Exam Questions N10-009

CompTIA Network+ Exam

https://www.2passeasy.com/dumps/N10-009/

NEW QUESTION 1
- (Exam Topic 1)
An IT director is setting up new disaster and HA policies for a company. Limited downtime is critical to operations. To meet corporate requirements, the director set up two different datacenters across the country that will stay current on data and applications. In the event of an outage, the company can immediately switch from one datacenter to another. Which of the following does this BEST describe?

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

Answer: E

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

NEW QUESTION 2
- (Exam Topic 1)
A technician wants to deploy a new wireless network that comprises 30 WAPs installed throughout a three-story office building. All the APs will broadcast the same SSID for client access. Which of the following BEST describes this deployment?

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

Answer: A

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

NEW QUESTION 3
- (Exam Topic 1)
A workstation is configured with the following network details:

IP address	Subnet mask	Default gateway
10.1.2.23	10.1.2.0/27	10.1.2.1

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

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

Answer: D

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

NEW QUESTION 4
- (Exam Topic 1)
A store owner would like to have secure wireless access available for both business equipment and patron use. Which of the following features should be configured to allow different wireless access through the same equipment?

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

Answer: D

Explanation:

SSID (Service Set Identifier) is a feature that should be configured to allow different wireless access through the same equipment. SSID is the name of a wireless network that identifies it from other networks in the same area. A wireless access point (AP) can support multiple SSIDs with different security settings and network policies. For example, a store owner can create one SSID for business equipment and another SSID for patron use, and assign different passwords, VLANs, and QoS levels for each SSID. References: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70931-multiple-ssid.html

NEW QUESTION 5
- (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 6
- (Exam Topic 1)
After the A record of a public website was updated, some visitors were unable to access the website. Which of the following should be adjusted to address the issue?

A. TTL
B. MX
C. TXT
D. SOA

Answer: A

Explanation:
TTL (Time To Live) should be adjusted to address the issue of some visitors being unable to access the website after the A record was updated. TTL is a value that specifies how long a DNS record should be cached by DNS servers and clients before it expires and needs to be refreshed. If the TTL is too high, some DNS servers and clients may still use the old A record that points to the previous IP address of the website, resulting in connection failures. By lowering the TTL, the DNS servers and clients will update their cache more frequently and use the new A record that points to the current IP address of the website. References: https://www.cloudflare.com/learning/dns/dns-records/dns-ttl/

NEW QUESTION 7
- (Exam Topic 1)
A technician is deploying a new switch model and would like to add it to the existing network monitoring software. The technician wants to know what metrics can be gathered from a given switch. Which of the following should the technician utilize for the switch?

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

Answer: A

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

NEW QUESTION 8
- (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 9
- (Exam Topic 1)
The network administrator is informed that a user's email password is frequently hacked by brute-force programs. Which of the following policies should the network administrator implements to BEST mitigate this issue? (Choose two.)

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

Answer: BC

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

NEW QUESTION 10
- (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 10
- (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 13
- (Exam Topic 1)
Which of the following provides redundancy on a file server to ensure the server is still connected to a LAN even in the event of a port failure on a switch?

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

Answer: A

Explanation:
NIC teaming, also known as network interface card teaming or link aggregation, allows multiple network interface cards to be grouped together to provide redundancy and increased throughput. In the event of a port failure on a switch, NIC teaming ensures that the file server remains connected to the LAN by automatically switching to another network interface card.
References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 16

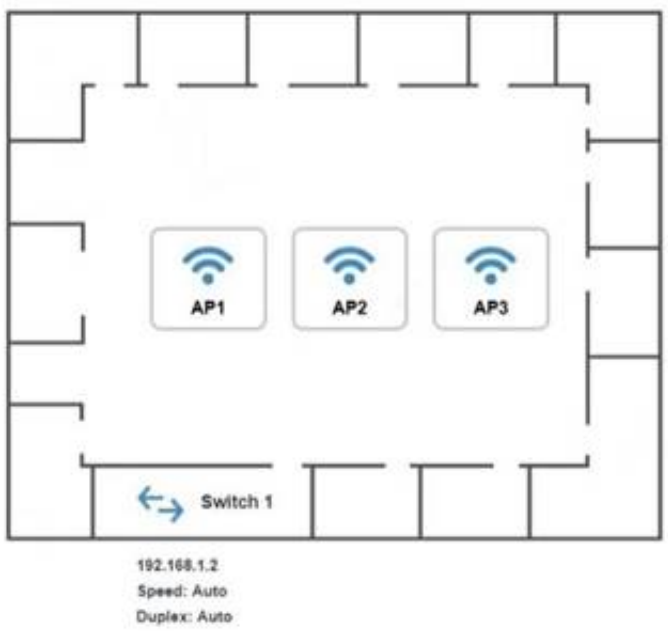
- (Exam Topic 1)
A website administrator is concerned the company's static website could be defaced by hacktivists or used as a pivot point to attack internal systems. Which of the following should a network security administrator recommend to assist with detecting these activities?

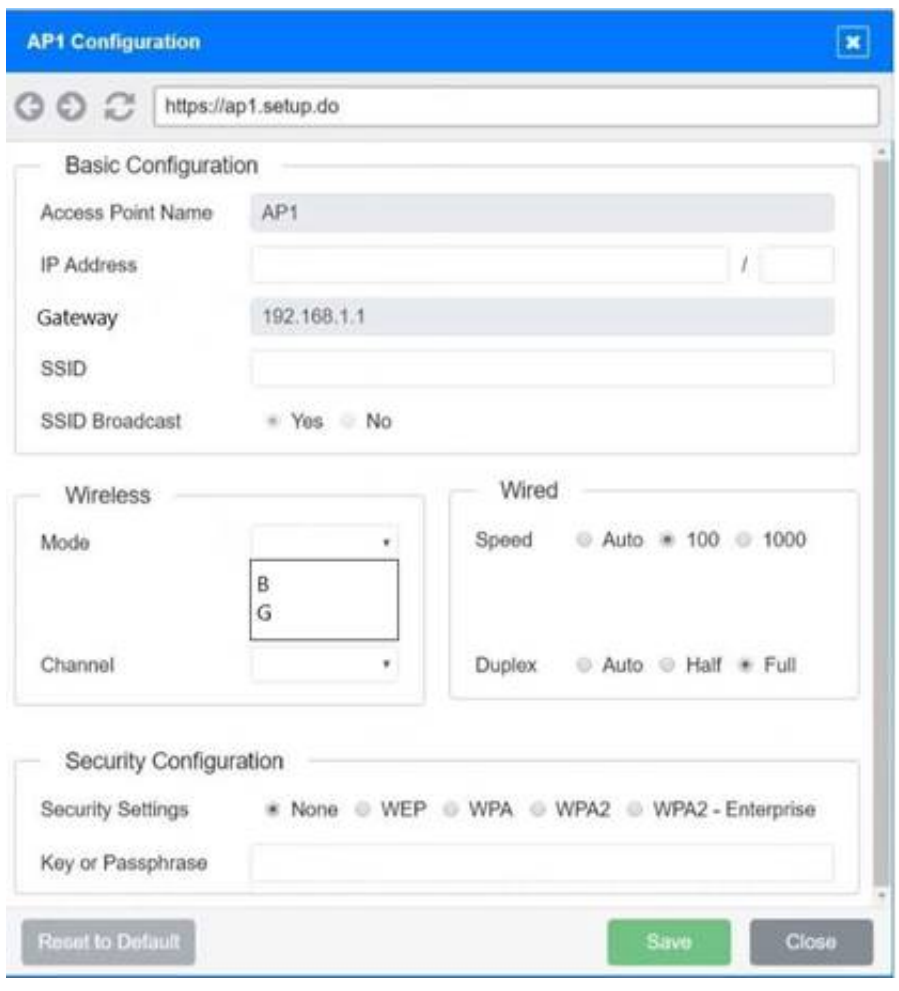
A. Implement file integrity monitoring.
B. Change the default credentials.
C. Use SSL encryption.
D. Update the web-server software.

