CompTIA

Exam Questions N10-009

CompTIA Network+ Exam

About Exambible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1
- (Exam Topic 1)
An 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 company built a new building at its headquarters location. The new building is connected to the company's LAN via fiber-optic cable. Multiple users in the new building are unable to access the company's intranet site via their web browser, but they are able to access internet sites. Which of the following describes how the network administrator can resolve this issue?

A. Correct the DNS server entries in the DHCP scope
B. Correct the external firewall gateway address
C. Correct the NTP server settings on the clients
D. Correct a TFTP Issue on the company's server

Answer: A

Explanation:
If multiple users in a new building are unable to access the company's intranet site via their web browser but are able to access internet sites, the network administrator can resolve this issue by correcting the DNS server entries in the DHCP scope. The DHCP scope is responsible for assigning IP addresses and DNS server addresses to clients. If the DNS server entries are incorrect, clients will not be able to access intranet sites.
References:
CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 4: Network Implementations, Objective 4.4: Explain the purpose and properties of DHCP.

NEW QUESTION 3
- (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 4
- (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 5
- (Exam Topic 1)
An attacker is attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt. Which of the following attack types BEST describes this action?

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

Answer: D

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

NEW QUESTION 6
- (Exam Topic 1)
A network administrator is installing a wireless network at a client's office. Which of the following IEEE 802.11 standards would be BEST to use for multiple simultaneous client access?

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

Answer: C

Explanation:
CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is an IEEE 802.11 standard that would be best to use for multiple simultaneous client access on a wireless network. CSMA/CA is a media access control method that allows multiple devices to share the same wireless channel without causing collisions or interference. It works by having each device sense the channel before transmitting data and waiting for an acknowledgment from the receiver after each transmission. If the channel is busy or no acknowledgment is received, the device will back off and retry later with a random delay. References: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-csma-ca.html

NEW QUESTION 7
- (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 8
- (Exam Topic 1)
Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

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

Answer: C

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

NEW QUESTION 9
- (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 10
- (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 10
- (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 12
- (Exam Topic 1)
A technician is searching for a device that is connected to the network and has the device’s physical network address. Which of the following should the technician review on the switch to locate the device’s network port?

A. IP route table
B. VLAN tag
C. MAC table
D. QoS tag

Answer: C

Explanation:
To locate a device's network port on a switch, a technician should review the switch's MAC address table. The MAC address table maintains a list of MAC addresses of devices connected to each port on the switch. By checking the MAC address of the device in question, the technician can identify the port to which the device is connected.
References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 16
- (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 17
- (Exam Topic 1)
Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

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

Answer: B

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

NEW QUESTION 21
- (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 24
- (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 25
- (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 30
- (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 35
- (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 36
- (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 38
- (Exam Topic 1)
Which of the following factors should be considered when evaluating a firewall to protect a datacenter’s east-west traffic?

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

Answer: B

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

NEW QUESTION 43
- (Exam Topic 1)
A user reports being unable to access network resources after making some changes in the office. Which of the following should a network technician do FIRST?

A. Check the system's IP address
B. Do a ping test against the servers
C. Reseat the cables into the back of the PC
D. Ask what changes were made

Answer: D

Explanation:
When a user reports being unable to access network resources after making some changes, the network technician should first ask the user what changes were made. This information can help the technician identify the cause of the issue and determine the appropriate course of action.
References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 48
- (Exam Topic 1)
A technician is assisting a user who cannot connect to a network resource. The technician first checks for a link light. According to troubleshooting methodology, this is an example of:

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

Answer: A

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

NEW QUESTION 53
- (Exam Topic 1)
Which of the following service models would MOST likely be used to replace on-premises servers with a cloud solution?

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

Answer: B

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

NEW QUESTION 58
- (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 62
- (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 65
- (Exam Topic 1)
Which of the following technologies provides a failover mechanism for the default gateway?

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

Answer: A

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

NEW QUESTION 69
- (Exam Topic 2)
Which of the following uses the destination IP address to forward packets?

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

Answer: C

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

NEW QUESTION 70
- (Exam Topic 2)
Which of the following services can provide data storage, hardware options, and scalability to a third-party company that cannot afford new devices?

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

Answer: B

Explanation:
IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources such as servers, storage, and networking over the Internet. IaaS can provide data storage, hardware options, and scalability to a third-party company that cannot afford new devices by allowing them to rent or lease the infrastructure they need from a cloud provider. The company can pay only for what they use and scale up or down as needed. References: https://www.comptia.org/blog/what-is-iaas

NEW QUESTION 75
- (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 77
- (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 82
- (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 86
- (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 87
- (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 89
- (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 92
- (Exam Topic 2)
A network administrator is talking to different vendors about acquiring technology to support a new project for a large company. Which of the following documents will MOST likely need to be signed before information about the project is shared?

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

Answer: B

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

NEW QUESTION 94
- (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 96
- (Exam Topic 2)
Which of the following security devices would be BEST to use to provide mechanical access control to the MDF/IDF?

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

Answer: D

Explanation:
A door lock would be the best security device to use to provide mechanical access control to the MDF/IDF. A door lock is a device that prevents unauthorized access to a physical area by requiring a key, a code, a card, a biometric scan, or a combination of these factors to open it. A door lock can provide mechanical access control to the MDF/IDF, which are rooms that house network equipment such as switches, routers, servers, or patch panels. A door lock can prevent unauthorized persons from tampering with or stealing the network equipment or data. References:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_6.html

NEW QUESTION 100
- (Exam Topic 2)
A company is being acquired by a large corporation. As part of the acquisition process, the company's address should now redirect clients to the corporate organization page. Which of the following DNS records needs to be created?

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

Answer: C

Explanation:
Reference:
https://www.namecheap.com/support/knowledgebase/article.aspx/9604/2237/types-of-domain-redirects-301-302
CNAME (Canonical Name) is a type of DNS record that maps an alias name to another name, which can be either another alias or the canonical name of a host or domain. A CNAME record can be used to redirect clients from one domain name to another domain name, such as from the company's address to the corporate organization page. SOA (Start of Authority) is a type of DNS record that specifies authoritative information about a DNS zone, such as the primary name server, contact email address, serial number, refresh interval, etc., which does not redirect clients to another domain name. NS (Name Server) is a type of DNS record that specifies which name server is authoritative for a domain or subdomain, which does not redirect clients to another domain name. TXT (Text) is a type of DNS record that provides arbitrary text information about a domain or subdomain, such as SPF (Sender Policy Framework) records or DKIM (DomainKeys Identified Mail) records, which does not redirect clients to another domain name.

NEW QUESTION 105
- (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 108
- (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 110
- (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 111
- (Exam Topic 2)
A technician is deploying a low-density wireless network and is contending with multiple types of building materials. Which of the following wireless frequencies would allow for the LEAST signal attenuation?

A. 2.4GHz
B. 5GHz
C. 850MHz
D. 900MHZ

Answer: A

Explanation:
* 2.4 GHz is the wireless frequency that would allow for the least signal attenuation when deploying a low-density wireless network with multiple types of building materials. Signal attenuation is the loss of signal strength or quality as it travels through a medium or over a distance. Signal attenuation can be affected by various factors such as distance, interference, reflection, refraction, diffraction, scattering, or absorption. Generally, lower frequencies have less signal attenuation than higher frequencies because they can penetrate obstacles better and travel farther. Therefore, 2.4GHz would have less signal attenuation than 5GHz, 850MHz, or 900MHz. References: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html

NEW QUESTION 115
- (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 119
- (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 121
- (Exam Topic 3)
Which of the following needs to be tested to achieve a Cat 6a certification for a company's data cawing?

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

Answer: D

NEW QUESTION 124
- (Exam Topic 3)
Which of the following layers of the OSI model has new protocols activated when a user moves from a wireless to a wired connection?

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

Answer: A

Explanation:
"The Data Link layer also determines how data is placed on the wire by using an access method. The wired access method, carrier-sense multiple access with

collision detection (CSMA/CD), was once used by all wired Ethernet networks, but is automatically disabled on switched full-duplex links, which have been the norm for decades. Carrier-sense multiple access with collision avoidance (CSMA/CA) is used by wireless networks, in a similar fashion."

NEW QUESTION 128
- (Exam Topic 3)
Which of the following devices would be used to extend the range of a wireless network?

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

Answer: A

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

NEW QUESTION 129
- (Exam Topic 3)
A large number of PCs are obtaining an APIPA IP address, and a number of new computers were added to the network. Which of the following is MOST likely causing the PCs to obtain an APIPA address?

