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

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

Answer: A

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

NEW QUESTION 3
- (Exam Topic 1)
A technician is installing a high-density wireless network and wants to use an available frequency that supports the maximum number of channels to reduce interference. Which of the following standard 802.11 frequency ranges should the technician look for while reviewing WAP specifications?

A. 2.4GHz
B. 5GHz
C. 6GHz
D. 900MHz

Answer: B

Explanation:
* 802.11 a/b/g/n/ac wireless networks operate in two frequency ranges: 2.4 GHz and 5 GHz. The 5 GHz frequency range supports more channels than the 2.4 GHz frequency range, making it a better choice for high-density wireless networks.
References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 4
- (Exam Topic 1)
A workstation is configured with the following network details:

IP address	Subnet mask	Default gateway
10.1.2.23	10.1.2.0/27	10.1.2.1

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

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

Answer: D

Explanation:
The software on the workstation should be configured to send the query to 10.1.2.255, which is the local subnet broadcast address. A broadcast address is a

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

NEW QUESTION 5
- (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 6
- (Exam Topic 1)
A technician is installing a new fiber connection to a network device in a datacenter. The connection from the device to the switch also traverses a patch panel connection. The chain of connections is in the following order:
Device
LC/LC patch cable Patch panel
Cross-connect fiber cable Patch panel
LC/LC patch cable Switch
The connection is not working. The technician has changed both patch cables with known working patch cables. The device had been tested and was working properly before being installed. Which of the following is the MOST likely cause of the issue?

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

Answer: A

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

NEW QUESTION 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 ports is commonly used by VoIP phones?

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

Answer: D

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

NEW QUESTION 9
- (Exam Topic 1)
A network administrator is designing a new datacenter in a different region that will need to communicate to the old datacenter with a secure connection. Which of the following access methods would provide the BEST security for this new datacenter?

A. Virtual network computing
B. Secure Socket Shell
C. In-band connection
D. Site-to-site VPN

Answer: D

Explanation:
Site-to-site VPN provides the best security for connecting a new datacenter to an old one because it creates a secure tunnel between the two locations, protecting data in transit. References: CompTIA Network+ Certification Study Guide, Chapter 5: Network Security.

NEW QUESTION 10
- (Exam Topic 1)
A company hired a technician to find all the devices connected within a network. Which of the following software tools would BEST assist the technician in completing this task?

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

Answer: A

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

NEW QUESTION 10
- (Exam Topic 1)
An engineer is configuring redundant network links between switches. Which of the following should the engineer enable to prevent network stability issues?

A. 802.1Q
B. STP
C. Flow control
D. CSMA/CD

Answer: B

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

NEW QUESTION 11
- (Exam Topic 1)
Which of the following routing protocols is used to exchange route information between public autonomous systems?

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

Answer: B

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

NEW QUESTION 14
- (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 15
- (Exam Topic 1)
Client devices cannot enter a network, and the network administrator determines the DHCP scope is exhausted. The administrator wants to avoid creating a new DHCP pool. Which of the following can the administrator perform to resolve the issue?

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

Answer: D

Explanation:
To resolve the issue of DHCP scope exhaustion without creating a new DHCP pool, the administrator can reduce the lease time. By decreasing the lease time, the IP addresses assigned by DHCP will be released back to the DHCP scope more quickly, allowing them to be assigned to new devices.
References:
- CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.3: Given a scenario, implement and configure the appropriate addressing schema.
- https://www.networkcomputing.com/data-centers/10-tips-optimizing-dhcp-performance

NEW QUESTION 16
- (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 17
- (Exam Topic 1)
A systems administrator needs to improve WiFi performance in a densely populated office tower and use the latest standard. There is a mix of devices that use 2.4 GHz and 5 GHz. Which of the following should the
systems administrator select to meet this requirement?