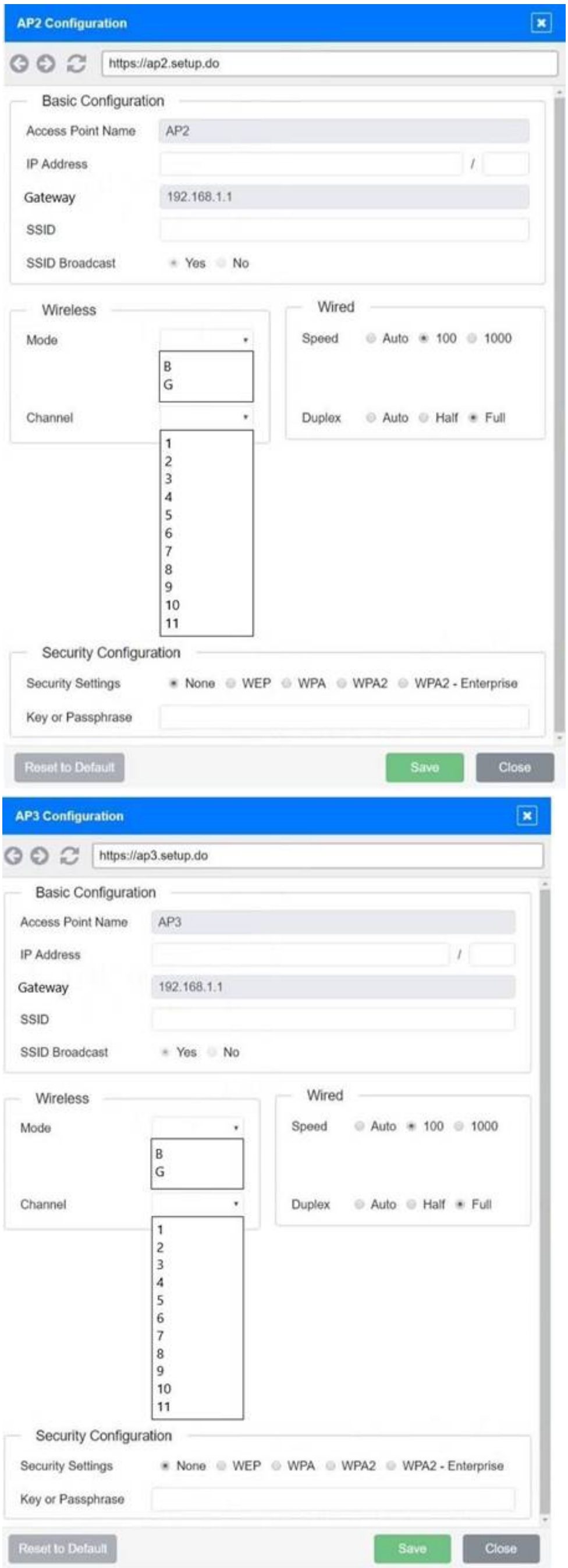
Answer: A

Explanation:
Implementing file integrity monitoring (FIM) would assist with detecting activities such as website defacement or internal system attacks. FIM is a process that monitors and alerts on changes to files or directories that are critical for security or functionality. FIM can help detect unauthorized modifications, malware infections, data breaches, or configuration errors. FIM can also help with compliance and auditing requirements. References: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/what-is-file-integrity-monitor

NEW QUESTION 18
- (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.