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

Answer: D

Explanation:
DHCP scope exhaustion means that there are no more available IP addresses in the DHCP server's pool of addresses to assign to new devices on the network. When this happens, the devices will use APIPA (Automatic Private IP Addressing) to self-configure an IP address in the range of 169.254.0.1 to 169.254.255.2541. These addresses are not routable and can only communicate with other devices on the same local network.
A rogue DHCP server (A) is an unauthorized DHCP server that can cause IP address conflicts or security issues by assigning IP addresses to devices on the network. A network collision (B) is a situation where two or more devices try to send data on the same network segment at the same time, causing interference and data loss. Incorrect DNS settings © can prevent devices from resolving domain names to IP addresses, but they do not affect the DHCP process.

NEW QUESTION 133
- (Exam Topic 3)
Which of the following devices Is used to configure and centrally manage access points Installed at different locations?

A. Wireless controller
B. Load balancer
C. Proxy server
D. VPN concentrator

Answer: A

Explanation:
Access points (APs) can be configured and centrally managed using a wireless LAN controller (WLC). A WLC is a device that connects to multiple APs and provides centralized management and control of those APs. The WLC can be used to configure settings such as wireless network parameters, security settings, and quality of service (QoS) policies. Additionally, the WLC can be used to monitor the status of connected APs, track client connections, and gather statistics on network usage. Some vendors such as Cisco, Aruba, Ruckus, etc. provide wireless LAN controllers as part of their wireless networking solutions.

NEW QUESTION 138
- (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 143
- (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

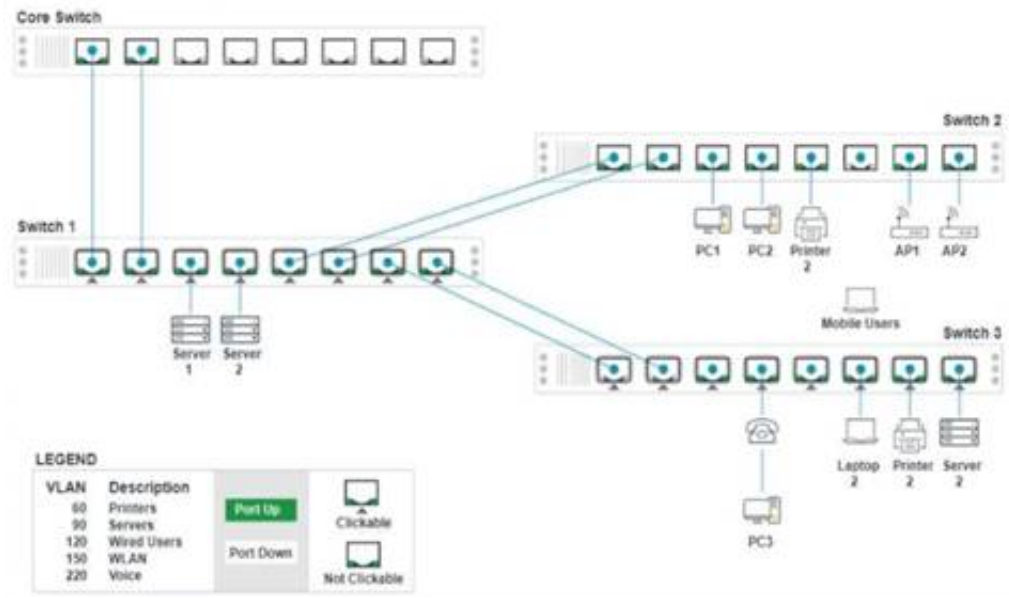
NEW QUESTION 146
- (Exam Topic 3)
A company with multiple routers would like to implement an HA network gateway with the least amount of downtime possible. This solution should not require changes on the gateway setting of the network clients. Which of the following should a technician configure?

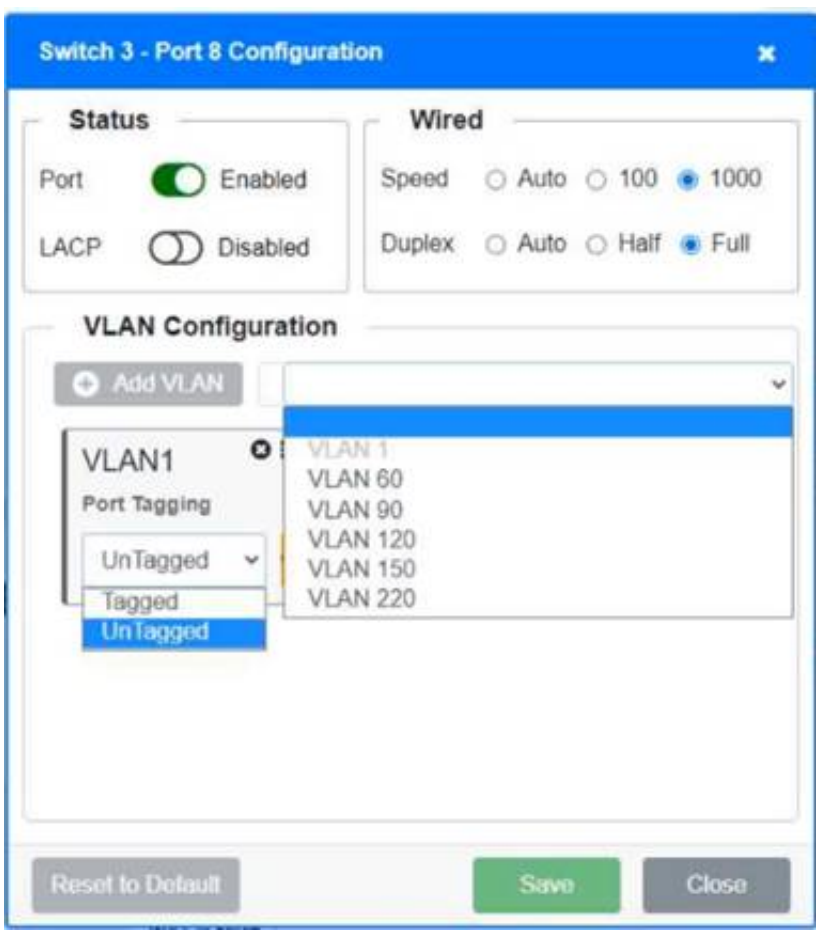
A. Automate a continuous backup and restore process of the system's state of the active gateway.
B. Use a static assignment of the gateway IP address on the network clients.
C. Configure DHCP relay and allow clients to receive a new IP setting.
D. Configure a shared VIP and deploy VRRP on the routers.

Answer: D

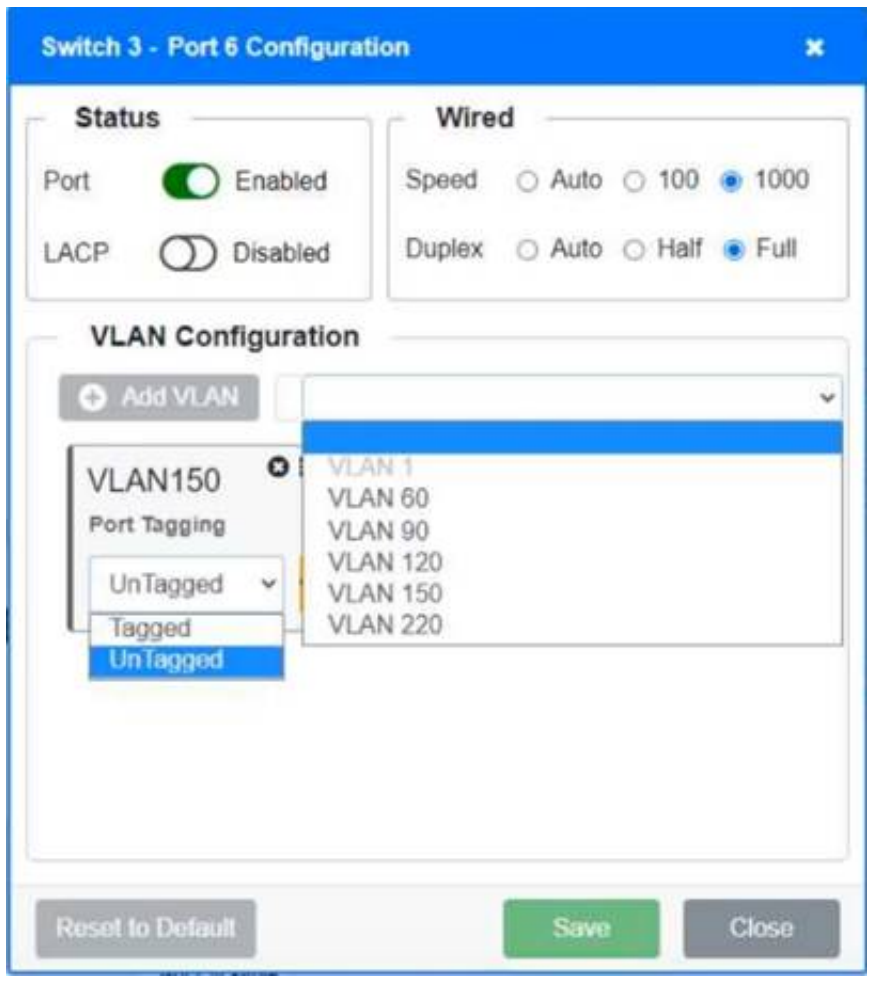
Explanation:
The open standard protocol Virtual Router Redundancy Protocol (VRRP) is similar to HSRP, the differences mainly being in terminology and packet formats. In VRRP, the active router is known as the master, and all other routers in the group are known as backup routers. There is no specific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