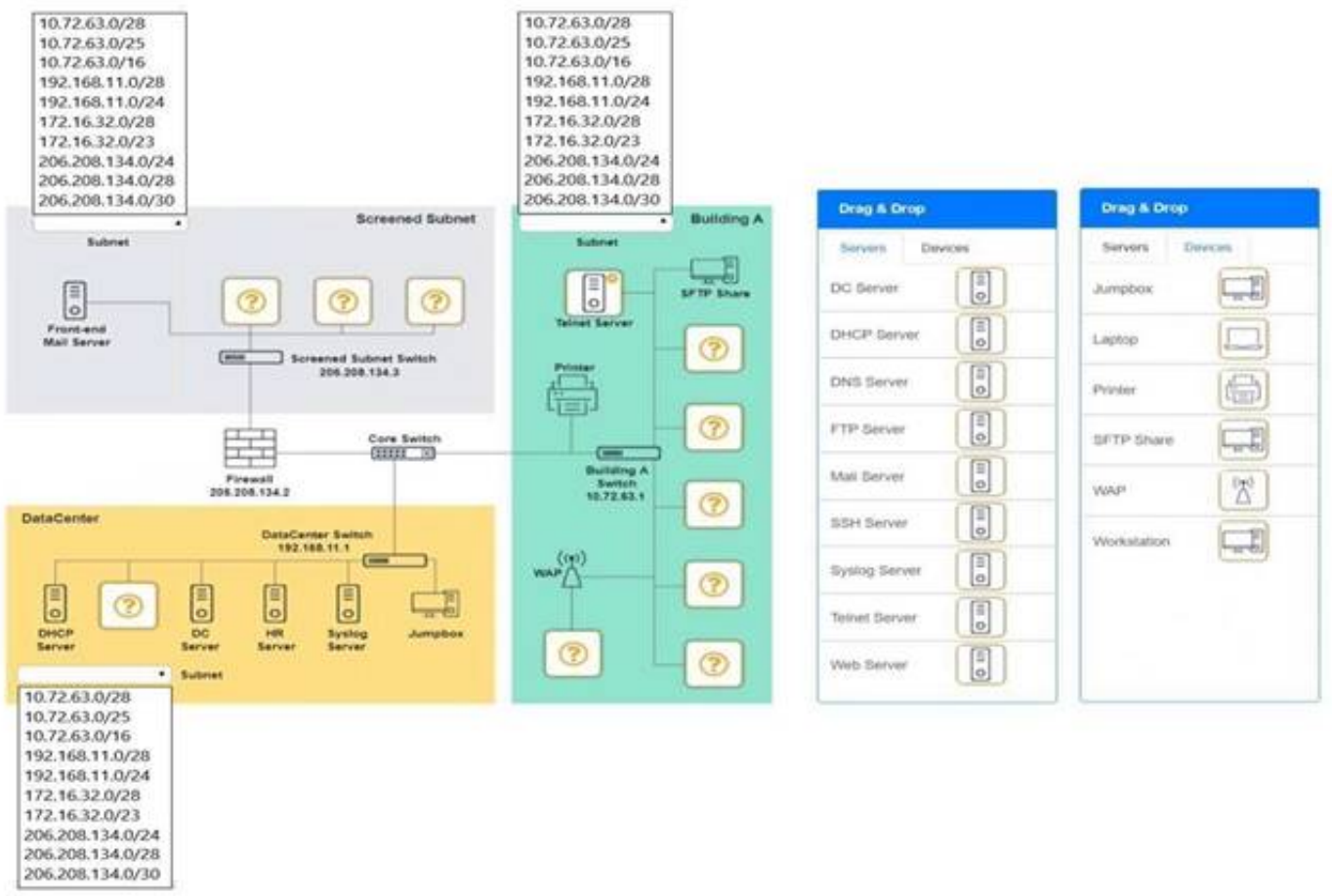
A. 802.11ac
B. 802.11ax
C. 802.11g
D. 802.11n

Answer: B

Explanation:
* 802.11 ax is the latest WiFi standard that improves WiFi performance in densely populated environments and supports both 2.4 GHz and 5 GHz bands. 802.11ac is the previous standard that only supports 5 GHz band. 802.11g and 802.11n are older standards that support 2.4 GHz band only or both bands respectively.
References:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0),
https://www.techtarget.com/searchnetworking/tip/Whats-the-difference-between-80211ax-vs-80211ac

NEW QUESTION 18
- (Exam Topic 1)
You are tasked with verifying the following requirements are met in order to ensure network security. Requirements:
Datacenter
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic Building A