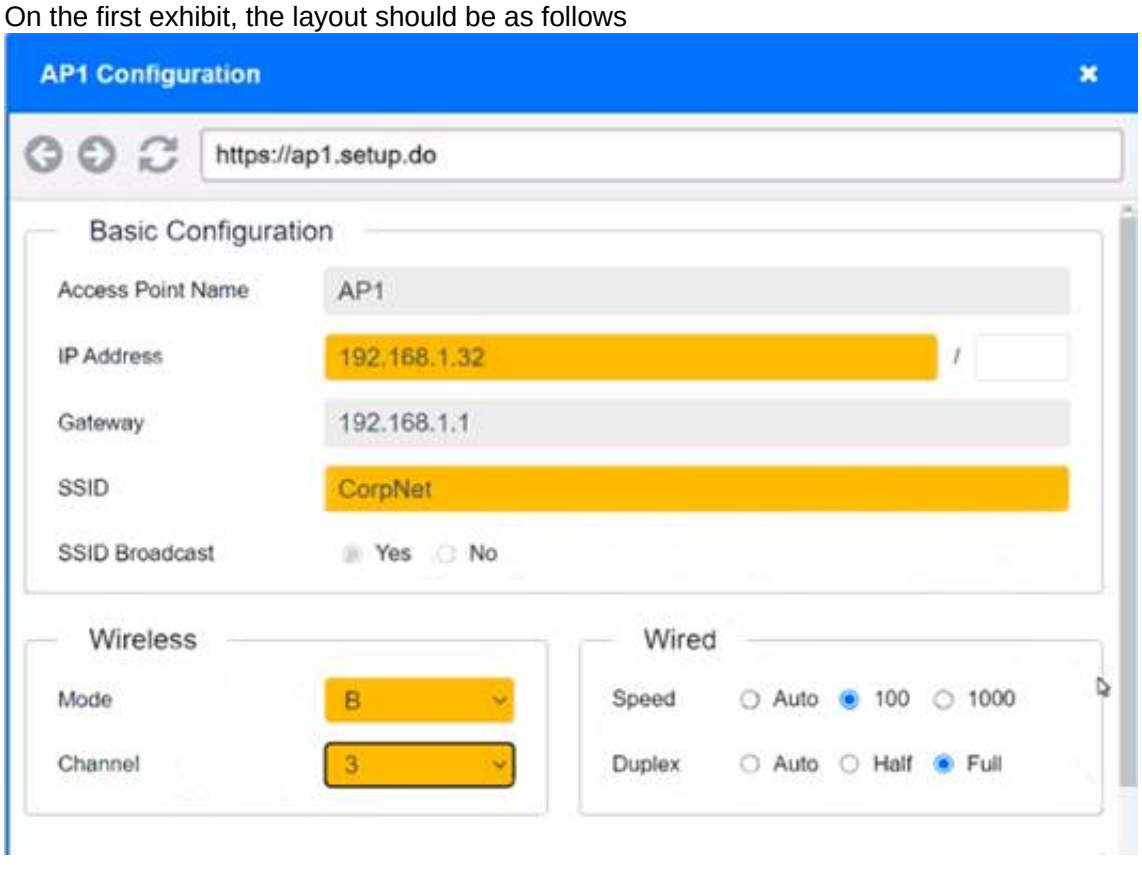




A. Mastered
B. Not Mastered

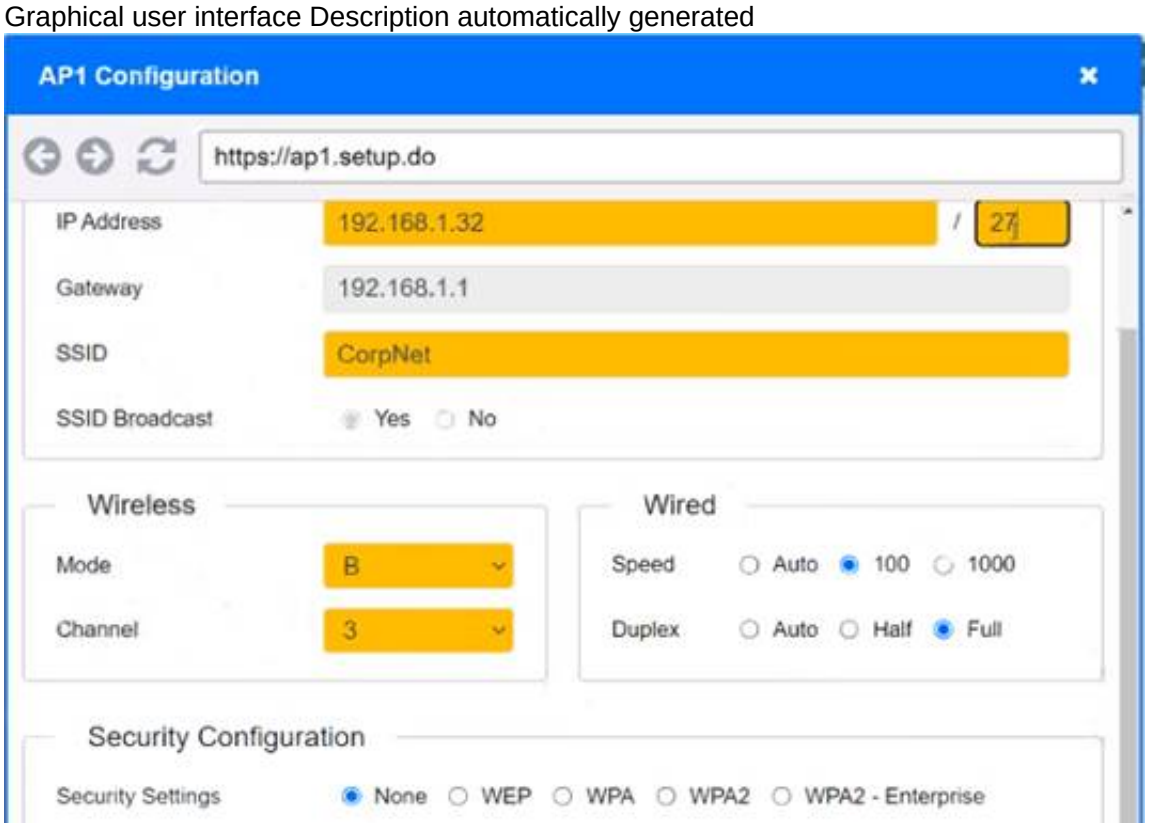
Answer: A

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



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

Graphical user interface Description automatically generated



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

Graphical user interface Description automatically generated

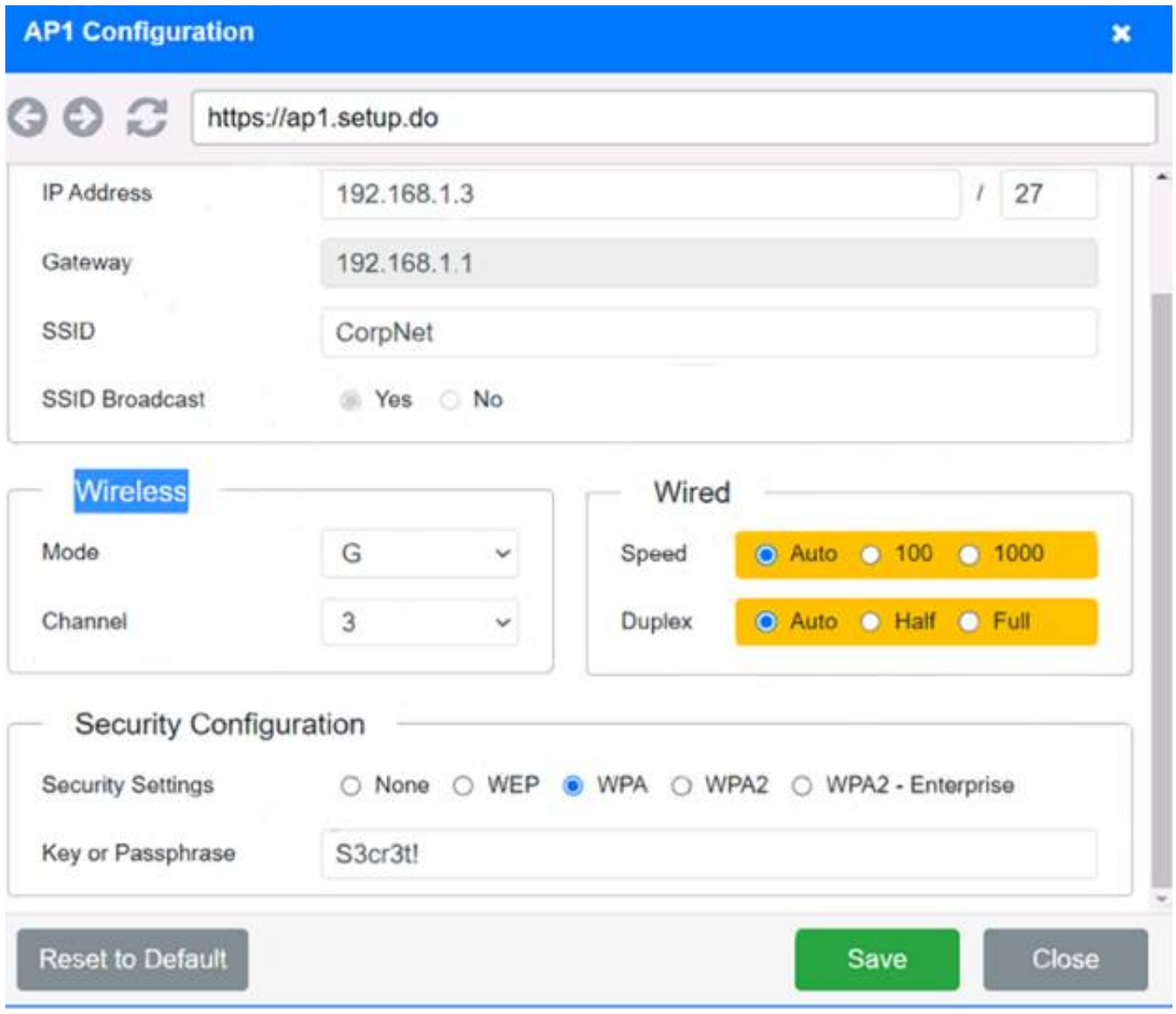
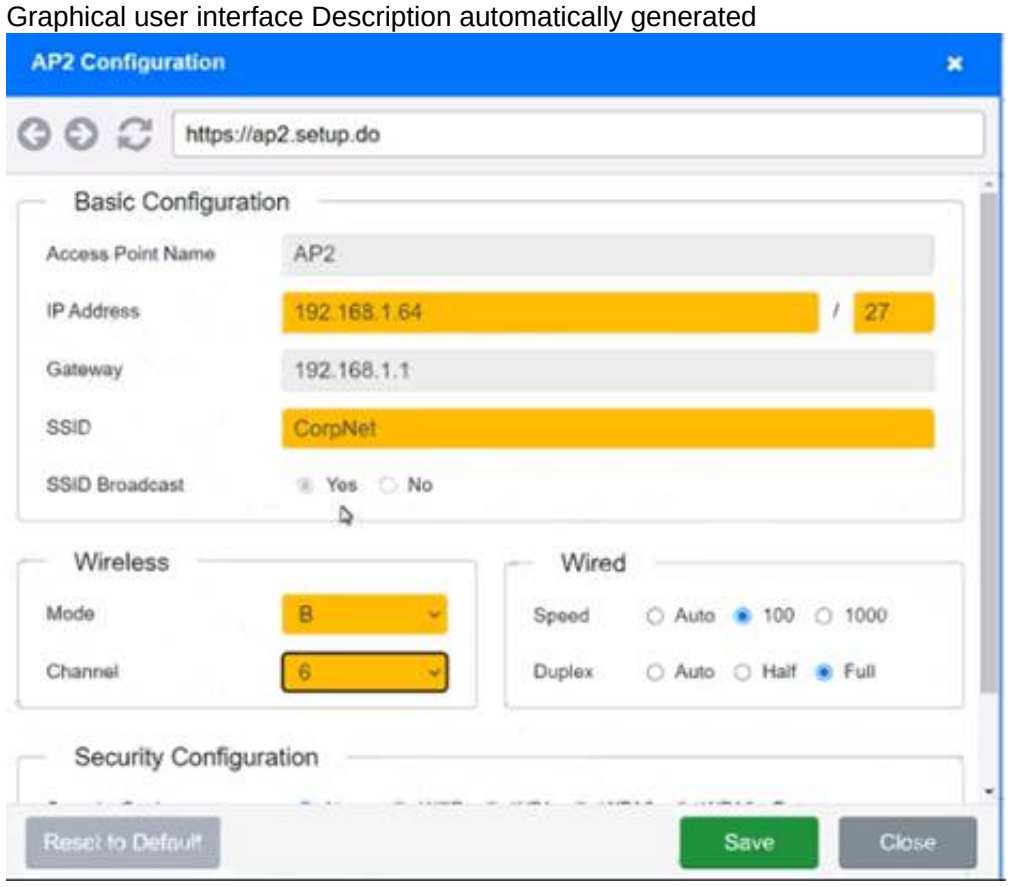


Exhibit 2 as follows Access Point Name AP2
Graphical user interface Description automatically generated