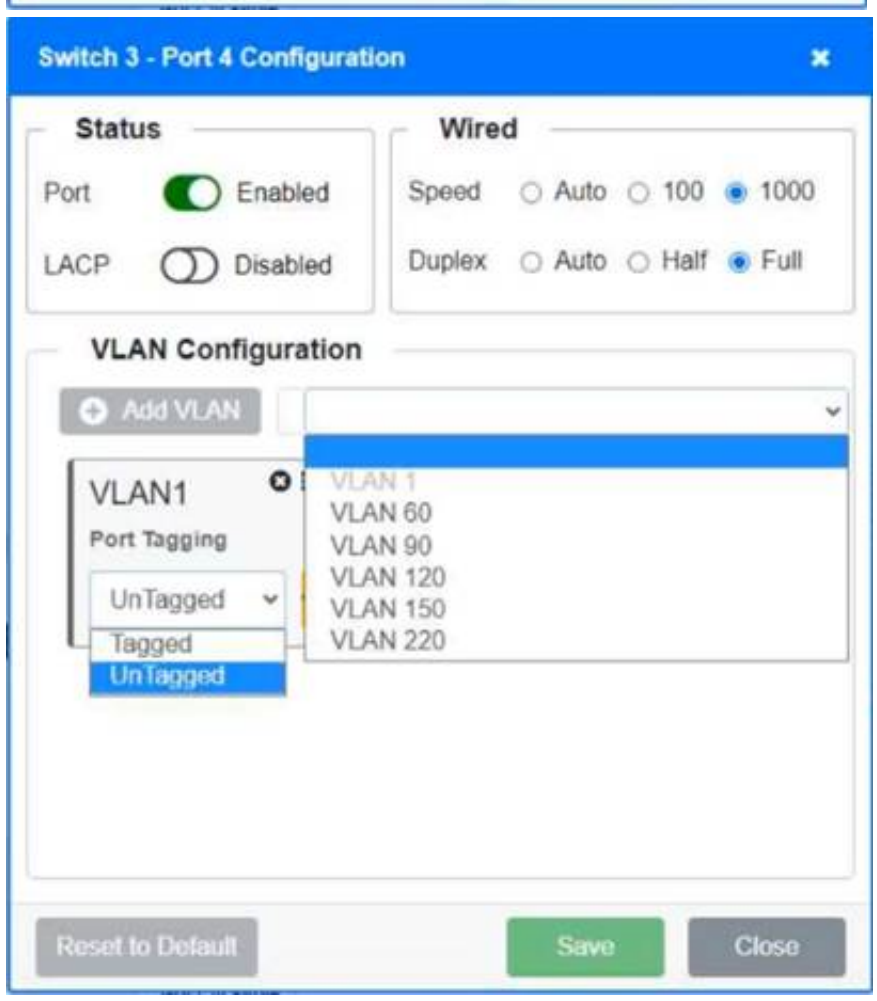
NEW QUESTION 151
- (Exam Topic 3)
SIMULATION
A network technician replaced a switch and needs to reconfigure it to allow the connected devices to connect to the correct networks.
INSTRUCTIONS
Click on the appropriate port(s) on Switch 1 and Switch 3 to verify or reconfigure the correct settings:
• Ensure each device accesses only its correctly associated network
• Disable all unused switch ports
• Require fault-tolerant connections between the switches
• Only make necessary changes to complete the above requirements
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



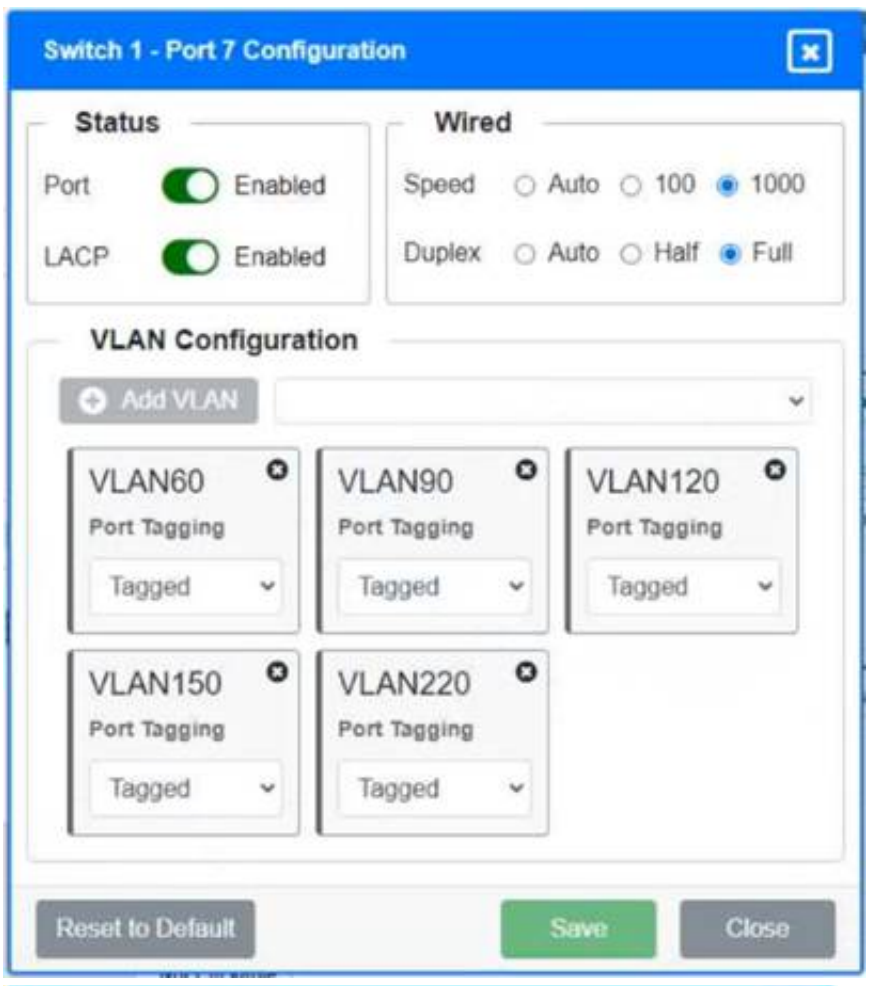


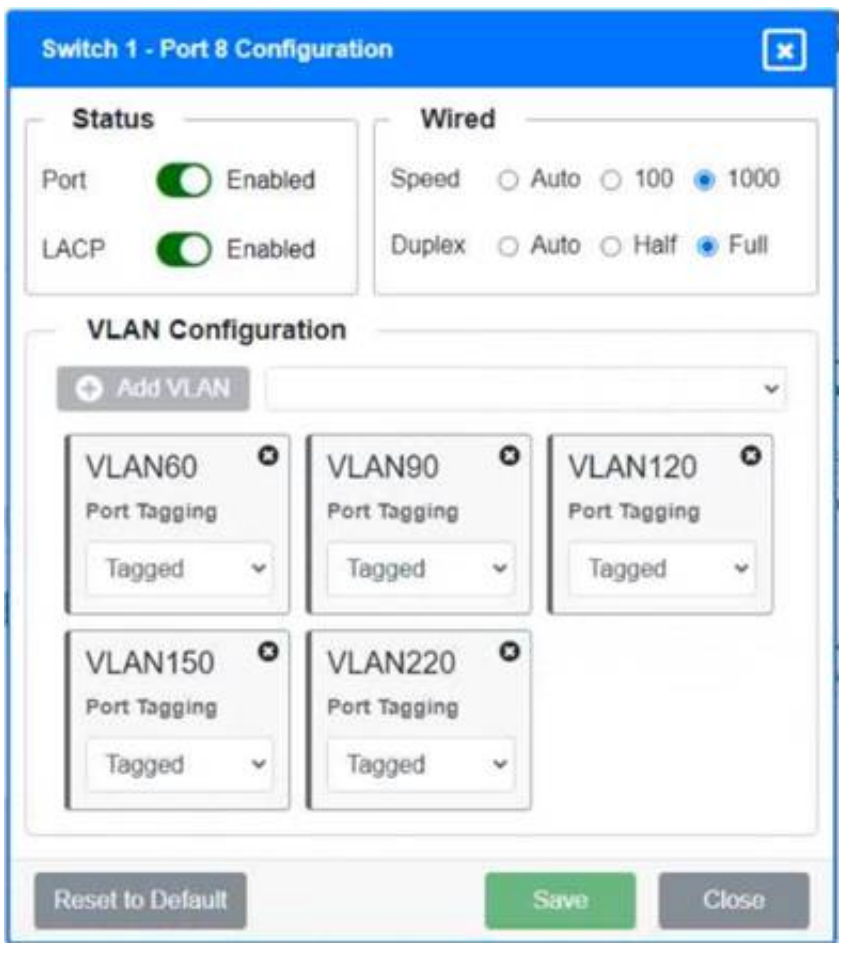
Switch 3 - Port 7 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close