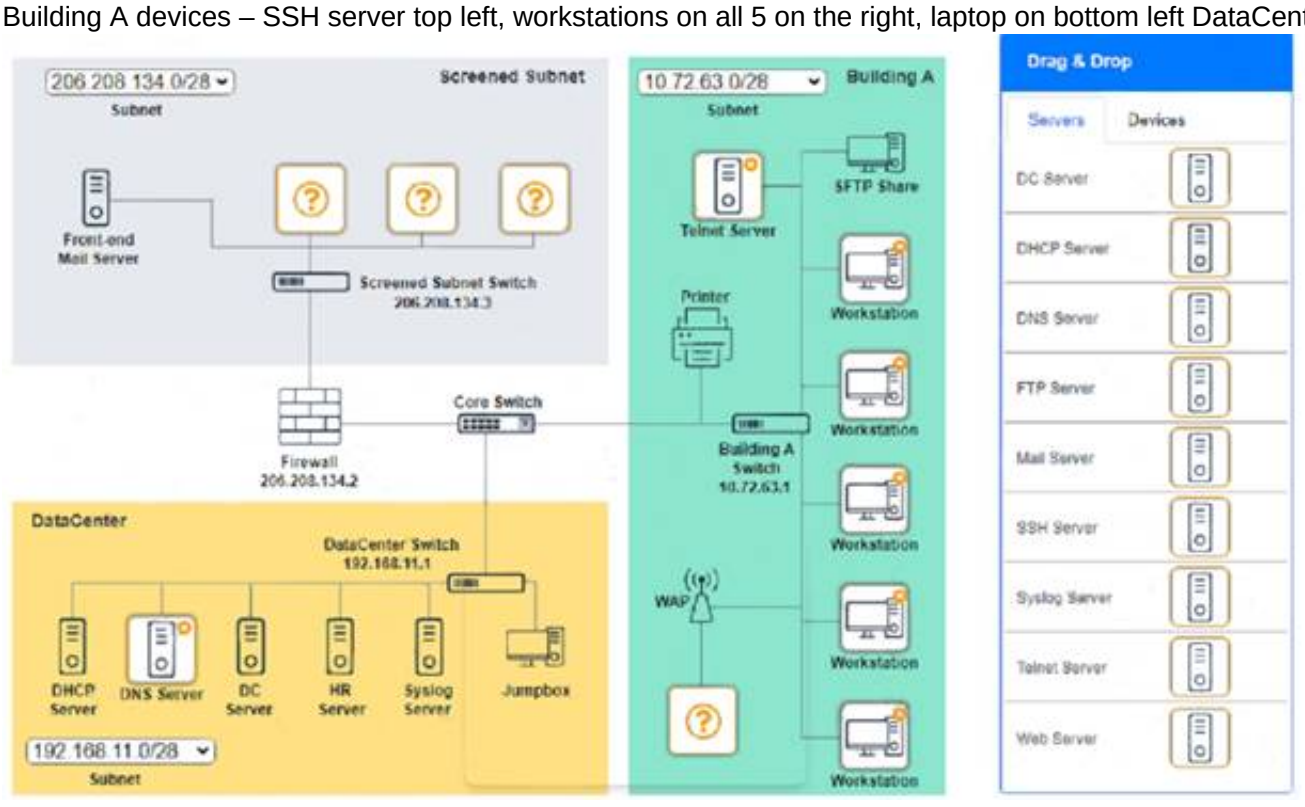
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
Provide devices to support 5 additional different office users
Add an additional mobile user
Replace the Telnet server with a more secure solution Screened subnet
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
Provide a server to handle external 80/443 traffic Provide a server to handle port 20/21 traffic INSTRUCTIONS
Drag and drop objects onto the appropriate locations. Objects can be used multiple times and not all placeholders need to be filled.
Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



A. Mastered
B. Not Mastered

Answer: A

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



NEW QUESTION 21
- (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 22
- (Exam Topic 1)
A network engineer configured new firewalls with the correct configuration to be deployed to each remote branch. Unneeded services were disabled, and all firewall rules were applied successfully. Which of the following should the network engineer perform NEXT to ensure all the firewalls are hardened successfully?

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

Answer: C

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

NEW QUESTION 27
- (Exam Topic 1)
The following configuration is applied to a DHCP server connected to a VPN concentrator:

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

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

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

Answer: A

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

NEW QUESTION 32
- (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 36
- (Exam Topic 2)
A network technician needs to correlate security events to analyze a suspected intrusion. Which of the following should the technician use?

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

Answer: D

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

NEW QUESTION 38
- (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 43
- (Exam Topic 2)
A network administrator is reviewing interface errors on a switch. Which of the following indicates that a switchport is receiving packets in excess of the configured MTU?

A. CRC errors
B. Giants
C. Runts
D. Flooding

Answer: B

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

NEW QUESTION 46
- (Exam Topic 2)
Which of the following protocol types describes secure communication on port 443?

A. ICMP
B. UDP
C. TCP
D. IP

Answer: C

Explanation:
TCP is the protocol type that describes secure communication on port 443. TCP (Transmission Control Protocol) is a connection-oriented protocol that provides reliable and ordered delivery of data packets over an IP network. TCP uses port numbers to identify different applications or services on a device. Port 443 is the default port for HTTPS (Hypertext Transfer Protocol Secure), which is an extension of HTTP that uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security) encryption to protect data in transit between a web server and a web browser. References:
https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

NEW QUESTION 48
- (Exam Topic 2)
A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the AP utilize?

A. Omni
B. Directional
C. Yagi
D. Parabolic

Answer: A

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

NEW QUESTION 53
- (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 57
- (Exam Topic 2)
Which of the following policies is MOST commonly used for guest captive portals?

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

Answer: A

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

NEW QUESTION 61
- (Exam Topic 2)
A network technician is investigating an issue with handheld devices in a warehouse. Devices have not been connecting to the nearest APs, but they have been connecting to an AP on the far side of the warehouse. Which of the following is the MOST likely cause of this issue?