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

Graphical user interface Description automatically generated

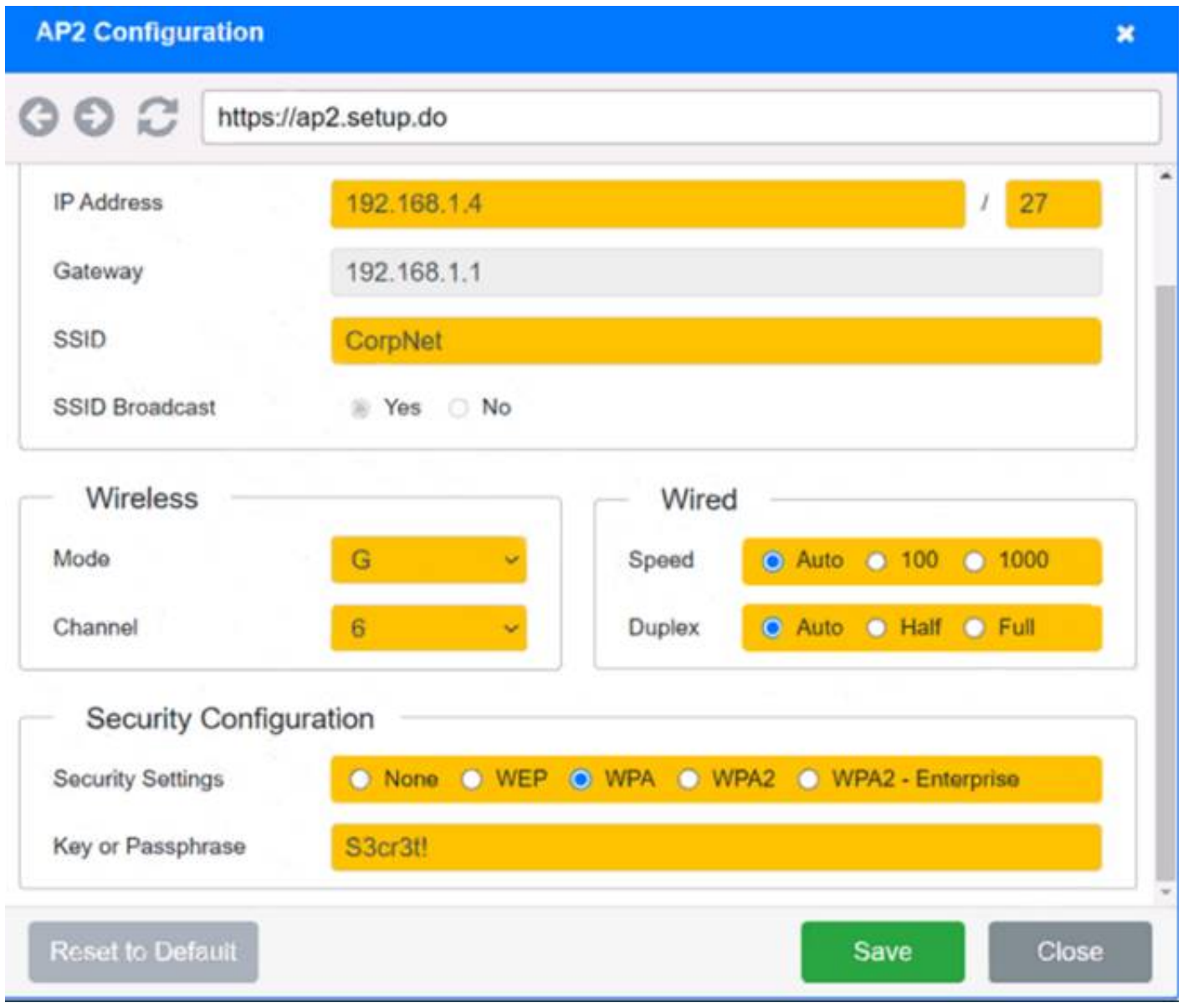
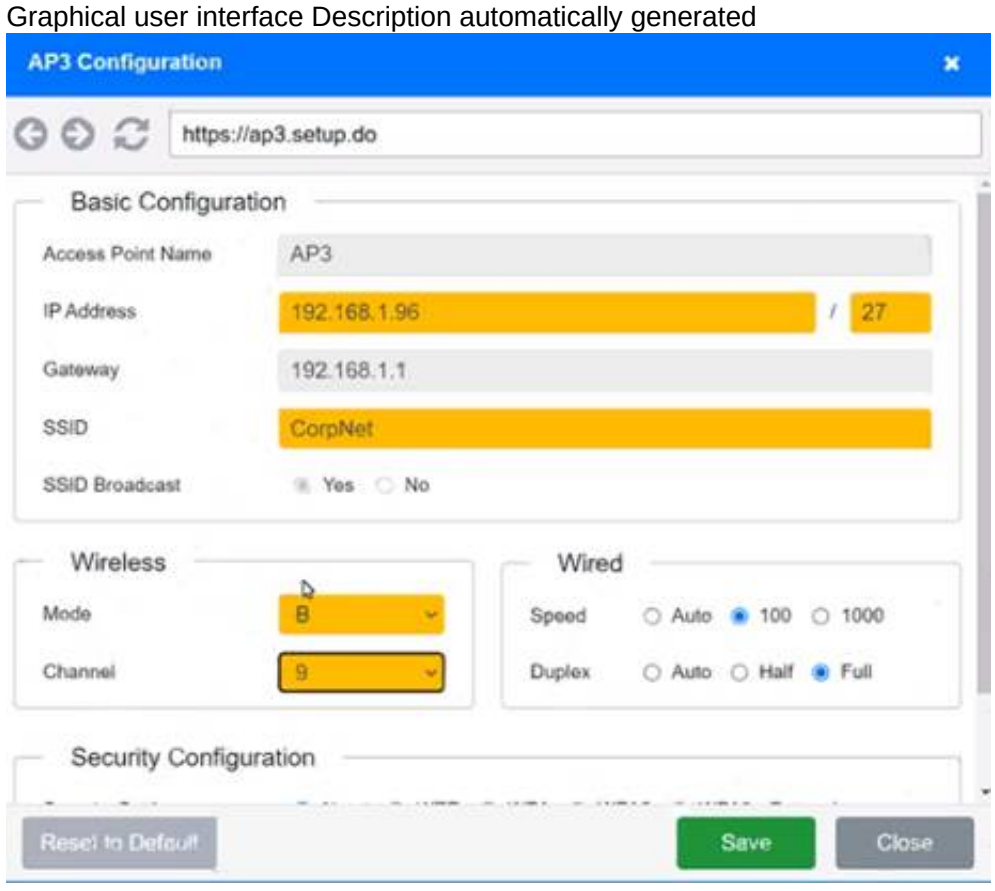
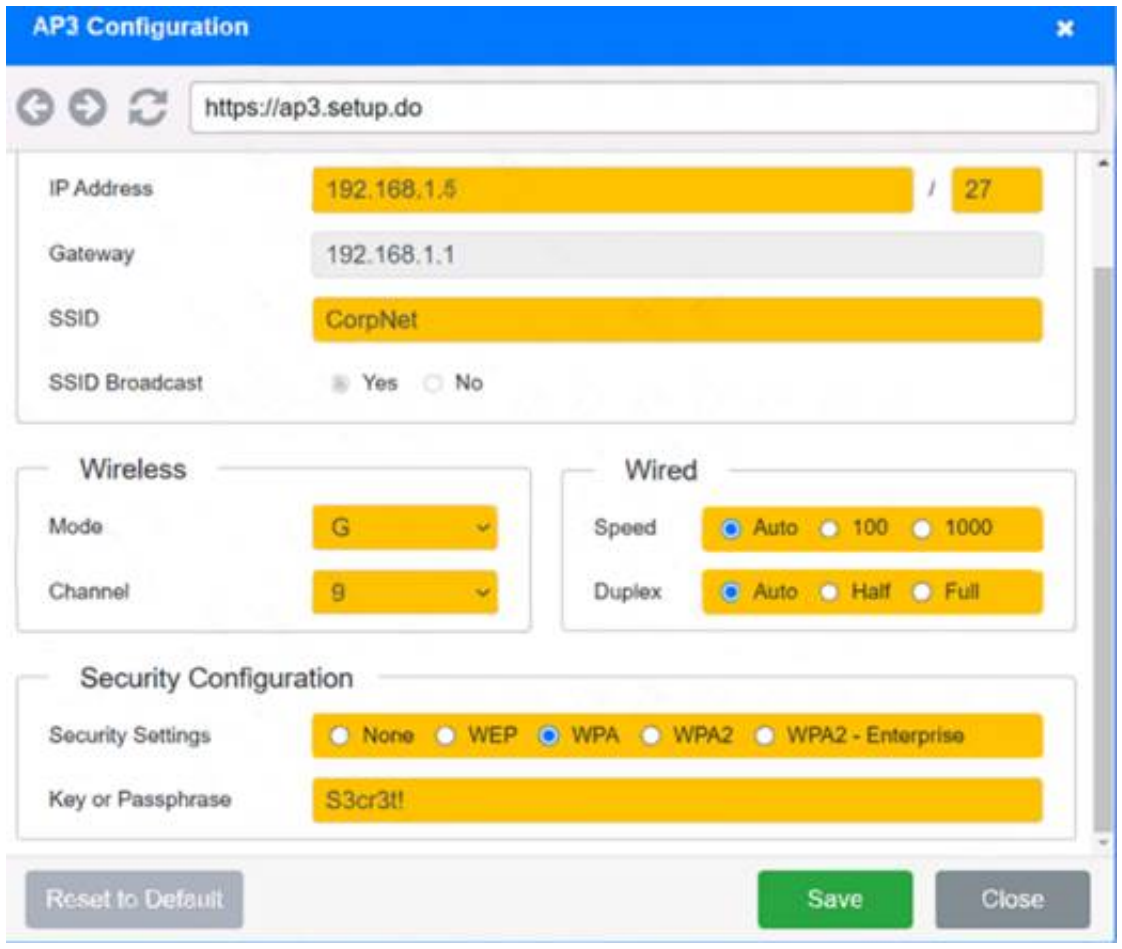