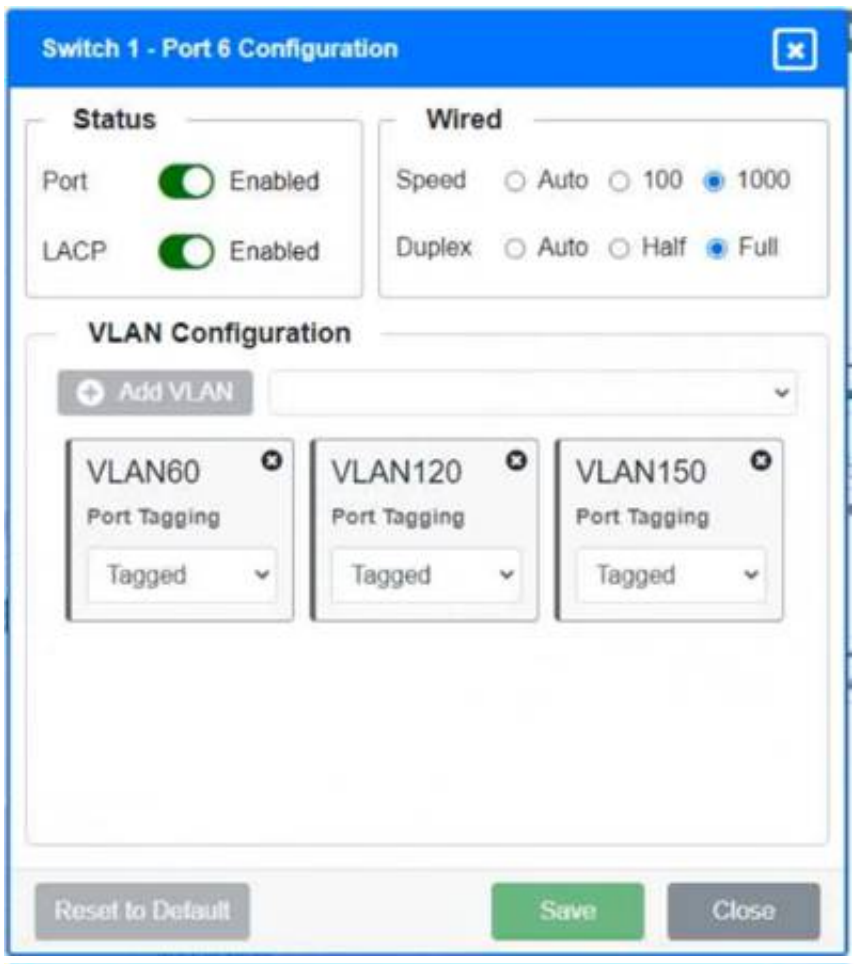

Switch 3 - Port 6 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN150
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close

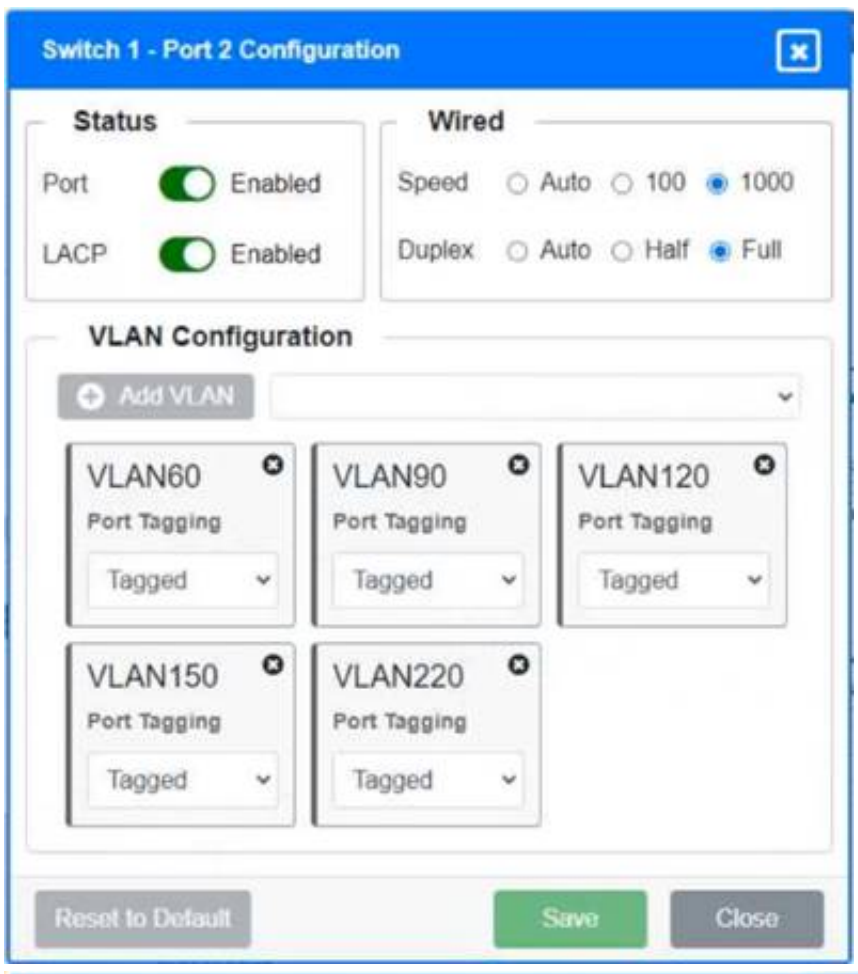

Switch 3 - Port 4 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close

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

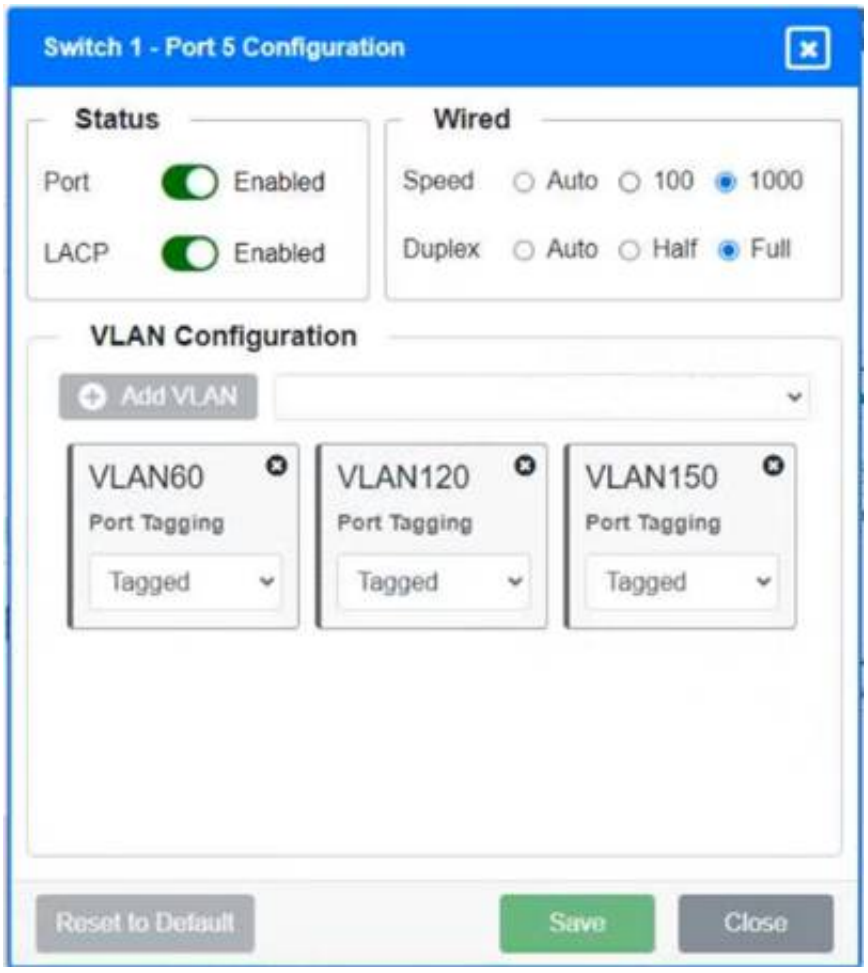

Switch 1 - Port 7 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save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