A. The nearest APs are configured for 802.11g.
B. An incorrect channel assignment is on the nearest APs.
C. The power level is too high for the AP on the far side.
D. Interference exists around the AP on the far side.

Answer: C

Explanation:
The power level is a setting that determines how strong the wireless signal is from an access point (AP). If the power level is too high for an AP on the far side of a warehouse, it can cause interference and overlap with other APs on the same channel or frequency. This can result in handheld devices not connecting to the nearest APs, but connecting to the AP on the far side instead. A technician should adjust the power level of the AP on the far side to reduce interference and improve connectivity. References:
https://www.comptia.org/blog/what-is-power-level

NEW QUESTION 63
- (Exam Topic 2)
Which of the following protocols will a security appliance that is correlating network events from multiple devices MOST likely rely on to receive event messages?

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

Answer: A

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

NEW QUESTION 66
- (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 69
- (Exam Topic 2)
A company requires a disaster recovery site to have equipment ready to go in the event of a disaster at its main datacenter. The company does not have the budget to mirror all the live data to the disaster recovery site. Which of the following concepts should the company select?

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

Answer: C

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

NEW QUESTION 74
- (Exam Topic 2)
Which of the following OSI model layers is where conversations between applications are established, coordinated, and terminated?

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

Answer: A

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

NEW QUESTION 75
- (Exam Topic 2)
During the security audit of a financial firm the Chief Executive Officer (CEO) questions why there are three employees who perform very distinct functions on the server. There is an administrator for creating users another for assigning the users lo groups and a third who is the only administrator to perform file rights assignment Which of the following mitigation techniques is being applied'

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

Answer: B

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

NEW QUESTION 79
- (Exam Topic 2)
Which of the following is MOST commonly used to address CVEs on network equipment and/or operating systems?

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

Answer: C

Explanation:

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

NEW QUESTION 82
- (Exam Topic 2)
A user recently made changes to a PC that caused it to be unable to access websites by both FQDN and IP Local resources, such as the file server remain accessible. Which of the following settings did the user MOST likely misconfigure?

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

Answer: B

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

NEW QUESTION 83
- (Exam Topic 2)
Which of the following would be used to expedite MX record updates to authoritative NSs?

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

Answer: D

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

NEW QUESTION 84
- (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 89
- (Exam Topic 3)
Network connectivity in an extensive forest reserve was achieved using fiber optics. A network fault was detected, and now the repair team needs to check the integrity of the fiber cable. Which of me following actions can reduce repair time?

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

Answer: C

NEW QUESTION 92
- (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 96
- (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 101
- (Exam Topic 3)
A systems operator is granted access to a monitoring application, configuration application, and timekeeping application. The operator is denied access to the financial and project management applications by the system's security configuration. Which of the following BEST describes the security principle in use?

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

Answer: D

NEW QUESTION 102
- (Exam Topic 3)
A network technician is troubleshooting an area where the wireless connection to devices is poor. The technician theorizes that the signal-to-noise ratio in the area is causing the issue. Which of the following should the technician do NEXT?

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

Answer: D

NEW QUESTION 106
- (Exam Topic 3)
Due to a surge in business, a company is onboarding an unusually high number of salespeople. The salespeople are assigned desktops that are wired to the network. The last few salespeople to be onboarded are able to access corporate materials on the network but not sales-specific resources. Which of the following is MOST likely the cause?

A. The switch was configured with port security.
B. Newly added machines are running into DHCP conflicts.
C. The IPS was not configured to recognize the new users.
D. Recently added users were assigned to the wrong VLAN

Answer: D

NEW QUESTION 109
- (Exam Topic 3)
Which of the following can be used to limit the ability of devices to perform only HTTPS connections to an internet update server without exposing the devices to the public internet?

A. Allow connections only to an internal proxy server.
B. Deploy an IDS system and place it in line with the traffic.
C. Create a screened network and move the devices to it.
D. Use a host-based network firewall on each device.

Answer: A

Explanation:
An internal proxy server is a server that acts as an intermediary between internal devices and external servers on the internet. An internal proxy server can be used to limit the ability of devices to perform only HTTPS connections to an internet update server by filtering and forwarding the requests and responses based on predefined rules or policies. An internal proxy server can also prevent the devices from being exposed to the public internet by hiding their IP addresses and providing a layer of security and privacy.

NEW QUESTION 112
- (Exam Topic 3)
A user from a remote office is reporting slow file transfers. Which of the following tools will an engineer MOST likely use to get detailed measurement data?

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

Answer: B

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

NEW QUESTION 113
- (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 118
- (Exam Topic 3)
A user reports that a new VoIP phone works properly but the computer that is connected to the phone cannot access any network resources. Which of the following MOST Likely needs to be configured correctly to provide network connectivity to the computer?