Exhibit 3 as follows Access Point Name AP3
Graphical user interface Description automatically generated



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

Graphical user interface Description automatically generated



NEW QUESTION 19
- (Exam Topic 1)
A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

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

Answer: A

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

NEW QUESTION 21
- (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 24
- (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 29
- (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 30
- (Exam Topic 2)
A technician is troubleshooting a previously encountered issue. Which of the following should the technician reference to find what solution was implemented to resolve the issue?

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

Answer: D

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

NEW QUESTION 35
- (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 37
- (Exam Topic 2)
A network administrator is downloading a large patch that will be uploaded to several enterprise switches simultaneously during the day's upgrade cycle. Which of the following should the administrator do to help ensure the upgrade process will be less likely to cause problems with the switches?

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

Answer: A

Explanation:
The network administrator should confirm the patch’s MD5 hash prior to the upgrade to help ensure the upgrade process will be less likely to cause problems with the switches. MD5 (Message Digest 5) is a cryptographic hash function that produces a 128-bit hash value for any given input. It can be used to verify the integrity and authenticity of a file by comparing its hash value with a known or expected value. If the hash values match, it means that the file has not been corrupted or tampered with during transmission or storage. If the hash values do not match, it means that the file may be damaged or malicious and should not be used for the upgrade. References:
https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/15292-scp.html

NEW QUESTION 41
- (Exam Topic 2)
There are two managed legacy switches running that cannot be replaced or upgraded. These switches do not support cryptographic functions, but they are password protected. Which of the following should a network administrator configure to BEST prevent unauthorized access?

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

Answer: E

Explanation:
Using an out-of-band access method is the best way to prevent unauthorized access to the legacy switches that do not support cryptographic functions. Out-of-band access is a method of accessing a network device through a dedicated channel that is separate from the main network traffic. Out-of-band access can use physical connections such as serial console ports or dial-up modems, or logical connections such as VPNs or firewalls. Out-of-band access provides more security and reliability than in-band access, which uses the same network as the data traffic and may be vulnerable to attacks or failures. References:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15mt/fundamentals-15-mt-book/

NEW QUESTION 42
- (Exam Topic 2)
A wireless network was installed in a warehouse for employees to scan crates with a wireless handheld scanner. The wireless network was placed in the corner of the building near the ceiling for maximum coverage However users in the offices adjacent lo the warehouse have noticed a large amount of signal overlap from the new network Additionally warehouse employees report difficulty connecting to the wireless network from the other side of the building; however they have no issues when Ihey are near the antenna Which of the following is MOST likely the cause?

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

Answer: C

Explanation:
An omnidirectional antenna was used instead of a unidirectional antenna, which is most likely the cause of the wireless network issues. An omnidirectional antenna provides wireless coverage in all directions from the antenna, which can cause signal overlap with adjacent offices and interference with other wireless networks. A unidirectional antenna, on the other hand, provides wireless coverage in a specific direction from the antenna, which can reduce signal overlap and interference and increase signal range and quality. A unidirectional antenna would be more suitable for a warehouse environment where users are located on one side of the building1. References:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html 1

NEW QUESTION 43
- (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 47
- (Exam Topic 2)
An ARP request is broadcasted and sends the following request. "Who is 192.168.1.200?
Tell 192.168.1.55"
At which of the following layers of the OSI model does this request operate?

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

Answer: B

Explanation:
An ARP request operates at the data link layer of the OSI model. ARP (Address Resolution Protocol) is a protocol that maps IP addresses to MAC addresses on a local area network. It allows devices to communicate with each other without knowing their MAC addresses beforehand. ARP operates at the data link layer (layer

2) of the OSI model, which is responsible for framing and addressing data packets on a physical medium.
References: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

NEW QUESTION 49
- (Exam Topic 2)
A technician is troubleshooting a workstation's network connectivity and wants to confirm which switchport corresponds to the wall jack the PC is using Which of the following concepts would BEST help the technician?

A. Consistent labeling
B. Change management
C. Standard work instructions
D. Inventory management
E. Network baseline

Answer: A

Explanation:
Consistent labeling would be the concept that would best help the technician to confirm which switchport corresponds to the wall jack the PC is using. Consistent labeling is a practice of using standardized and descriptive labels for network devices, ports, cables, jacks, and other components. It can help with identifying, locating, and troubleshooting network issues. For example, a technician can use consistent labeling to trace a cable from a PC to a wall jack, and then from a patch panel to a switchport. References: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_6.html

NEW QUESTION 50
- (Exam Topic 2)
An IDS was installed behind the edge firewall after a network was breached. The network was then breached again even though the IDS logged the attack. Which of the following should be used in place of these devices to prevent future attacks?

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

Answer: C

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

NEW QUESTION 54
- (Exam Topic 2)
A network administrator is required to ensure that auditors have read-only access to the system logs, while systems administrators have read and write access to the system logs, and operators have no access to the system logs. The network administrator has configured security groups for each of these functional categories. Which of the following security capabilities will allow the network administrator to maintain these permissions with the LEAST administrative effort?

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

Answer: C

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

NEW QUESTION 55
- (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 57
- (Exam Topic 2)
A network requirement calls for segmenting departments into different networks. The campus network is set up with users of each department in multiple buildings. Which of the following should be configured to keep the design simple and efficient?

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

Answer: C

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

NEW QUESTION 59
- (Exam Topic 2)
A client moving into a new office wants the IP network set up to accommodate 412 network-connected devices that are all on the same subnet. The subnet needs to be as small as possible. Which of the following subnet masks should be used to achieve the required result?

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

Answer: B

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

NEW QUESTION 64
- (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 67
- (Exam Topic 2)
A network administrator is setting up several loT 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 loT device to accomplish the requirements of reducing manual configuration, assigning a specific IP address, and allowing devices to move to different switchports on the same VLAN. References: https://www.comptia.org/blog/what-is-dhcp

NEW QUESTION 72
- (Exam Topic 3)

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

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

Answer: A

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

NEW QUESTION 75
- (Exam Topic 3)
A network device needs to discover a server that can provide it with an IPv4 address. Which of the following does the device need to send the request to?

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

Answer: B

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

NEW QUESTION 77
- (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 81
- (Exam Topic 3)
Several employees have expressed concerns about the company monitoring their internet activity when they are working from home. The company wants to mitigate this issue and reassure employees that their private internet activity is not being monitored. Which of the following would satisfy company and employee needs?

A. Split tunnel
B. Full tunnel
C. Site-to-site tunnel
D. Virtual desktop

Answer: A

Explanation:
Split tunnel is a configuration that allows a remote user to access both the local network and the Internet at the same time. In a split tunnel configuration, only traffic destined for the corporate network is sent through the VPN tunnel, while all other traffic is sent directly to the Internet. This allows the remote user to access the Internet without the company's VPN server being able to monitor or intercept their traffic. Using a split tunnel configuration can help the company to mitigate employee concerns about internet activity being monitored and reassure employees that their private internet activity is not being monitored.