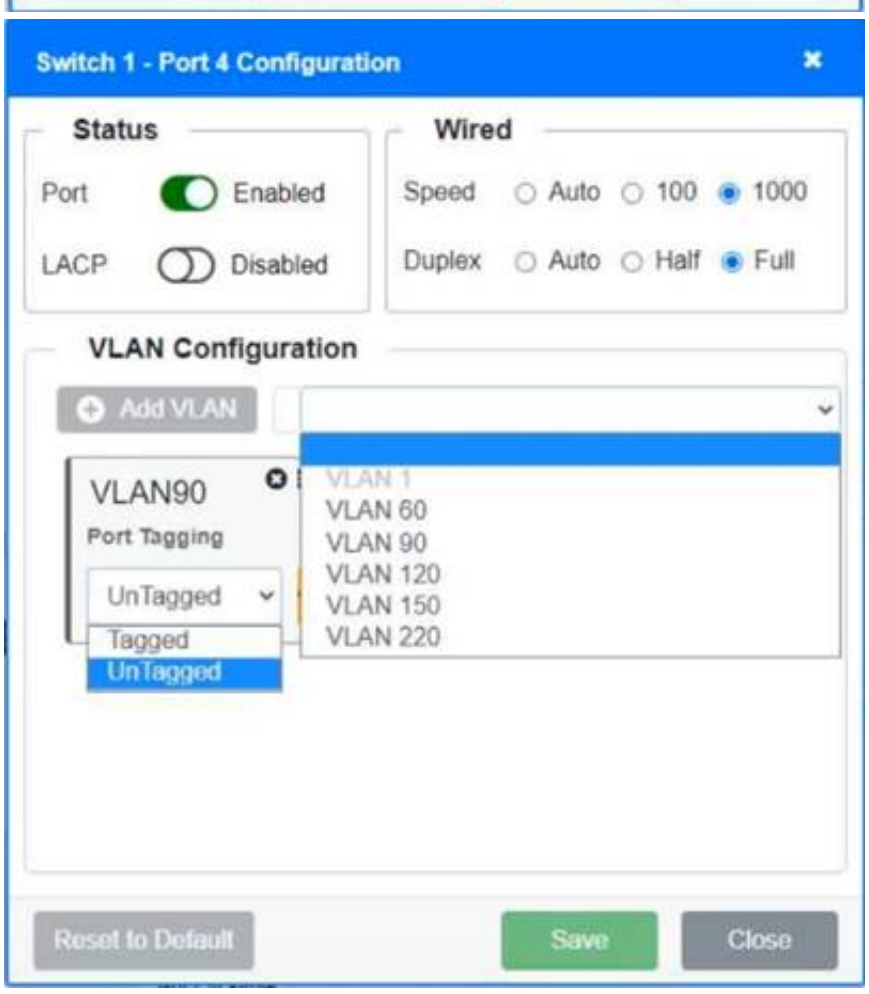

Switch 1 - Port 8 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save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


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

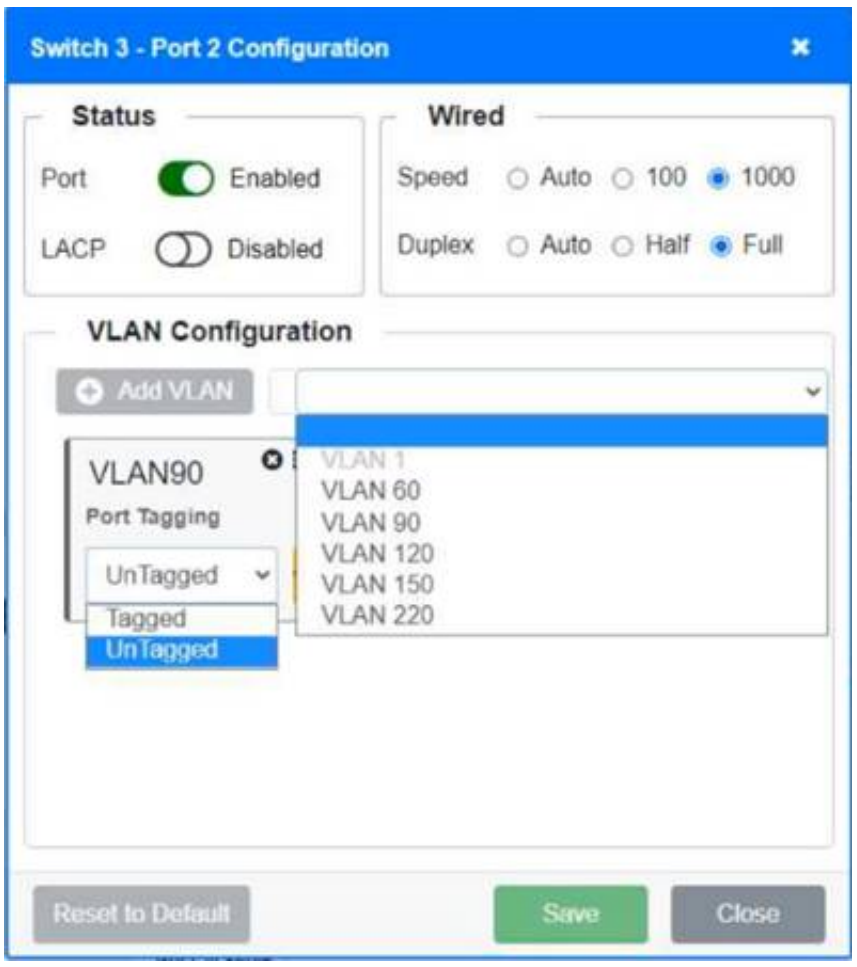

Switch 1 - Port 2 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save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

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


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


Switch 1 - Port 4 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN90
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 156
- (Exam Topic 3)
Which of the following would be the MOST cost-effective recovery solution for a company's lower-priority applications?

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

Answer: C

NEW QUESTION 159
- (Exam Topic 3)
Many IP security cameras use RTSP to control media playback. Which of the following default transport layer port numbers does RTSP use?

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

Answer: B

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

NEW QUESTION 161
- (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 163
- (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 167
- (Exam Topic 3)
When accessing corporate network resources, users are required to authenticate to each application they try to access. Which of the following concepts does this BEST represent?

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

Answer: B

NEW QUESTION 169
- (Exam Topic 3)
A company is opening a new building on the other side of its campus. The distance from the closest building to the new building is 1,804ft (550m). The company needs to connect the networking equipment in the new building to the Other buildings on the campus without using a repeater. Which Of the following transceivers should the company use?

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

Answer: B

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

NEW QUESTION 173
- (Exam Topic 3)
Which of the following protocols can be routed?

A. FCoE
B. Fibre Channel
C. iSCSl
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 178
- (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 181
- (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 182
- (Exam Topic 3)
A new company recently moved into an empty office space Within days, users in the next office began noticing increased latency and packet drops with their Wi-Fi-connected devices. Which of the following is the MOST likely reason for this issue?

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

Answer: A

NEW QUESTION 184
- (Exam Topic 3)
A network technician receives a report about a performance issue on a client PC that is connected to port 1/3 on a network switch. The technician observes the following configuration output from the switch:

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

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

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

Answer: A

NEW QUESTION 188
- (Exam Topic 3)
Which of the following protocols is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links?

A. OSPF
B. RIPv2
C. QoS

D. STP

Answer: A

NEW QUESTION 193
- (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 195
- (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 197
- (Exam Topic 3)
Which of the following layers of the OSI model receives data from the application layer and converts it into syntax that is readable by other devices on the network?

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

Answer: C

NEW QUESTION 198
- (Exam Topic 3)
The Chief Executive Officer of a company wants to ensure business operations are not disrupted in the event of a disaster. The solution must have fully redundant equipment, real-time synchronization, and zero data loss. Which Of the following should be prepared?

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

Answer: C

Explanation:
A hot site is a backup site that is fully equipped and ready to take over the operations of the primary site in the event of a disaster. A hot site has real-time synchronization with the primary site and can provide zero data loss. A hot site is the most expensive and reliable option for disaster recovery.
References: Network+ Study Guide Objective 5.3: Explain common scanning, monitoring and patching processes and summarize their expected outputs.

