, DHCP snooping is not a firewall rule; it is a switch feature.

NEW QUESTION 193
- (Exam Topic 2)
A network administrator has been directed to present the network alerts from the past week to the company's executive staff. Which of the following will provide the BEST collection and presentation of this data?

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

Answer: C

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

NEW QUESTION 197
- (Exam Topic 2)
An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch. Which of the following command-line tools should the technician use to determine where the incident is occurring?

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

Answer: D

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

NEW QUESTION 202
- (Exam Topic 2)
Which of the following OSI model layers is where conversations between applications are established, coordinated, and terminated?

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

Answer: A

Explanation:
Reference: https://www.techtarget.com/searchnetworking/definition/OSI#:~:text=The%20session%20layer,and%20termina
The session layer is where conversations between applications are established, coordinated, and terminated. It is responsible for creating, maintaining, and ending sessions between different devices or processes. The physical layer deals with the transmission of bits over a medium. The presentation layer formats and translates data for different applications. The data link layer provides reliable and error-free delivery of frames within a network.

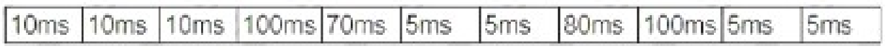
NEW QUESTION 207
- (Exam Topic 2)
A network administrator needs to implement an HDMI over IP solution. Which of the following will the network administrator MOST likely use to ensure smooth video delivery?

A. Link aggregation control
B. Port tagging
C. Jumbo frames
D. Media access control

Answer: C

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

NEW QUESTION 208
- (Exam Topic 2)
A company that uses VoIP telephones is experiencing intermittent issues with one-way audio and dropped conversations The manufacturer says the system will work if ping times are less than 50ms. The company has recorded the following ping times:



10ms	10ms	10ms	100ms	70ms	5ms	5ms	80ms	100ms	5ms	5ms

Which of the following is MOST likely causing the issue?

A. Attenuation
B. Latency
C. VLAN mismatch
D. Jitter

Answer: D

Explanation:
Jitter is most likely causing the issue of intermittent one-way audio and dropped conversations for the company that uses VoIP telephones. Jitter is a 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 10m1s. The company has recorded ping times that exceed 50ms, which indicates high jitter and latency on their network. References: https://www.voip-info.org/voip-jitter/ 1

NEW QUESTION 212
- (Exam Topic 2)
A technician is connecting DSL for a new customer. After installing and connecting the on-premises equipment, the technician verifies DSL synchronization. When connecting to a workstation, however, the link LEDs on the workstation and modem do not light up. Which of the following should the technician perform during troubleshooting?

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

Answer: D

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

NEW QUESTION 213
- (Exam Topic 2)
Which of the following is MOST commonly used to address CVEs on network equipment and/or operating systems?

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

Answer: C

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

NEW QUESTION 215
- (Exam Topic 2)
A city has hired a new employee who needs to be able to work when traveling at home and at the municipal sourcing of a neighboring city that snares services. The employee is issued a laptop, and a technician needs to train the employee on the appropriate solutions for secure access to the network from all the possible locations On which of the following solutions would the technician MOST likely train the employee?

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

D. Site-to-site VPNs between the home and city locations and site-to-site software on the employee's laptop for all other remote access

Answer: A

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

NEW QUESTION 216
- (Exam Topic 2)
Which of the following would be used to expedite MX record updates to authoritative NSs?

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

Answer: D

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

NEW QUESTION 220
- (Exam Topic 2)
A small, family-run business uses a single SOHO router to provide Internet and WiFi to its employees At the start of a new week, employees come in and find their usual WiFi network is no longer available, and there is a new wireless network to which they cannot connect. Given that information, which of the following should have been done to avoid this situation'

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

Answer: D

Explanation:
The default credentials are the username and password that come with a device or service when it is first installed or configured. They are often easy to guess or find online, which makes them vulnerable to unauthorized access or attacks. The default credentials should be changed to something unique and strong as soon as possible to avoid this situation. If the default credentials were not changed, someone could have accessed the SOHO router and changed the WiFi settings without the employees’ knowledge. References: https://www.comptia.org/blog/network-security-basics-6-easy-ways-to-protect-your-network

NEW QUESTION 225
- (Exam Topic 2)
A company wants to implement a large number of WAPs throughout its building and allow users to be able to move around the building without dropping their connections Which of the following pieces of equipment would be able to handle this requirement?