NEW QUESTION 86
- (Exam Topic 3)
During a recent security audit, a contracted penetration tester discovered the organization uses a number of insecure protocols. Which of the following ports should be disallowed so only encrypted protocols are allowed? (Select TWO).

A. 22
B. 23
C. 69
D. 443
E. 587
F. 8080

Answer: BC

NEW QUESTION 87
- (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 88
- (Exam Topic 3)
A security vendor needs to add a note to the DNS to validate the ownership of a company domain before services begin. Which of the following records did the security company MOST likely ask the company to configure?

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

Answer: A

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

NEW QUESTION 93
- (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 96
- (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 97
- (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 98
- (Exam Topic 3)
A user from a remote office is reporting slow file transfers. Which of the following tools will an engineer MOST likely use to get detailed measurement data?

A. Packet capture
B. IPerf
C. SIEM log review
D. Internet speed test

Answer: B

Explanation:
An engineer will most likely use IPerf to get detailed measurement data about the user's slow file transfers. IPerf is a tool used for measuring network performance and bandwidth, and it can be used to measure the speed and throughput of file transfers from the remote office. It can also provide detailed information about the latency and jitter of the connection, which can be used to troubleshoot the slow file transfers. Reference: CompTIA Network+ Study Manual (Chapter 10, Page 214).

NEW QUESTION 103
- (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 105
- (Exam Topic 3)
Switch 3 was recently added lo an existing stack to extend connectivity to various parts of the network. After the update, new employees were not able to print to the main networked copiers from then workstations. Following are the port configurations for the switch stack in question:

Switch 1:

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

Switch 2:

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

Switch 3:

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

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

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

Answer: AE

NEW QUESTION 107
- (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 110
- (Exam Topic 3)
A technician knows the MAC address of a device and is attempting to find the device's IP address. Which of the following should the technician look at to find the IP address? (Select TWO).

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

Answer: BE

NEW QUESTION 115
- (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 118
- (Exam Topic 3)
A user calls the IT department to report being unable to log in after locking the computer The user resets the password, but later in the day the user is again unable to log in after locking the computer Which of the following attacks against the user IS MOST likely taking place?

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

Answer: A

NEW QUESTION 122
- (Exam Topic 3)
A Network engineer is investigating issues on a Layer 2 Switch. The department typically snares a Switchport during meetings for presentations, but atter the first user Shares, no Other users can connect. Which Of the following is MOST likely related to this issue?

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

Answer: C

NEW QUESTION 127
- (Exam Topic 3)
A systems administrator wants to use the least amount of equipment to segment two departments that nave cables terminating in the same room. Which of the following would allow this to occur?

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

Answer: C

NEW QUESTION 130
- (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 133
- (Exam Topic 3)
A network technician recently installed 35 additional workstations. After installation, some users are unable to access network resources. Many of the original workstations that are experiencing the network access issue were offline when the new workstations were turned on. Which of the following is the MOST likely cause of this issue?

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

Answer: B

NEW QUESTION 136
- (Exam Topic 3)
Which of the following layers of the OSI model receives data from the application layer and converts it into syntax that is readable by other devices on the network?

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

Answer: C

NEW QUESTION 138
- (Exam Topic 3)
A network technician is working at a new office location and needs to connect one laptop to another to transfer files. The laptops are newer models and do not have Ethernet ports. Access points are not available either. Which Of the following types Of wireless network SSIDs does the network technician need to configure to be able to connect the laptops together?

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

Answer: A

Explanation:
An Independent Basic Service Set (IBSS) is a type of wireless network that does not require an access point or a wired network. An IBSS allows wireless devices to communicate directly with each other using ad hoc mode. An IBSS is also known as an ad hoc network or a peer-to-peer network. A network technician can configure an IBSS to connect two laptops together and transfer files.
References: Network+ Study Guide Objective 1.4: Explain the properties and characteristics of TCP/IP

NEW QUESTION 139
- (Exam Topic 3)
An international company is transferring its IT assets including a number of WAPs from the United States to an office in Europe for deployment. Which of the following considerations should the company research
before Implementing the wireless hardware?

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

Answer: B

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

NEW QUESTION 140
- (Exam Topic 3)

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

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

Answer: A

Explanation:
Client roaming refers to the ability of a wireless device to seamlessly connect to a different access point (AP) as the user moves around the facility. This can help to improve network stability and reduce interruptions in mobile applications. An extended service deployment is a type of wireless network configuration that uses multiple APs to cover a large area, such as a warehouse facility. By using a wireless controller to manage the APs, the network can be better optimized for client roaming, which can improve network stability.
"Roaming With multiple WAPs in an ESS, clients will connect to whichever WAP has the strongest signal. As clients move through the space covered by the broadcast area, they will change WAP connections seamlessly, a process called roaming."

NEW QUESTION 142
- (Exam Topic 3)
An engineer needs to restrict the database servers that are in the same subnet from communicating with each other. The database servers will still need to communicate with the application servers in a different subnet. In some cases, the database servers will be clustered, and the servers will need to communicate with other cluster members. Which of the following technologies will be BEST to use to implement this filtering without creating rules?

A. Private VLANs
B. Access control lists
C. Firewalls
D. Control plane policing

Answer: A

Explanation:
"Use private VLANs: Also known as port isolation, creating a private VLAN is a method of restricting switch ports (now called private ports) so that they can communicate only with a particular uplink. The private VLAN usually has numerous private ports and only one uplink, which is usually connected to a router, or firewall."

NEW QUESTION 147
- (Exam Topic 3)
A company's web server is hosted at a local ISP. This is an example of:

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

Answer: D

NEW QUESTION 151
- (Exam Topic 3)
Which of the following is most likely to have the HIGHEST latency while being the most accessible?

A. Satellite
B. DSL
C. Cable
D. 4G

Answer: A

NEW QUESTION 153
- (Exam Topic 3)
A technician is installing the Wi-Fi infrastructure for legacy industrial machinery at a warehouse. The equipment only supports 802.11a and 802.11b standards. Speed of transmission is the top business requirement. Which of the following is the correct maximum speed for this scenario?

A. 11Mbps
B. 54Mbps
C. 128Mbps
D. 144Mbps

Answer: B

Explanation:
802.11b (Wi-Fi 1)
11 Mbps
100 meter maximum effective range 802.11a (Wi-Fi 2)
54 Mbps
50 meter maximum effective range

NEW QUESTION 155
- (Exam Topic 3)
A technician was cleaning a storage closet and found a box of transceivers labeled 8Gbps. Which of the following protocols uses those transceivers?

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

Answer: C

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

NEW QUESTION 158
- (Exam Topic 3)
A switch is connected to another switch. Incompatible hardware causes a surge in traffic on both switches. Which of the following configurations will cause traffic to pause, allowing the switches to drain buffers?

A. Speed
B. Flow control
C. 802.1Q
D. Duplex

Answer: B

Explanation:
Flow control is a mechanism that allows a network device to regulate the amount of traffic it can receive or send. Flow control can help prevent congestion and buffer overflow by sending pause frames or signals to the sender when the receiver's buffer is full or nearly full. Flow control can cause traffic to pause, allowing the switches to drain buffers and resume normal operation. Speed is a parameter that determines the data transfer rate of a network link. 802.1Q is a standard for VLAN (Virtual Local Area Network) tagging, which allows multiple logical networks to share the same physical infrastructure. Duplex is a mode of communication that determines how data is transmitted and received on a link. Full duplex allows simultaneous transmission and reception, while half duplex allows only one direction at a time.
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 163
- (Exam Topic 3)
After rebooting an AP a user is no longer able to conned to me enterprise LAN A technician plugs a laptop In to the same network jack and receives the IP 169.254 0 200. Which of the following is MOST likely causing the issue?

A. DHCP scope exhaustion
B. Signal attenuation
C. Channel overlap
D. Improper DNS configuration

Answer: A

Explanation:
DHCP scope exhaustion occurs when the number of available IP addresses to be leased from a DHCP server have been used up. This could be caused by a large number of clients on the network, or a misconfigured DHCP scope. When this happens, clients will be assigned an IP address from the APIPA range (169.254.0.0 to 169.254.255.255). To resolve this issue, the DHCP scope needs to be expanded or adjusted to accommodate the number of clients on the network.

NEW QUESTION 166
- (Exam Topic 3)
A Wi-Fi network was recently deployed in a new, multilevel budding. Several issues are now being reported related to latency and drops in coverage. Which of the following is the FIRST step to troubleshoot the issues?