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

Answer: D

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

NEW QUESTION 119
- (Exam Topic 3)
Switch 3 was recently added lo an existing stack to extend connectivity to various parts of the network. After the update, new employees were not able to print to the main networked copiers from then workstations. Following are the port configurations for the switch stack in question:

Switch 1:

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

Switch 2:

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

Switch 3:

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

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

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

Answer: AE

NEW QUESTION 124
- (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 125
- (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 127
- (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 131
- (Exam Topic 3)
A company cell phone was stolen from a technician's vehicle. The cell phone has a passcode, but it contains sensitive information about clients and vendors. Which of the following should also be enabled?

A. Factory reset
B. Autolock
C. Encryption
D. Two-factor authentication

Answer: C

NEW QUESTION 134
- (Exam Topic 3)
A technician is trying to determine whether an LACP bundle is fully operational. Which of the following commands will the technician MOST likely use?

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

Answer: A

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

NEW QUESTION 137
- (Exam Topic 3)
ARP spoofing would normally be a part of:

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

Answer: A

NEW QUESTION 142
- (Exam Topic 3)
A network technician is selecting a replacement for a damaged fiber cable that goes directly to an SFP transceiver on a network switch. Which of the following cable connectors should be used?

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

Answer: C

NEW QUESTION 144
- (Exam Topic 3)
A large metropolitan city is looking to standardize the ability tor police department laptops to connect to the city government's VPN The city would like a wireless solution that provides the largest coverage across the city with a minimal number of transmission towers Latency and overall bandwidth needs are not high priorities. Which of the following would BEST meet the city's needs?

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

Answer: B

NEW QUESTION 146

- (Exam Topic 3)
Which of the following is considered a physical security detection device?

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

Answer: A

NEW QUESTION 149
- (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 154
- (Exam Topic 3)
Which of the following can be used to decrease latency during periods of high utilization of a firewall?

A. Hot site
B. NIC teaming
C. HA pair
D. VRRP

Answer: B

Explanation:
NIC Teaming, also known as load balancing and failover (LBFO), allows multiple network adapters on a computer to be placed into a team for the following purposes: (https://www.bing.com/search?q=what+is+nic+teaming+used+for%3F&form=QBLH&sp=-1&pq=what+is+nic

NEW QUESTION 157
- (Exam Topic 3)
An ISP is unable to provide services to a user in a remote area through cable and DSL. Which of the following is the NEXT best solution to provide services without adding external infrastructure?

A. Fiber
B. Leased line
C. Satellite
D. Metro optical

Answer: C

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

NEW QUESTION 161
- (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 165

- (Exam Topic 3)
An AP uses a 98ft (30m) Cat 6 cable to connect to an access switch. The cable is wired through a duct close to a three-phase motor installation. Anytime the three-phase is turned on, all users connected to the switch experience high latency on the network. Which Of the following is MOST likely the cause Of the issue?

A. Interference
B. Attenuation
C. Open circuit
D. Short circuit

Answer: A

Explanation:
Interference is a phenomenon that occurs when unwanted signals or noise affect the transmission or reception of data signals on a network. Interference can cause network issues such as high latency, low throughput, packet loss, or errors. Interference can be caused by various sources, such as electromagnetic fields, radio waves, power lines, or electrical devices. In this scenario, the three-phase motor installation is a source of interference that affects the Cat 6 cable that connects the AP to the access switch. The cable is wired through a duct close to the motor installation, which exposes it to the electromagnetic fields generated by the motor. Anytime the motor is turned on, the interference causes high latency for all users connected to the switch.

NEW QUESTION 170
- (Exam Topic 3)
A network engineer is concerned about VLAN hopping happening on the network. Which of the following should the engineer do to address this concern?

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

Answer: B

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

NEW QUESTION 172
- (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 175
- (Exam Topic 3)
A network administrator is setting up a new phone system and needs to define the location where VoIP phones can download configuration files. Which of the following DHCP services can be used to accomplish this task?

A. Scope options
B. Exclusion ranges
C. Lease time
D. Relay

Answer: A

Explanation:
To define the location where VoIP phones can download configuration files, the network administrator can use scope options within the Dynamic Host Configuration Protocol (DHCP) service. Scope options are a set of values that can be configured within a DHCP scope, which defines a range of IP addresses that can be leased to clients on a network. One of the scope options that can be configured is the option for the location of the configuration file server, which specifies the URL or IP address of the server where the configuration files can be downloaded.
https://pbxbook.com/voip/dhcpcfg.html

NEW QUESTION 180
- (Exam Topic 3)
A newly installed VoIP phone is not getting the DHCP IP address it needs to connect to the phone system. Which of the following tasks needs to be completed to allow the phone to operate correctly?