NEW QUESTION 203
- (Exam Topic 3)
A network administrator wants to test the throughput of a new metro Ethernet circuit to verify that its
performance matches the requirements specified m the SLA. Which of the following would BEST help measure the throughput?

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

Answer: A

NEW QUESTION 204
- (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 206
- (Exam Topic 3)
A network administrator is trying to add network redundancy for the server farm. Which of the following can the network administrator configure to BEST provide this capability?

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

Answer: A

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

NEW QUESTION 211
- (Exam Topic 3)
Which of the following is used when a workstation sends a DHCP broadcast to a server on another LAN?

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

Answer: C

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

NEW QUESTION 214
- (Exam Topic 3)
A computer engineer needs to ensure that only a specific workstation can connect to port 1 on a switch. Which of the following features should the engineer configure on the switch interface?

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

Answer: B

Explanation:
Port security is a feature that can be configured on a switch interface to limit and identify the MAC addresses of workstations that are allowed to connect to that specific port. This can help ensure that only a specific workstation (or workstations) can connect to the interface. According to the CompTIA Network+ Study Manual, “Port security can be used to specify which MAC addresses are allowed to connect to a particular switch port. If a port security violation is detected, the switch can take a number of different actions, such as shutting down the port, sending an SNMP trap, or sending an email alert.”

NEW QUESTION 219
- (Exam Topic 3)
A building was recently remodeled in order to expand the front lobby. Some mobile users have been unable to connect to the available network jacks within the new lobby, while others have had no issues. Which of the following is the MOST likely cause of the connectivity issues?

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

Answer: B

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

NEW QUESTION 221
- (Exam Topic 3)
Which of the following topologies is designed to fully support applications hosted in on-premises data centers, public or private clouds, and SaaS services?

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

Answer: A

NEW QUESTION 223
- (Exam Topic 3)
A network administrator is implementing process changes based on recommendations following a recent penetration test. The testers used a method to gain access to the network that involved exploiting a publicly available and fixed remote code execution vulnerability in the VPN appliance. Which of the following should the administrator do to BEST prevent this from happening again?

A. Change default passwords on internet-facing hardware.
B. Implement robust ACLs with explicit deny-all entries.
C. Create private VLANs for management plane traffic.
D. Routinely upgrade all network equipment firmware.

Answer: D

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

NEW QUESTION 225
- (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 229
- (Exam Topic 3)
A network administrator is troubleshooting a client's device that cannot connect to the network. A physical inspection of the switch shows the RJ45 is connected. The NIC shows no activity lights. The network administrator moves the device to another location and connects to the network without issues. Which Of the following tools would be the BEST option for the network administrator to use to further troubleshoot?

A. Tone generator
B. Multimeter
C. Optical time-domain reflectometer
D. Cable tester

Answer: D

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

NEW QUESTION 233

- (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 237
- (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 241
- (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 245
- (Exam Topic 3)
A desktop support department has observed slow wireless speeds for a new line of laptops using the organization's standard image. No other devices have experienced the same issue. Which of the following should the network administrator recommend troubleshooting FIRST to resolve this issue?

A. Increasing wireless signal power
B. Installing a new WAP
C. Changing the protocol associated to the SSID
D. Updating the device wireless drivers

Answer: D

Explanation:
Wireless drivers can affect the performance and compatibility of your wireless connection5. If only a new line of laptops using the organization’s standard image has experienced slow wireless speeds, it could be that their wireless drivers are outdated or incompatible with the network. Updating the device wireless drivers could resolve this issue.
Wireless drivers play an important role in the performance of a wireless connection, as they control how the device interacts with the wireless network. If the laptops in question are using an outdated version of the wireless driver, it could be causing the slow speeds. The network administrator should recommend updating the device wireless drivers first to see if this resolves the issue.

NEW QUESTION 250
- (Exam Topic 3)
A technician is contracted to install a redundant cluster of devices from the ISP In case of a hardware failure within the network. Which of the following would provide the BEST redundant solution in Layer 2 devices?

A. Multiple routers
B. Multiple switches
C. Multiple firewalls
D. Multiple budges

Answer: B

NEW QUESTION 254
- (Exam Topic 3)
A new office space is being designed. The network switches are up. but no services are running yet A network engineer plugs in a laptop configured as a DHCP client to a switch Which ol the following IP addresses should be assigned to the laptop?

A. 10.1.1.1
B. 169.254.1.128

C. 172 16 128 128
D. 192 168.0.1

Answer: B

Explanation:
When a DHCP client is connected to a network and no DHCP server is available, the client can automatically configure a link-local address in the 169.254.0.0/16 range using the Automatic Private IP Addressing (APIPA) feature. So, the correct answer is option B, 169.254.1.128. This is also known as an APIPA address.
Reference: CompTIA Network+ Study Guide, Exam N10-007, Fourth Edition, by Todd Lammle (Chapter 4: IP Addressing)

NEW QUESTION 257
- (Exam Topic 3)
An ISP configured an internet connection to provide 20Mbps, but actual data rates are occurring at 10Mbps and causing a significant delay in data transmission. Which of the following specifications should the ISP check?

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

Answer: A

Explanation:
Throughput is the actual amount of data that can be transferred over a network in a given time. Throughput can be affected by various factors such as congestion, interference, errors, or hardware limitations. If the throughput is lower than the configured internet connection speed, it can cause a significant delay in data transmission. The ISP should check the throughput and identify the source of the problem.
References: Network+ Study Guide Objective 2.2: Explain the concepts and characteristics of routing and switching.

NEW QUESTION 259
- (Exam Topic 3)
A new student is given credentials to log on to the campus Wi-Fi. The student stores the password in a laptop and is able to connect; however, the student is not able to connect with a phone when only a short distance from the laptop. Given the following information:

Signal strength	90%
Coverage	80%
Interference	15%
Number of connection attempts	10

Which of the following is MOST likely causing this connection failure?

A. Transmission speed
B. Incorrect passphrase
C. Channel overlap
D. Antenna cable attenuation/signal loss

Answer: B

NEW QUESTION 263
- (Exam Topic 3)
Which of the following would be used to forward requests and replies between a DHCP server and client?

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

Answer: A

NEW QUESTION 266
- (Exam Topic 3)
A network administrator is testing performance improvements by configuring channel bonding on an 802.Hac AP. Although a site survey detected the majority of the 5GHz frequency spectrum was idle, being used only by the company's WLAN and a nearby government radio system, the AP is not allowing the administrator to manually configure a large portion of the 5GHz frequency range. Which of the following would be BEST to configure for the WLAN being tested?

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

Answer: C

NEW QUESTION 268
- (Exam Topic 3)
A company, which is located in a coastal town, retrofitted an office building for a new data center. The underground fiber optics were brought in and connected to the switches in the basement network MDF. A server data center was built on the fifth floor with the two rooms vertically connected by fiber optics. Which of the following types of environmental sensors is MOST needed?

A. Temperature sensor in the network MDF
B. Water sensor in the network MDF
C. Temperature sensor in the data center
D. Water sensor in the data center

Answer: B

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

NEW QUESTION 270
- (Exam Topic 3)
In which of the following components do routing protocols belong in a software-defined network?

A. Infrastructure layer
B. Control layer
C. Application layer
D. Management plane

Answer: B

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

NEW QUESTION 273
- (Exam Topic 3)
Which of the following physical security methods Is the MOST effective to prevent tailgating?

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

Answer: A

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

NEW QUESTION 277
- (Exam Topic 3)
A network security engineer locates an unapproved wireless bridge connected to the corporate LAN that is broadcasting a hidden SSID, providing unauthenticated access to internal resources. Which of the following types of attacks BEST describes this finding?

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

Answer: A

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

NEW QUESTION 279
- (Exam Topic 3)
A network engineer receives the following when connecting to a switch to configure a port:

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

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

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

Answer: D

NEW QUESTION 281
- (Exam Topic 3)
A client who shares office space and an IT closet with another company recently reported connectivity issues throughout the network. Multiple third-party vendors regularly perform on-site maintenance in the shared IT closet. Which of the following security techniques would BEST secure the physical networking equipment?

A. Disabling unneeded switchports
B. Implementing role-based access
C. Changing the default passwords
D. Configuring an access control list

Answer: B

Explanation:
Role-based access is a security technique that assigns permissions and privileges to users or groups based on their roles or functions within an organization. Role-based access can help secure the physical networking equipment by limiting who can access, modify, or manage the devices in the shared IT closet. Only authorized personnel with a valid role and credentials should be able to access the networking equipment. Disabling unneeded switchports is a security technique that prevents unauthorized devices from connecting to the network by turning off unused ports on a switch. Changing the default passwords is a security technique that prevents unauthorized access to network devices by replacing the factory-set passwords with strong and unique ones. Configuring an access control list is a security technique that filters network traffic by allowing or denying packets based on criteria such as source and destination IP addresses, ports, or protocols.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.2: Given a scenario, use appropriate network hardening techniques.