A. A VPN concentrator
B. A load balancer
C. A wireless controller
D. A RADIUS server

Answer: C

Explanation:
A wireless controller would be able to handle the requirement of implementing a large number of WAPs throughout the building and allowing users to move around without dropping their connections. A wireless controller is a device that centrally manages and configures multiple wireless access points (WAPs) on a network. It can provide features such as load balancing, roaming, security, QoS, and monitoring for the wireless network. A wireless controller can also support wireless mesh networks, where some WAPs act as relays for other WAPs to extend the wireless coverage. References: https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/index.html

NEW QUESTION 227
- (Exam Topic 2)
A network administrator is setting up several IoT devices on a new VLAN and wants to accomplish the following
* 1. Reduce manual configuration on each system
* 2. Assign a specific IP address to each system
* 3. Allow devices to move to different switchports on the same VLAN
Which of the following should the network administrator do to accomplish these requirements?

A. Set up a reservation for each device

B. Configure a static IP on each device
C. Implement private VLANs for each device
D. Use DHCP exclusions to address each device

Answer: A

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 IoT 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.
References: https://www.comptia.org/blog/what-is-dhcp

NEW QUESTION 228
- (Exam Topic 3)
A technician is investigating a misconfiguration on a Layer 3 switch. When the technician logs in and runs a command, the following data is shown:
Which of the following commands generated this output?

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

Answer: C

Explanation:
The output shown in the image is from the show interface command, which displays information about the status and configuration of a network interface on a switch or router. The output includes the interface name, description, MAC address, IP address, speed, duplex mode, status, and statistics. The show route command displays the routing table of the device. The show config command displays the current configuration of the device. The tcpdump command captures and analyzes network traffic. The netstat -s command displays statistics for each protocol.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.4: Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

NEW QUESTION 230
- (Exam Topic 3)
Which of the following network devices can perform routing between VLANs?

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

Answer: B

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

NEW QUESTION 231
- (Exam Topic 3)
Which of the following is used to elect an STP root?

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

Answer: B

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

NEW QUESTION 235
- (Exam Topic 3)
Which of the following devices have the capability to allow communication between two different subnetworks? (Select TWO).

A. IDS
B. Access point
C. Layer 2 switch
D. Layer 3 switch
E. Router
F. Media converter

Answer: DE

NEW QUESTION 237

- (Exam Topic 3)
Which of the following has the capability to centrally manage configuration, logging, and firmware versioning for distributed devices?

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

Answer: A

Explanation:
A WLAN controller is a device that manages and controls multiple wireless access points (WAPs) in a wireless LAN (WLAN). A WLAN controller has the capability to centrally manage configuration, logging, and firmware versioning for distributed WAPs. A WLAN controller can also provide load balancing, security, and quality of service (QoS) for the WLAN.
References: Network+ Study Guide Objective 3.1: Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 238
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 242
- (Exam Topic 3)
A network administrator is installing a new server in the data center. The administrator is concerned the amount of traffic generated will exceed 1GB. and higher-throughput NiCs are not available for installation. Which of the following is the BEST solution for this issue?

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

Answer: A

NEW QUESTION 244
- (Exam Topic 3)
A non-employee was able to enter a server room. Which of the following could have prevented this from happening?

A. A security camera
B. A biometric reader
C. OTP key fob
D. Employee training

Answer: B

Explanation:
A biometric reader is a device that scans a person’s physical characteristics, such as fingerprints, iris, or face, and compares them to a database of authorized users. A biometric reader can be used to restrict access to a server room and prevent unauthorized entry. A biometric reader provides a high level of security and cannot be easily bypassed or duplicated.
References: Network+ Study Guide Objective 5.1: Summarize the importance of physical security controls.

NEW QUESTION 245
- (Exam Topic 3)
Which of the following would MOST likely utilize PoE?

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

Answer: A

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

NEW QUESTION 250

- (Exam Topic 3)
Which of the following OSI model layers would allow a user to access and download files from a remote computer?

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

Answer: D

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

NEW QUESTION 255
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 258
- (Exam Topic 3)
A technician thinks one of the router ports is flapping. Which of the following available resources should the technician use in order to determine if the router is flapping?

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

Answer: C

Explanation:
Syslog is a protocol that allows network devices to send event messages to a centralized server or console for logging and analysis1. Syslog can help a technician to determine if a router port is flapping by providing timestamps, severity levels, and descriptions of the events that occur on the router, such as interface up or down, link state change, or error messages. Syslog can also help to identify the cause and frequency of the port flapping and troubleshoot the issue.
Audit logs are records of actions or events that occur on a system or network, such as user login, file access, configuration change, or policy violation. Audit logs can help to monitor and verify the activities and behaviors of users, devices, or applications on a system or network. Audit logs can also help to detect and investigate security incidents, compliance issues, or performance problems. However, audit logs do not provide detailed information about router port flapping.
NetFlow is a protocol that collects and analyzes network traffic data for monitoring and troubleshooting purposes2. NetFlow can help to identify the sources, destinations, volumes, and types of traffic on a network. NetFlow can also help to optimize network performance, security, and capacity planning. However, NetFlow does not provide detailed information about router port flapping.
Traffic logs are records of network traffic that pass through a device or application, such as a firewall, proxy, or web server. Traffic logs can help to monitor and filter the network traffic based on rules or policies. Traffic logs can also help to detect and prevent malicious traffic, such as malware, attacks, or unauthorized access. However, traffic logs do not provide detailed information about router port flapping.