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

Answer: A

NEW QUESTION 168
- (Exam Topic 3)
An auditor assessing network best practices was able to connect a rogue switch into a network Jack and get network connectivity. Which of the following controls would BEST address this risk?

A. Activate port security on the switchports providing end user access.
B. Deactivate Spanning Tree Protocol on network interfaces that are facing public areas.
C. Disable Neighbor Resolution Protocol in the Layer 2 devices.

D. Ensure port tagging is in place for network interfaces in guest areas

Answer: A

NEW QUESTION 171
- (Exam Topic 3)
Which of the following options represents the participating computers in a network?

A. Nodes
B. CPUs
C. Servers
D. Clients

Answer: A

NEW QUESTION 173
- (Exam Topic 3)
A newly installed VoIP phone is not getting the DHCP IP address it needs to connect to the phone system. Which of the following tasks needs to be completed to allow the phone to operate correctly?

A. Assign the phone's switchport to the correct VLAN
B. Statically assign the phone's gateway address.
C. Configure a route on the VoIP network router.
D. Implement a VoIP gateway

Answer: A

NEW QUESTION 177
- (Exam Topic 3)
Which of the following is the NEXT step to perform network troubleshooting after identifying an issue?

A. Implement a solution.
B. Establish a theory.
C. Escalate the issue.
D. Document the findings.

Answer: B

Explanation:
1 Identify the Problem. 2 Develop a Theory.
3 Test the Theory. 4 Plan of Action.
5 Implement the Solution.
6 Verify System Functionality. 7 Document the Issue.

NEW QUESTION 178
- (Exam Topic 3)
A network administrator received a report staling a critical vulnerability was detected on an application that is exposed to the internet. Which of the following Is the appropriate NEXT step?

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

Answer: A

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

NEW QUESTION 181
- (Exam Topic 3)
Two users on a LAN establish a video call. Which of the following OSI model layers ensures the initiation coordination, and termination of the call?

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

Answer: A

Explanation:
The OSI model layer that ensures the initiation, coordination, and termination of a video call is the session layer. The session layer is responsible for establishing,

maintaining, and terminating communication sessions between two devices on a network.

NEW QUESTION 183
- (Exam Topic 3)
Which of the following would be BEST suited for use at the access layer in a three-tier architecture system?

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

Answer: C

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

NEW QUESTION 188
- (Exam Topic 3)
A company is utilizing multifactor authentication for data center access. Which of the following is the MOST effective security mechanism against physical intrusions due to stolen credentials?

A. Biometrics security hardware
B. Access card readers
C. Access control vestibule
D. Motion detection cameras

Answer: C

NEW QUESTION 191
- (Exam Topic 3)
Which of the following would be the MOST likely attack used to bypass an access control vestibule?

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

Answer: A

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

NEW QUESTION 193
- (Exam Topic 3)
Which of the following is a valid and cost-effective solution to connect a fiber cable into a network switch without available SFP ports?

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

Answer: A

NEW QUESTION 197
- (Exam Topic 3)
A network technician is configuring a wireless access point and wants to only allow company-owned devices to associate with the network. The access point uses PSKs,
and a network authentication system does not exist on the network. Which of the following should the technician implement?

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

Answer: C

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

NEW QUESTION 198

- (Exam Topic 3)
Which of the following is a requirement when certifying a network cabling as Cat 7?

A. Ensure the patch panel is certified for the same category.
B. Limit 10Gb transmissions to 180ft (55m).
C. Use F-type connectors on the network terminations.
D. Ensure the termination standard is TIA/EIA-568-A.

Answer: D

Explanation:
Category 7 (Cat 7) is a cabling standard that supports 10GBASE-T Ethernet connections up to 100 meters (328 feet). In order for a cabling system to be certified as Cat 7, all components, including the patch panel, must meet the TIA/EIA-568-A standard. This standard requires the use of shielded cables with F-type connectors for the network terminations. Reference: CompTIA Network+ Study Manual, 8th Edition, page 158.

NEW QUESTION 199
- (Exam Topic 3)
Several users with older devices are reporting intermittent connectivity while in an outdoor patio area. After some research, the network administrator determines that an outdoor WAP might help with the issue. However, the company does not want the signal to bleed into the building and cause interference. Which of the following should the network administrator perform to BEST resolve the issue?

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

Answer: C

NEW QUESTION 204
- (Exam Topic 3)
Which of the following would be used when connecting devices that have different physical characteristics?

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

Answer: D

NEW QUESTION 207
- (Exam Topic 3)
A technician is investigating packet loss to a device that has varying data bursts throughout the day. Which of the following will the technician MOST likely configure to resolve the issue?

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

Answer: A

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

NEW QUESTION 210
- (Exam Topic 3)
A cafeteria is lacing lawsuits related to criminal internet access that was made over its guest network. The marketing team, however, insists on keeping the cafeteria phone number as the wireless passphrase. Which of the following actions would Improve wireless security while accommodating the marketing team and accepting the terms of use?

A. Setting WLAN security to use EAP-TLS
B. Deploying a captive portal tor user authentication
C. Using geofencing to limit the area covered by the WLAN
D. Configuring guest network isolation

Answer: B

Explanation:
A captive portal is a web page that is presented to a user before they are allowed to access a network. It is used to authenticate users and to ensure that all users have accepted the terms of use for the network. By deploying a captive portal, the cafeteria can require users to enter their phone number as the passphrase, while still providing an additional layer of security. Reference: CompTIA Network+ Study Guide, 8th Edition, page 182.

NEW QUESTION 213
- (Exam Topic 3)
At which of the following OSI model layers does routing occur?

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

Answer: D

NEW QUESTION 215
- (Exam Topic 3)
A technician is tasked with setting up a mail server and a DNS server. The mail port should be secured and have the ability to transfer large files. Which of the following ports should be opened? (Select TWO).

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

Answer: BE

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

NEW QUESTION 217
- (Exam Topic 3)
A network administrator is given the network 80.87.78.0/26 for specific device assignments. Which of the following describes this network?

A. 80.87.78 0 - 80.87.78.14
B. 80.87.78 0 - 80.87.78.110
C. 80.87.78 1 - 80.87.78.62
D. 80.87.78.1 - 80.87.78.158

Answer: C

Explanation:
The network 80.87.78.0/26 is a Class A network with a subnet mask of /26, which means that it contains 26 bits of network information and 6 bits of host information. The range of valid host addresses for this network is 80.87.78.1 to 80.87.78.62. Any addresses outside of this range are reserved for special purposes or are not used.

NEW QUESTION 218
- (Exam Topic 3)
A network administrator responds to a support ticket that was submitted by a customer who is having issues connecting to a website inside of the company network The administrator verities that the customer could not connect to a website using a URL Which of the following troubleshooting steps would be BEST for the administrator to take?

A. Check for certificate issues
B. Contact the ISP
C. Attempt to connect to the site via IP address
D. Check the NTP configuration.

Answer: C

Explanation:
The best option for the administrator to take would be to attempt to connect to the site via IP address. This will help to determine if the issue is related to the website's DNS address or if the site itself is not accessible. Checking for certificate issues may be necessary, but this should be done after the administrator has attempted to connect to the site via IP address. Contacting the ISP is unnecessary since the issue is related to the website inside of the company network, and checking the NTP configuration is not relevant to this issue.
When a customer is having issues connecting to a website using a URL, one of the first troubleshooting steps a network administrator should take is attempting to connect to the site using the IP address of the website. This will help to determine if the issue is related to a DNS resolution problem or a connectivity problem. If the administrator is able to connect to the website using the IP address, then the issue may be related to a DNS problem. However, if the administrator is still unable to connect, then the issue may be related to a connectivity problem. In either case, further troubleshooting steps will be necessary. Checking for certificate issues or NTP configuration, and contacting the ISP would not be the BEST initial steps in this scenario.

NEW QUESTION 221
- (Exam Topic 3)
A network administrator installed a new data and VoIP network. Users are now experiencing poor call quality when making calls. Which of the following should the administrator do to increase VoIP performance?