NEW QUESTION 283
- (Exam Topic 3)
Which of the following types of attacks can be used to gain credentials by setting up rogue APs with identical corporate SSIDs?

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

Answer: B

NEW QUESTION 287
- (Exam Topic 3)
A technician is troubleshooting reports that a networked printer is unavailable. The printer's IP address is configured with a DHCP reservation, but the address cannot be pinged from the print server in the same subnet. Which of the following is MOST likely the cause of me connectivity failure?

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

Answer: D

NEW QUESTION 291
- (Exam Topic 3)
After HVAC failures caused network outages, the support team decides to monitor the temperatures of all the devices. The network administrator cannot find a command that will display this information. Which of the following will retrieve the necessary information?

A. SNMP OID values
B. NetFlow data export
C. Network baseline configurations
D. Security information and event management

Answer: A

Explanation:
The network administrator can use the Simple Network Management Protocol (SNMP) to monitor the temperatures of all the devices. SNMP is a widely-used protocol for managing and monitoring network devices, such as routers, switches, servers, and other networking equipment. SNMP allows network administrators to gather information about the performance and status of devices on the network, including temperature readings.
To retrieve the temperature information, the administrator will have to configure SNMP on the devices and configure SNMP manager software on their computer. Once the SNMP manager software is configured, it will be able to send SNMP requests to the devices and retrieve information such as temperature, voltage, fan speeds, etc. Many network devices have built-in SNMP support, and the administrator may also need to install SNMP agent software on the devices to enable SNMP monitoring.
The administrator can also use some specific command or tool like IPMI (Intelligent Platform Management Interface) or DCIM (Data Center Infrastructure Management) tools for monitoring the temperatures of all the devices.

NEW QUESTION 295
- (Exam Topic 3)
Which of the following can be used to validate domain ownership by verifying the presence of pre-agreed content contained in a DNS record?

A. SOA
B. SRV
C. AAA
D. TXT

Answer: D

Explanation:
"One final usage of the TXT resource record is how some cloud service providers, such as Azure, validate ownership of custom domains. You are provided with data to include in your TXT record, and once that is created, the domain is verified and able to be used. The thought is that if you control the DNS, then you own the domain name."

NEW QUESTION 298
- (Exam Topic 3)
Which of the following protocols uses Dijkstra's algorithm to calculate the LOWEST cost between routers?

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

Answer: B

Explanation:
OSPF stands for Open Shortest Path First and is a link-state routing protocol that uses Dijkstra's algorithm to calculate the lowest cost between routers. OSPF assigns a cost value to each link based on factors such as bandwidth, delay, or reliability, and builds a map of the network topology. OSPF then uses Dijkstra's algorithm to find the shortest path from each router to every other router in the network1. RIP stands for Routing Information Protocol and is a distance-vector routing protocol that uses hop count as the metric to find the best path. BGP stands for Border Gateway Protocol and is a path-vector routing protocol that uses attributes such as AS path, local preference, or origin to select the best route. EIGRP stands for Enhanced Interior Gateway Routing Protocol and is a hybrid routing protocol that uses a composite metric based on bandwidth, delay, load, and reliability.
References: 1 Dijkstra's algorithm - Wikipedia (https://en.wikipedia.org/wiki/Dijkstra%27s_algorithm)

NEW QUESTION 301
- (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 303
- (Exam Topic 3)
A network technician has determined the cause of a network disruption. Which of the following is the NEXT step for the technician to perform?

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

Answer: C

NEW QUESTION 304
- (Exam Topic 3)
A technician is configuring a wireless network and needs to ensure users agree to an AUP before connecting. Which of the following should be implemented to achieve this goal?

A. Captive portal
B. Geofencing
C. Wireless client isolation
D. Role-based access

Answer: A

NEW QUESTION 307
- (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 312
- (Exam Topic 3)
Which of the following is conducted frequently to maintain an updated list of a system's weaknesses?

A. Penetration test
B. Posture assessment
C. Risk assessment
D. Vulnerability scan

Answer: D

NEW QUESTION 314
- (Exam Topic 3)
Two network technicians are installing a fiber-optic link between routers. The technicians used a light meter to verify the correct fibers However, when they connect the fibers to the router interface the link does not connect. Which of the following would explain the issue? (Select TWO).

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

Answer: AB

NEW QUESTION 319
- (Exam Topic 3)
A network technician receives a report from the server team that a server's network connection is not working correctly. The server team confirms the server is operating correctly except for the network connection. The technician checks the switchport connected to the server and reviews the following data;

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

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

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

Answer: A

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

NEW QUESTION 322
- (Exam Topic 3)
Which of the following describes traffic going in and out of a data center from the internet?

A. Demarcation point
B. North-South
C. Fibre Channel
D. Spine and leaf

Answer: B

NEW QUESTION 325
- (Exam Topic 3)

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

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

Answer: D

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

NEW QUESTION 329
- (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 333
- (Exam Topic 3)
Network traffic is being compromised by DNS poisoning every time a company's router is connected to the internet. The network team detects a non-authorized DNS server being assigned to the network clients and remediates the incident by setting a trusted DNS server, but the issue occurs again after internet exposure. Which of the following best practices should be implemented on the router?

A. Change the device's default password.
B. Disable router advertisement guard.
C. Activate control plane policing.
D. Disable unneeded network services.

Answer: A

NEW QUESTION 338
- (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 340

- (Exam Topic 3)
Which of the following connector types would be used to connect to the demarcation point and provide network access to a cable modem?

A. F-type
B. RJ45
C. LC
D. RJ11

Answer: A

Explanation:
An F-type connector is a type of coaxial connector that is commonly used to connect a cable modem to the demarcation point, which is the point at which the cable provider's network ends and the customer's network begins. The F-type connector is a threaded connector that is typically used for television, cable modem, and satellite antenna connections.

NEW QUESTION 341
- (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 343
- (Exam Topic 3)
A network administrator determines that even when optimal wireless coverage is configured, the network users still report constant disconnections After troubleshooting, the administrator determines that moving from one location to another causes the disconnection Which of the following settings should provide better network stability?

A. Client association timeout
B. RSSl roaming threshold
C. RF attenuation ratio
D. EIRP power setting

Answer: B

Explanation:
In this case, the most likely cause of the constant disconnections when moving from one location to another is likely due to a problem with the roaming functionality of the wireless network. The setting that would likely provide better network stability in this situation is the RSSI roaming threshold, which determines the signal strength required for a client device to remain connected to the wireless network. If the roaming threshold is set too low, the client device may disconnect and reconnect to the network too frequently as it moves between different access points. On the other hand, if the threshold is set too high, the client device may not roam to a new access point when necessary, leading to a loss of connectivity. Adjusting the RSSI roaming threshold to an appropriate value may help to improve the stability of the wireless network in this situation.

NEW QUESTION 346
- (Exam Topic 3)
A company's data center is hosted at its corporate office to ensure greater control over the security of sensitive data. During times when there are increased workloads, some of the company’s non-sensitive data is shifted to an external cloud provider. Which of the following cloud deployment models does this describe?

A. Hybrid
B. Community
C. Public
D. Private

Answer: A

NEW QUESTION 347
- (Exam Topic 3)
A WAN technician reviews activity and identifies newly installed hardware that is causing outages over an eight-hour period. Which of the following should be considered FIRST?

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

Answer: D

NEW QUESTION 351
- (Exam Topic 3)
An office area contains two PoE-enabled WAPs. After the area was remodeled, new cable uplinks were installed in the ceiling above the fluorescent lights. However, after the WAPs were reconnected, users reported slowness and application errors. An intern reviewed the network and discovered a lot of CRC errors. A network engineer reviewed the intern's work and realized UTP cabling was used. Which of the following is the MOST likely cause of the CRC errors?

A. Insufficient power at the antennas
B. PoE and UTP incompatibility
C. Electromagnetic interference
D. Wrong cable pinout

Answer: C

Explanation:
"EMI is a problem when cables are installed near electrical devices, such as air conditioners or fluorescent light fixtures. If a network medium is placed close enough to such a device, the signal within the cable might become corrupt. Network media vary in their resistance to the effects of EMI. Standard unshielded twisted-pair (UTP) cable is susceptible to EMI, whereas fiber cable, with its light transmissions, is resistant to EMI. When deciding on a particular medium, consider where it will run and the impact EMI can have on the installation."

NEW QUESTION 355
- (Exam Topic 3)
An engineer is designing a network topology for a company that maintains a large on-premises private cloud. A design requirement mandates internet-facing hosts to be partitioned off from the internal LAN and internal server IP ranges. Which Of the following defense strategies helps meet this requirement?