NEW QUESTION 259
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 261
- (Exam Topic 3)
A network is experiencing extreme latency when accessing a particular website. Which of the following commands will BEST help identify the issue?

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

Answer: C

NEW QUESTION 264
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 266
- (Exam Topic 3)
An administrator is attempting to add a new system to monitoring but is unsuccessful. The administrator notices the system is similar to another one on the network; however, the new one has an updated OS version. Which of the following should the administrator consider updating?

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

Answer: A

NEW QUESTION 271
- (Exam Topic 3)
Several end users viewing a training video report seeing pixelated images while watching. A network administrator reviews the core switch and is unable to find an immediate cause. Which of the following BEST explains what is occurring?

A. Jitter
B. Bandwidth
C. Latency
D. Giants

Answer: A

Explanation:
"Jitter is the loss of packets due to an overworked WAP. Jitter shows up as choppy conversations over a video call, strange jumps in the middle of an online game—pretty much anything that feels like the network has missed some data. Latency is when data stops moving for a moment due to a WAP being unable to do the work. This manifests as a Word document that stops loading, for example, or an online file that stops downloading."

NEW QUESTION 275
- (Exam Topic 3)
A network technician is troubleshooting an area where the wireless connection to devices is poor. The technician theorizes that the signal-to-noise ratio in the area is causing the issue. Which of the following should the technician do NEXT?

A. Run diagnostics on the relevant devices.
B. Move the access point to a different location.
C. Escalate the issue to the vendor's support team.
D. Remove any electronics that might be causing interference.

Answer: D

NEW QUESTION 279
- (Exam Topic 3)
An administrator needs to connect two laptops directly to each other using 802.11ac but does not have an AP available. Which of the following describes this configuration?

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

Answer: C

NEW QUESTION 281
- (Exam Topic 3)
A technician wants to monitor and provide traffic segmentation across the network. The technician would like to assign each department a specific identifier. Which of the following will the technician MOST likely use?

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

Answer: C

Explanation:
To monitor and provide traffic segmentation across the network, a technician may use the concept of VLANs (Virtual Local Area Networks). VLANs are a way of dividing a single physical network into multiple logical networks, each with its own unique identifier or "tag."
By assigning each department a specific VLAN identifier, the technician can segment the network traffic and ensure that the different departments' traffic is kept

separate from one another. This can help to improve network security, performance, and scalability, as well as allowing for better monitoring and control of the network traffic.
To implement VLANs, the technician will need to configure VLAN tagging on the network devices, such as switches and routers, and assign each department's devices to the appropriate VLAN. The technician may also need to configure VLAN trunking to allow the different VLANs to communicate with each other.
By using VLANs, the technician can effectively monitor and segment the network traffic, providing better control and visibility into the network.

NEW QUESTION 284
- (Exam Topic 3)
A network administrator installed an additional IDF during a building expansion project. Which of the following documents need to be updated to reflect the change? (Select TWO).

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

Answer: BF

NEW QUESTION 285
- (Exam Topic 3)
An ISP is providing Internet to a retail store and has terminated its point of connection using a standard Cat 6 pin-out Which of me following terminations should the technician use when running a cable from the ISP's port lo the front desk?

A. F-type connector
B. TIA/E1A-56S-B
C. LC
D. SC

Answer: B

Explanation:
The termination that the technician should use when running a cable from the ISP’s port to the front desk is B. TIA/EIA-568-B. This is a standard pin-out for Cat 6 cables that is used for Ethernet and other network physical layers1. It specifies how to arrange the eight wires in an RJ45 connector, which is a common type of connector for network cables.

NEW QUESTION 286
- (Exam Topic 3)
A network administrator would like to purchase a device that provides access ports to endpoints and has the ability to route between networks. Which of the following would be BEST for the administrator to purchase?

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

Answer: B

NEW QUESTION 290
- (Exam Topic 3)
All packets arriving at an interface need to be fully analyzed. Which of me following features should be used to enable monitoring of the packets?