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

Answer: A

NEW QUESTION 181
- (Exam Topic 3)
An IT technician installs five old switches in a network. In addition to the low port rates on these switches, they also have improper network configurations. After three hours, the network becomes overwhelmed by continuous traffic and eventually shuts down. Which Of the following is causing the issue?

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

Answer: A

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

NEW QUESTION 183
- (Exam Topic 3)
A technician is configuring a static IP address on a new device in a newly created subnet. The work order specifies the following requirements:
• The IP address should use the highest address available in the subnet.
• The default gateway needs to be set to 172.28.85.94.
• The subnet mask needs to be 255.255.255.224.
Which of the following addresses should the engineer apply to the device?

A. 172.28.85.93
B. 172.28.85.95
C. 172.28.85.254
D. 172.28.85.255

Answer: A

Explanation:
https://www.tunnelsup.com/subnet-calculator/ IP Address: 172.28.85.95/27
Netmask: 255.255.255.224
Network Address: 172.28.85.64
Usable Host Range: 172.28.85.65 - 172.28.85.94
Broadcast Address: 172.28.85.95

NEW QUESTION 184
- (Exam Topic 3)
A corporation is looking for a method to secure all traffic between a branch office and its data center in order to provide a zero-touch experience for all staff members who work there. Which of the following would BEST meet this requirement?

A. Site-to-site VPN
B. VNC
C. Remote desktop gateway
D. Virtual LANs

Answer: A

Explanation:
A site-to-site VPN is a method that creates a secure and encrypted connection between two internet gateways, such as routers or firewalls, that belong to different networks1. A site-to-site VPN can secure all traffic between a branch office and its data center by creating a virtual tunnel that protects the data from interception or tampering. A site-to-site VPN can also provide a zero-touch experience for all staff members who work there, as they do not need to install any software or configure any settings on their devices to access the data center resources. They can simply use their local network as if they were physically connected to the data center network.
VNC (Virtual Network Computing) is a method that allows remote access and control of a computer's desktop from another device over a network2. VNC can enable staff members to work remotely by accessing their office computers from their home computers or mobile devices. However, VNC does not secure all traffic between a branch office and its data center, as it only works at the application layer and does not encrypt the network layer. VNC also does not provide a zero-touch experience for staff members, as they need to install software and configure settings on both the host and the client devices.
Remote desktop gateway is a method that allows remote access and control of a computer's desktop from another device over a network using the Remote Desktop Protocol (RDP). Remote desktop gateway can also enable staff members to work remotely by accessing their office computers from their home computers or mobile devices. However, remote desktop gateway does not secure all traffic between a branch office and its data center, as it only works at the application layer and does not encrypt the network layer. Remote desktop gateway also does not provide a zero-touch experience for staff members, as they need to install software and configure settings on both the host and the client devices.
Virtual LANs (VLANs) are methods that create logical subdivisions of a physical network based on criteria such as function, department, or security level. VLANs can improve network performance, security, and management by reducing broadcast domains, isolating traffic, and enforcing policies. However, VLANs do not secure all traffic between a branch office and its data center, as they only work at the data link layer and do not encrypt the network layer. VLANs also do not provide a zero-touch experience for staff members, as they need to configure settings on their network devices to join or leave a VLAN.

NEW QUESTION 185
- (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 188
- (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 190
- (Exam Topic 3)
A device is connected to a managed Layer 3 network switch. The MAC address of the device is known, but the static IP address assigned to the device is not. Which of the following features of a Layer 3 network switch should be used to determine the IPv4 address of the device?

A. MAC table
B. Neighbor Discovery Protocol
C. ARP table
D. IPConfig
E. ACL table

Answer: C

Explanation:
The ARP table is a database that is used by a device to map MAC addresses to their corresponding IP addresses. When a device sends a packet to another device on the same network, it uses the MAC address of the destination device to deliver the packet. The ARP table allows the device to determine the IP address of the destination device based on its MAC address.

NEW QUESTION 195
- (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 198
- (Exam Topic 3)
Which of the following issues are present with RIPv2? (Select TWO).

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

Answer: BC

Explanation:
The disadvantages of RIP (Routing Information Protocol) include the following.
---Outdated, insecure, and slow. This is your parents' protocol. It was a thing before the Web was born.
---The more well-known problem of the 15 hop limitation in which data must travel
---Convergence time is terrible for information propagation in a network
---Metrics. It determines the number of hops from source to destination, and gives no regard to other factors when determining the best path for data to travel
---Overhead. A good example would be routing tables. These are broadcast at half-minute intervals to other routers regardless of whether the data has changed or not. It's essentially like those old cartoons where the
town guard in the walled city cries out, '10 o' the clock and all is well!'.
RIPv2 introduced more security and reduced broadcast traffic, which is relevant for some available answers here.