A. Implementing a screened subnet
B. Deploying a honeypot
C. Utilizing network access control
D. Enforcing a Zero Trust model

Answer: A

Explanation:
A screened subnet is a network segment that is isolated from both the internal LAN and the Internet by firewalls. A screened subnet can be used to host internet-facing hosts such as web servers, email servers, or DNS servers. A screened subnet provides an additional layer of security and prevents direct access to the internal network from the Internet.
References: Network+ Study Guide Objective 3.1: Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 357
- (Exam Topic 3)
Which of the following is a security flaw in an application or network?

A. A threat
B. A vulnerability
C. An exploit
D. A risk

Answer: B

Explanation:
A vulnerability is a security flaw in an application or network that can be exploited by an attacker, allowing them to gain access to sensitive data or take control of the system. Vulnerabilities can range from weak authentication methods to unpatched software, allowing attackers to gain access to the system or data they would not otherwise be able to access. Exploits are programs or techniques used to take advantage of vulnerabilities, while threats are potential dangers, and risks are the likelihood of a threat becoming a reality.

NEW QUESTION 361
- (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 365
- (Exam Topic 3)
While setting up a new workstation, a technician discovers that the network connection is only 100 full duplex (FD), although it is connected to a gigabit switch. While reviewing the interface information in the switch CLI, the technician notes the port is operating at IOOFD but Shows many RX and TX errors. The technician

moves the computer to another switchport and experiences the same issues.
Which of the following is MOST likely the cause of the low data rate and port errors?

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

Answer: B

NEW QUESTION 369
- (Exam Topic 3)
A company needs to virtualize a replica of its internal physical network without changing the logical topology and the way that devices behave and are managed.
Which of the following technologies meets this requirement?

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

Answer: A

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

NEW QUESTION 373
- (Exam Topic 3)
A WAN technician reviews activity and identifies newly installed hardware that is causing outages over an eight-hour period. Which of the following should be considered FIRST?

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

Answer: D

Explanation:
The most likely cause of outages due to newly installed hardware is a misconfiguration of the device settings. Therefore, the first step should be to review the device configuration and check for any errors or inconsistencies that might affect the WAN connectivity.
References: Network+ Study Guide Objective 2.1: Explain the importance of network documentation.

NEW QUESTION 378
- (Exam Topic 3)
A network administrator is reviewing the following metrics from a network management system regarding a switchport. The administrator suspects an issue because users are calling in regards to the switchport's performance:

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

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

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

Answer: A

NEW QUESTION 381
- (Exam Topic 3)
Which of the following attacks, if successful, would provide a malicious user who is connected to an isolated guest network access to the corporate network?

A. VLAN hopping
B. On-path attack
C. IP spoofing
D. Evil twin

Answer: A

Explanation:
The attack which, if successful, would provide a malicious user who is connected to an isolated guest network access to the corporate network is VLAN hopping. VLAN hopping is an attack technique which involves tricking a switch into sending traffic from one VLAN to another. This is done by sending specially crafted packets, which force the switch to send traffic from one VLAN to another, thus allowing the malicious user to gain access to the corporate network.
VLAN hopping is an attack technique which involves tricking a switch into sending traffic from one VLAN to another. This is done by sending specially crafted packets, which force the switch to send traffic from one VLAN to another, thus allowing the malicious user to gain access to the corporate network. According to the CompTIA Network+ N10-008 Exam Guide VLAN hopping is a type of attack that is used to gain access to network resources that are not meant to be accessible by a user on a guest network.

NEW QUESTION 385
- (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 390
- (Exam Topic 3)
Logs show an unauthorized IP address entering a secure part of the network every night at 8:00 pm. The network administrator is concerned that this IP address will cause an issue to a critical server and would like to deny the IP address at the edge of the network. Which of the following solutions would address these concerns?

A. Changing the VLAN of the web server
B. Changing the server's IP address
C. Implementing an ACL
D. Instating a rule on the firewall connected to the web server

Answer: D

NEW QUESTION 393
- (Exam Topic 3)
Which of the following OSI model layers is where a technician would view UDP information?

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

Answer: D

NEW QUESTION 397
- (Exam Topic 3)
Which of the following must be functioning properly in order for a network administrator to create an accurate timeline during a troubleshooting process?

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

Answer: A

NEW QUESTION 400
- (Exam Topic 3)
A technician is investigating why a PC cannot reach a file server with the IP address 192.168.8.129. Given the following TCP/IP network configuration:

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

Which of the following configurations on the PC is incorrect?

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

Answer: C

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

NEW QUESTION 404
- (Exam Topic 3)
Which of the following architectures is used for FTP?

A. Client-server
B. Service-oriented
C. Connection-oriented
D. Data-centric

Answer: A

Explanation:
FTP (File Transfer Protocol) is a client-server based protocol, meaning that the two computers involved communicate with each other in a request-response pattern. The client sends a request to the server and the server responds with the requested data. This type of architecture is known as client-server, and it is used for many different types of applications, including FTP. Other architectures, such as service-oriented, connection-oriented, and data-centric, are not used for FTP.

NEW QUESTION 407
- (Exam Topic 3)
To access production applications and data, developers must first connect remotely to a different server From there, the developers are able to access production data Which of the following does this BEST represent?

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

Answer: E

NEW QUESTION 411
- (Exam Topic 3)
A technician is trying to install a VolP phone, but the phone is not turning on. The technician checks the cable gong from the phone to the switch, and the cable is good. Which of the following actions IS needed for this phone to work?

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

Answer: A

NEW QUESTION 414
- (Exam Topic 3)
A network administrator is preparing answers for an annual risk assessment that is required for compliance purposes. Which of the following would be an example of an internal threat?

A. An approved vendor with on-site offices
B. An infected client that pulls reports from the firm
C. A malicious attacker from within the same country
D. A malicious attacker attempting to socially engineer access into corporate offices

Answer: A

Explanation:
Insider threat= insider threat is defined as the threat that an employee or a contractor will use his or her authorized access, wittingly or unwittingly, to do harm

NEW QUESTION 417
- (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 421
- (Exam Topic 3)
A network engineer needs to pass both data and telephony on an access port. Which or the following features should be configured to meet this requirement?

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

Answer: A

NEW QUESTION 422
- (Exam Topic 3)
A network engineer is monitoring a fiber uplink to a remote office and notes the uplink has been operating at 100% capacity for a long duration. Which of the following performance metrics is MOST likely to be impacted with sustained link saturation?

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

Answer: A

Explanation:
When a fiber uplink is operating at 100% capacity for an extended period of time, it can cause sustained link saturation. This can impact the network's performance by increasing latency. Latency is the time it takes for a packet to travel from the source to its destination. When there is link saturation, packets may have to wait in a queue before being transmitted, which increases the time it takes for them to reach their destination. As a result, users may experience delays or timeouts when accessing network resources.
Other metrics such as jitter, speed, and bandwidth are also important, but they are not as directly impacted by sustained link saturation as latency.

NEW QUESTION 423
- (Exam Topic 3)
Users in a branch can access an In-house database server, but II is taking too long to fetch records. The analyst does not know whether the Issue is being caused by network latency. Which of the following will the analyst MOST likely use to retrieve the metrics that are needed to resolve this issue?

A. SNMP
B. Link state
C. Syslog
D. QoS
E. Traffic shaping

Answer: A

NEW QUESTION 424
- (Exam Topic 3)
An engineer was asked to update an MX record for an upcoming project. Which of the following server types is MOST likely to be in scope for the project?

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

Answer: A

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

NEW QUESTION 428
- (Exam Topic 3)
Which of the following is the primary function of the core layer of the three-tiered model?

A. Routing
B. Repeating
C. Bridging
D. Switching

Answer: A

Explanation:
https://www.omnisecu.com/cisco-certified-network-associate-ccna/three-tier-hierarchical-network-model.php Core Layer consists of biggest, fastest, and most expensive routers with the highest model numbers and Core Layer is considered as the back bone of networks. Core Layer routers are used to merge geographically separated networks. The Core Layer routers move information on the network as fast as possible. The switches operating at core layer switches packets as fast as possible.

NEW QUESTION 429
- (Exam Topic 3)
Which of the following topologies requires me MOST connections when designing a network?

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

Answer: A

NEW QUESTION 434
- (Exam Topic 3)
A technician notices that equipment is being moved around and misplaced in the server room, even though the room has locked doors and cabinets. Which of the following would be the BEST solution to identify who is responsible?

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

Answer: B

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

NEW QUESTION 439
.....

Relate Links

100% Pass Your N10-009 Exam with Exambible Prep Materials

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

Contact us

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

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