A. LACP
B. Flow control
C. Port mirroring
D. NetFlow exporter

Answer: C

Explanation:
Port mirroring is a feature that can be used to enable monitoring of all packets arriving at an interface. This feature is used to direct a copy of all traffic passing through the switch to a monitoring device, such as a network analyzer. This allows the switch to be monitored with the network analyzer in order to identify any malicious or suspicious activity. Additionally, port mirroring can be used to troubleshoot network issues, such as latency or poor performance.

NEW QUESTION 293
- (Exam Topic 3)
A network technician is implementing a solution that will allow end users to gain access to multiple applications after logging on. Which of the following authentication methods would allow this type of access?

A. SSO
B. LDAP
C. EAP
D. TACACS+

Answer: A

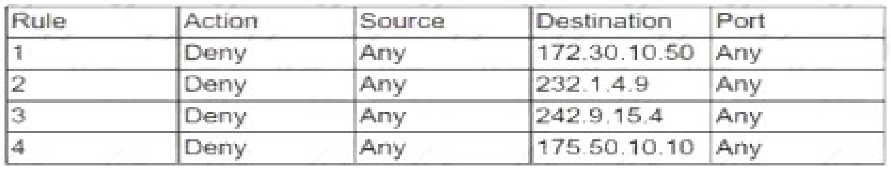
NEW QUESTION 294
- (Exam Topic 3)
A new global ISP needs to connect from central offices in North America to the United Kingdom. Which of the following would be the BEST cabling solution for this project?

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

Answer: A

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.

NEW QUESTION 298
- (Exam Topic 3)
An administrator is setting up a multicast server on a network, but the firewall seems to be dropping the traffic. After logging in to the device, me administrator sees me following entries:



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

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

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

Answer: A

NEW QUESTION 301
- (Exam Topic 3)
Which of the following allows for an devices within a network to share a highly reliable time source?

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

Answer: A

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

NEW QUESTION 302
- (Exam Topic 3)
A public, wireless ISP mounts its access points on top of traffic signal poles. Fiber-optic cables are installed from a fiber switch through the ground and up the pole to a fiber-copper media converter, and then connected to the AP. In one location, the switchport is showing sporadic link loss to the attached AP. A similar link loss is not seen at the AP interface. The fiber-optic cable is moved to another unused switchport with a similar result. Which of the following steps should the assigned technician complete NEXT?

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

Answer: B

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

NEW QUESTION 306
- (Exam Topic 3)
Users within a corporate network need to connect to the Internet, but corporate network policy does not allow direct connections. Which of the following is MOST likely to be used?

A. Proxy server

B. VPN client
C. Bridge
D. VLAN

Answer: A

NEW QUESTION 308
- (Exam Topic 3)
A technician needs to configure a routing protocol for an internet-facing edge router. Which of the following routing protocols will the technician MOST likely use?

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

Answer: A

NEW QUESTION 311
- (Exam Topic 3)
Which of the following describes the ability of a corporate IT department to expand its cloud-hosted VM environment with minimal effort?

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

Answer: A

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

NEW QUESTION 315
- (Exam Topic 3)
Which of the following protocols can be routed?

A. FCoE
B. Fibre Channel
C. iSCSI
D. NetBEUI

Answer: C

Explanation:
iSCSI (Internet Small Computer System Interface) is a protocol that allows SCSI commands to be transported over IP networks1. iSCSI can be routed because it contains a network address and a device address, as required by a routable protocol2. iSCSI can be used to access block-level storage devices over a network, such as SAN (Storage Area Network).
FCoE (Fibre Channel over Ethernet) is a protocol that allows Fibre Channel frames to be encapsulated and transported over Ethernet networks1. FCoE cannot be routed because it does not contain a network address, only a device address. FCoE operates at the data link layer and requires special switches and adapters to support it. FCoE can also be used to access block-level storage devices over a network, such as SAN.
Fibre Channel is a protocol that provides high-speed and low-latency communication between servers and storage devices1. Fibre Channel cannot be routed because it does not use IP networks, but rather its own dedicated network infrastructure. Fibre Channel operates at the physical layer and the data link layer and requires special cables, switches, and adapters to support it. Fibre Channel can also be used to access block-level storage devices over a network, such as SAN.
NetBEUI (NetBIOS Extended User Interface) is an old protocol that provides session-level communication between devices on a local network1. NetBEUI cannot be routed because it does not contain a network address, only a device address. NetBEUI operates at the transport layer and relies on NetBIOS for name resolution. NetBEUI is obsolete and has been replaced by other protocols, such as TCP/IP.

NEW QUESTION 317
- (Exam Topic 3)
A security administrator is trying to prevent incorrect IP addresses from being assigned to clients on the network. Which of the following would MOST likely prevent this and allow the network to continue to operate?