NEW QUESTION 199
- (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 202
- (Exam Topic 3)
A false camera is installed outside a building to assist with physical security. Which of the following is the device assisting?

A. Detection
B. Recovery
C. Identification
D. Prevention

Answer: A

NEW QUESTION 204
- (Exam Topic 3)
A network administrator is troubleshooting a connectivity performance issue. As part of the troubleshooting process, the administrator performs a traceout from the client to the server, and also from the server to the client. While comparing the outputs, the administrator notes they show different hops between the hosts. Which of the following BEST explains these findings?

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

Answer: C

NEW QUESTION 207
- (Exam Topic 3)
A network administrator is designing a wireless network. The administrator must ensure a rented office space has a sufficient signal. Reducing exposure to the wireless network is important, but it is secondary to the primary objective. Which of the following would MOST likely facilitate the correct accessibility to the Wi-Fi network?

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

Answer: B

NEW QUESTION 212
- (Exam Topic 3)
An IT administrator received an assignment with the following objectives
• Conduct a total scan within the company's network tor all connected hosts
• Detect all the types of operating systems running on all devices
• Discover all services offered by hosts on the network
• Find open ports and detect security risks.
Which of the following command-line tools can be used to achieve these objectives?

A. nmap
B. arp

C. netatat
D. tcpdump

Answer: A

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

NEW QUESTION 217
- (Exam Topic 3)
The power company notifies a network administrator that it will be turning off the power to the building over the weekend. Which of the following is the BEST solution to prevent the servers from going down?

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

Answer: A

NEW QUESTION 222
- (Exam Topic 3)
A small office has a wireless network with several access points that are used by mobile devices. Users occasionally report that the wireless connection drops or becomes very slow. Reports confirm that this only happens when the devices are connected to the office wireless network. Which of the following is MOST likely the cause?

A. The configuration of the encryption protocol
B. Interference from other devices
C. Insufficient bandwidth capacity
D. Duplicate SSIDs

Answer: B

Explanation:
Interference from other devices can cause wireless connection drops or slow performance. This can happen when devices use the same or overlapping frequency channels as the wireless network, such as cordless phones, microwaves, Bluetooth devices, etc. To avoid interference, it is recommended to use non-overlapping channels and avoid placing wireless access points near potential sources of interference. References: Network+ Study Guide Objective 2.1: Explain the purposes and use cases for advanced network devices. Subobjective: Wireless controllers.

NEW QUESTION 224
- (Exam Topic 3)
An engineer recently decided to upgrade the firmware on a router. During the upgrade, the help desk received calls about a network outage, and a critical ticket was opened. The network manager would like to create a policy to prevent this from happening in the future. Which of the following documents should the manager create?

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

Answer: A

NEW QUESTION 225
- (Exam Topic 3)
Which of the following records can be used to track the number of changes on a DNS zone?

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

Answer: A

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

NEW QUESTION 226
- (Exam Topic 3)
A network administrator needs to monitor traffic on a specific port on a switch. Which of the following should the administrator configure to accomplish the task?

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

D. Media access control

Answer: C

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

NEW QUESTION 227
- (Exam Topic 3)
Which of the following protocols can be used to change device configurations via encrypted and authenticated sessions? (Select TWO).

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

Answer: BD

NEW QUESTION 229
- (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. RSSI 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 230
- (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 234
- (Exam Topic 3)
A corporate client is experiencing global system outages. The IT team has identified multiple potential underlying causes throughout the enterprise Each team member has been assigned an area to trouble shoot. Which of the following approaches is being used?

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

Answer: A

NEW QUESTION 239
- (Exam Topic 3)
Network users reported that a recent firmware upgrade to a firewall did not resolve the issue that prompted the upgrade. Which of the following should be performed NEXT?

A. Reopen the service ticket, request a new maintenance window, and roll back to the anterior firmware version.
B. Gather additional information to ensure users' concerns are not been caused by a different issue withsimilar symptoms.
C. Employ a divide-and-conquer troubleshooting methodology by engaging the firewall vendor's support.
D. Escalate the issue to the IT management team in order to negotiate a new SLA with the user's manager.