A. Configure a voice VLAN.
B. Configure LACP on all VoIP phones.
C. Configure PoE on the network.

D. Configure jumbo frames on the network.

Answer: A

Explanation:
"Benefits of Voice VLAN
It ensures that your VoIP (Voice over Internet Phone) devices do not have to contend directly with all the broadcasts and other traffic from the data VLAN. A voice VLAN can simplify network configuration in some circumstances."
https://community.fs.com/blog/auto-voip-vs-voice-vlan-what-s-the-difference.html Jumbo Frames
"When jumbo frames on a VoIP/UC network are enabled, it can cause the same kind of delay to your network transmissions."
"VoIP uses will always not benefit from jumbo frame, as VoIP like gaming, is latency and time sensitive. Jumbo Frame for Internet Purpose: You will not see any performance boost as the files that came across the internet does not support jumbo frame."
https://www.ankmax.com/newsinfo/1358641.html#:~:text=VoIP%20uses%20will%20always%20not,does%20n "To summarize this general best practice guide, you should NOT enable jumbo frame feature as a general home user."

NEW QUESTION 226
- (Exam Topic 3)
A malicious user is using special software 10 perform an on-path attack. Which of the following best practices should be configured to mitigate this threat?

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

Answer: A

NEW QUESTION 227
- (Exam Topic 3)
A company is moving to a new building designed with a guest waiting area that has existing network ports. Which of the following practices would BEST secure the network?

A. Ensure all guests sign an NDA.
B. Disable unneeded switchports in the area.
C. Lower the radio strength to reduce Wi-Fi coverage in the waiting area.
D. Enable MAC filtering to block unknown hardware addresses.

Answer: B

Explanation:
One of the best practices to secure the network would be to disable unneeded switchports in the guest waiting area. This will prevent unauthorized users from connecting to the network through these ports. It's important to identify which switchports are not in use and disable them, as this will prevent unauthorized access to the network.
Other practices such as ensuring all guests sign an NDA, lowering the radio strength to reduce Wi-Fi coverage in the waiting area and enabling MAC filtering to block unknown hardware addresses are not as effective in securing the network as disabling unneeded switchports. Enforcing an NDA with guests may not stop a malicious user from attempting to access the network, reducing the radio strength only limits the Wi-Fi coverage, and MAC filtering can be easily bypassed by hackers.

NEW QUESTION 230
- (Exam Topic 3)
A technician removes an old PC from the network and replaces it with a new PC that is unable to connect to the LAN. Which of the Mowing is MOST likely the cause of the issue?

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

Answer: A

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

NEW QUESTION 231
- (Exam Topic 3)
A network technician is troubleshooting a new web server connectivity issue. The network technician discovers the following on the support ticket
• The server's IP address can be pinged from the client PCs,
• Access to the web resource works correctly when on the server's console.
• No clients can access the servers data via URL.
• The server does not have a firewall configured
• No ACLs are preventing connectivity from the client's network.
• All services on the server are operating normally, which was confirmed by the server team. Which of the following actions will resolve the issue?

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

Answer: C

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

NEW QUESTION 235
- (Exam Topic 3)
Which of me following security controls indicates unauthorized hardware modifications?

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

Answer: A

NEW QUESTION 238
- (Exam Topic 3)
Which of the following would be used to adjust resources dynamically for a virtual web server under variable loads?

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

Answer: B

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

NEW QUESTION 243
- (Exam Topic 3)
Which of the following would enable a network technician to implement dynamic routing?

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

Answer: C

NEW QUESTION 247
- (Exam Topic 3)
A network technician is hired to review all the devices within a network and make recommendations to improve network efficiency. Which of the following should the technician do FIRST before reviewing and making any recommendations?

A. Capture a network baseline
B. Perform an environmental review.
C. Read the network logs
D. Run a bandwidth test

Answer: A

Explanation:
Before making any recommendations, a network technician should first capture a network baseline, which is a snapshot of the current performance of the network. This will give the technician a baseline to compare against after any changes are made. According to the CompTIA Network+ Study Manual, the technician should "capture the state of the network before making any changes and then compare the performance after the changes have been made. This will provide an accurate baseline to compare the performance of the network before and after the changes have been made."

NEW QUESTION 252
- (Exam Topic 3)
During a client audit, a network analyst is tasked with recommending changes to upgrade the client network and readiness. Afield technician has submitted the following report:

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

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

A. Electrical
B. Humidity

C. Flooding
D. Temperature

Answer: B

Explanation:
Humidity is the amount of water vapor in the air. High humidity can cause corrosion, condensation, and short circuits in electronic devices. Low humidity can cause static electricity and damage sensitive components. The optimal humidity range for a data center is between 40% and 60%. Based on the report, the humidity level in the server room is 70%, which is too high and can affect the performance and reliability of the network equipment. Therefore, the best recommendation to the client is to install a humidity sensor and a dehumidifier to control the humidity level in the server room.
References: Network+ Study Guide Objective 5.1: Summarize the importance of physical security controls.

NEW QUESTION 256
- (Exam Topic 3)
An administrator would like to have two servers at different geographical locations provide fault tolerance and high performance while appearing as one URL to users. Which of the following should the administrator implement?

A. Load balancing
B. Multipathing
C. NIC teaming
D. Warm site

Answer: A

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

NEW QUESTION 260
- (Exam Topic 3)
Which of the following connectors and terminations are required to make a Cat 6 cable that connects from a PC to a non-capable MDIX switch? (Select TWO).

A. T1A-568-A - TIA-568-B
B. TIA-568-B - TIA-568-B
C. RJ11
D. RJ45
E. F-type

Answer: AD

NEW QUESTION 262
- (Exam Topic 3)
A network technician is investigating a trouble ticket for a user who does not have network connectivity. All patch cables between the wall jacks and computers in the building were upgraded over the weekend from Cat 5 to Cat 6. The newly installed cable is crimped with a TIA/EIA 568A on one end and a TIA/EIA 568B on the other end.
Which of the following should the technician do to MOST likely fix the issue?

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

Answer: B

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

NEW QUESTION 267
- (Exam Topic 3)
A Chief Executive Officer and a network administrator came to an agreement With a vendor to purchase new equipment for the data center A document was drafted so all parties would be Informed about the scope of the project before It started. Which of the following terms BEST describes the document used?

A. Contract
B. Project charter
C. Memorandum of understanding
D. Non-disclosure agreement

Answer: B

Explanation:
The document used to inform all parties about the scope of the project before it starts is likely a project charter. A project charter is a document that outlines the key aspects of a project, including the project's objectives, scope, stakeholders, and resources. It serves as a formal agreement between the project team and the stakeholders, and helps to define the project's goals and constraints.
A project charter typically includes information about the project's scope, including the specific deliverables that are expected and any constraints or limitations that

may impact the project. It may also include details about the project team and stakeholders, the project schedule and budget, and the roles and responsibilities of each party.
By creating a project charter, the Chief Executive Officer and the network administrator can ensure that all parties involved in the project have a clear understanding of the project's goals and objectives, and can help to prevent misunderstandings or miscommunications during the project.
What is in a project charter?
A project charter is a formal short document that states a project exists and provides project managers with written authority to begin work. A project charter document describes a project to create a shared understanding of its goals, objectives and resource requirements before the project is scoped out in detail.
What are the 5 elements of the project charter?
What Are the Contents of a Project Charter? A project charter should always include an overview, an outline of scope, an approximate schedule, a budget estimate, anticipated risks, and key stakeholders

NEW QUESTION 271
- (Exam Topic 3)
An organization set up its offices so that a desktop is connected to the network through a VoIP phone. The VoIP vendor requested that voice traffic be segmented separately from non-voice traffic. Which of the following would allow the organization to configure multiple devices with network isolation on a single switch port?

A. Subinterfaces
B. Link aggregation
C. Load balancing
D. Tunneling

Answer: A

NEW QUESTION 275
- (Exam Topic 3)
Which of the Mowing architectures reduces network latency by enforcing a limit on the number of switching devices on the frame's path between any internal hosts?

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

Answer: A

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

NEW QUESTION 280
- (Exam Topic 3)
A network administrator has received calls every day for the past few weeks from three users who cannot access the network. The administrator asks all the users to reboot their PCs, but the same users still cannot access the system. The following day, three different users report the same issue, and the administrator asks them all to reboot their PCs; however, this does not fix the issue. Which of the following is MOST likely occurring?

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

Answer: E

NEW QUESTION 285
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual N10-009 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the N10-009 Product From:

https://www.2passeasy.com/dumps/N10-009/

Money Back Guarantee

N10-009 Practice Exam Features:

* N10-009 Questions and Answers Updated Frequently

* N10-009 Practice Questions Verified by Expert Senior Certified Staff

* N10-009 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* N10-009 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year