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

Answer: A

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

NEW QUESTION 319

- (Exam Topic 3)
A technician discovered that some information on the local database server was changed during a tile transfer to a remote server. Which of the following should concern the technician the MOST?

A. Confidentiality
B. Integrity
C. DDoS
D. On-path attack

Answer: B

Explanation:
The technician should be most concerned about data integrity and security. If information on the local database server was changed during a file transfer to a remote server, it could indicate that unauthorized access or modifications were made to the data. It could also indicate a failure in the file transfer process, which could result in data loss or corruption. The technician should investigate the cause of the changes and take steps to prevent it from happening again in the future. Additionally, they should verify the integrity of the data and restore it from a backup if necessary to ensure that the correct and complete data is available. The technician should also take appropriate actions such as notifying the system administrator and management of the incident, and following the incident management process to minimize the damage caused by the incident.

NEW QUESTION 324
- (Exam Topic 3)
A network administrator is configuring logging on an edge switch. The requirements are to log each time a switch port goes up or down. Which of the following logging levels will provide this information?

A. Warnings
B. Notifications
C. Alert
D. Errors

Answer: B

Explanation:
Notifications are the lowest logging level and will provide the desired information regarding switch port up/down activity. According to the CompTIA Network+ Study Manual, notifications "are used for logging
normal activities, such as port up/down events, link changes, and link flaps."

NEW QUESTION 326
- (Exam Topic 3)
An IT technician needs to increase bandwidth to a server. The server has multiple gigabit ports. Which of the following can be used to accomplish this without replacing hardware?

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

Answer: D

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

NEW QUESTION 327
- (Exam Topic 3)
A network technician needs to select an AP that will support at least 1.3Gbps and 5GHz only. Which of the following wireless standards must the AP support to meet the requirements?

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

Answer: B

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

NEW QUESTION 330
- (Exam Topic 3)
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

Answer: A

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. References: https://www.comptia.org/training/books/network-n10-008-study-guide (page 414)

NEW QUESTION 334
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 335
- (Exam Topic 3)
A technician is trying to determine whether an LACP bundle is fully operational. Which of the following commands will the technician MOST likely use?

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

Answer: A

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

NEW QUESTION 337
- (Exam Topic 3)
A company wants to add a local redundant data center to its network in case of failure at its primary location. Which of the following would give the LEAST amount of redundancy for the company's network?

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

Answer: A

NEW QUESTION 342
- (Exam Topic 3)
ARP spoofing would normally be a part of:

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

Answer: A

NEW QUESTION 344
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 347
- (Exam Topic 3)
An IT technician successfully connects to the corporate wireless network at a hank. While performing some tests, the technician observes that the physical address of the DHCp server has changed even though the network connection has not been lost. Which of the following would BEST explain this change?

A. Server upgrade
B. Duplicate IP address
C. Scope exhaustion
D. Rogue server

Answer: D

Explanation:
A rogue server is a DHCP server on a network that is not under the administrative control of the network staff 1. It may provide incorrect IP addresses or other network configuration information to devices on the network, causing them to lose connectivity or be vulnerable to attacks2. The physical address of the DHCP server may change if a rogue server takes over the role of assigning IP addresses to devices on the network. This can be detected by monitoring DHCP traffic or using tools such as RogueChecker2.

NEW QUESTION 350
- (Exam Topic 3)
Which of the following is an advanced distance vector routing protocol that automates routing tables and also uses some features of link-state routing protocols?

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

Answer: C

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

NEW QUESTION 353
- (Exam Topic 3)
A network technician is attempting to increase throughput by configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch. Which of the following is the BEST choice concerning speed and duplex for all interfaces that are participating in the link aggregation?

A. Half duplex and 1GB speed
B. Full duplex and 1GB speed
C. Half duplex and 10OMB speed
D. Full duplex and 100MB speed

Answer: B

Explanation:
The best choice for configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch is to use full duplex and 1GB speed for all interfaces that are participating in the link aggregation. This will allow for maximum throughput, as the full duplex connection will enable simultaneous sending and receiving of data, and the 1GB speed will ensure that the data is transferred quickly.
According to the CompTIA Network+ Study Guide, “Full-duplex Ethernet allows the network adapter to transmit and receive data simultaneously, which can result in double the bandwidth of half-duplex Ethernet.” Additionally, the official text states, “Ethernet and Fast Ethernet use different speeds for data transmission, with Ethernet being 1,000 megabits (1 gigabit) per second and Fast Ethernet being 100 megabits per second.”

NEW QUESTION 355
......