Answer: B

Explanation:
Before taking any further action, it is important to verify that the problem reported by the users is the same as the one that prompted the firmware upgrade. It is possible that the firmware upgrade did resolve the original issue, but a new or different issue has arisen with similar symptoms. By gathering additional information from the users, such as error messages, screenshots, logs, or network traces, the technician can confirm or rule out this possibility and avoid wasting time and resources on unnecessary steps.
Reopening the service ticket, requesting a new maintenance window, and rolling back to the anterior firmware version (A) is a possible option if the firmware upgrade did not resolve the original issue and caused more problems. However, this should not be done without first verifying that the users' concerns are related to the firmware upgrade and not a different issue.
Employing a divide-and-conquer troubleshooting methodology by engaging the firewall vendor's support © is another possible option if the technician needs assistance from the vendor to diagnose or resolve the issue. However, this should also not be done without first gathering additional information from the users to narrow down the scope of the problem and provide relevant details to the vendor.
Escalating the issue to the IT management team in order to negotiate a new SLA with the user's manager (D) is not a relevant option at this stage. An SLA (Service Level Agreement) is a contract that defines the expectations and responsibilities of both parties in terms of service quality, availability, performance, and response time. Negotiating a new SLA does not address the root cause of the issue or help to resolve it. Moreover, escalating an issue to management should only be done when all other options have been exhausted or when there is a significant impact or risk to the business.

NEW QUESTION 244
- (Exam Topic 3)
A technician is deploying a new SSID for an industrial control system. The control devices require the network to use encryption that employs TKIP and a symmetrical password to connect. Which of the following should the technician configure to ensure compatibility with the control devices?

A. WPA2-Enterprise
B. WPA-Enterprise
C. WPA-PSK
D. WPA2-PSK

Answer: C

Explanation:
"WPA uses Temporal Key Integrity Protocol (TKIP) for enhanced encryption. TKIP uses RC4 for the encryption algorithm, and the CompTIA Network+ exam may reference TKIP-RC4 in a discussion of wireless."
" WPA2 uses Counter Mode with Cipher Block Chaining Message Authentication Code
Protocol (CCMP) for integrity checking and Advanced Encryption Standard (AES) for encryption. On the Network+ exam, you might find this referenced as simply CCMP-AES"

NEW QUESTION 248
- (Exam Topic 3)
Users are reporting poor wireless performance in some areas of an industrial plant The wireless controller is measuring a tow EIRP value compared to me recommendations noted on me most recent site survey. Which of the following should be verified or replaced for the EIRP value to meet the site survey's specifications? (Select TWO).

A. AP transmit power
B. Channel utilization
C. Signal loss
D. Update ARP tables
E. Antenna gain
F. AP association time

Answer: AE

Explanation:
- AP transmit power: You should check if your APs have sufficient power output and adjust them if needed. You should also make sure they are not exceeding regulatory limits for your region.
- Antenna gain: You should check if your antennas have adequate gain for your coverage area and replace them if needed. You should also make sure they are aligned properly and not obstructed by any objects.

In the scenario described, the wireless controller is measuring a low EIRP value compared to the recommendations noted in the most recent site survey. EIRP is the combination of the power transmitted by the access point and the antenna gain. Therefore, to increase the EIRP value to meet the site survey's specifications, the administrator should verify or replace the AP transmit power (option A) and the antenna gain (option E). This can be achieved by adjusting the transmit power settings on the AP or by replacing the AP's antenna with one that has a higher gain

NEW QUESTION 251
- (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 255
- (Exam Topic 3)
A customer needs to distribute Ethernet to multiple computers in an office. The customer would like to use non-proprietary standards. Which of the following blocks does the technician need to install?

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

Answer: A

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

NEW QUESTION 259
- (Exam Topic 3)
Which of the following is a benefit of the spine-and-leaf network topology?

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

Answer: A

NEW QUESTION 264
- (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 269
- (Exam Topic 3)
A store owner would like to have secure wireless access available for both business equipment and patron use. Which of the following features should be configured to allow different wireless access through the same equipment?

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

Answer: D

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

NEW QUESTION 271
- (Exam Topic 3)
Which of the following connectors and terminations are required to make a Cat 6 cable that connects from a PC to a non-capable MDIX switch? (Select TWO).

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

Answer: AD

NEW QUESTION 274
- (Exam Topic 3)
A network technician 13 troubleshooting a network issue for employees who have reported Issues with speed when accessing a server in another subnet. The server is in another building that is 410ft (125m) away from the employees' building. The 10GBASE-T connection between the two buildings uses Cat 5e. Which of the following BEST explains the speed issue?

A. The connection type is not rated for that distance
B. A broadcast storm is occurring on the subnet.
C. The cable run has interference on it
D. The connection should be made using a Cat 6 cable

Answer: D

Explanation:
The 10GBASE-T connection between the two buildings uses Cat 5e, which is not rated for a distance of 410ft (125m). According to the CompTIA Network+ Study Manual, for 10GBASE-T connections, "Cat 5e is rated for up to 55m, Cat 6a is rated for 100m, and Cat 7 is rated for 150m." Therefore, the speed issue is likely due to the fact that the connection type is not rated for the distance between the two buildings. To resolve the issue, the technician should consider using a Cat 6a or Cat 7 cable to increase the distance the connection is rated for.

NEW QUESTION 275
- (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 278
- (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 281
- (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 284
.....

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/