CompTIA

Exam Questions N10-009

CompTIA Network+ Exam

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

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

Answer: D

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

NEW QUESTION 4
- (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 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 technician is connecting multiple switches to create a large network for a new office. The switches are unmanaged Layer 2 switches with multiple connections between each pair. The network is experiencing an extreme amount of latency. Which of the following is MOST likely occurring?

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

Answer: C

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

NEW QUESTION 8
- (Exam Topic 1)
A network administrator discovers that users in an adjacent building are connecting to the company's guest wireless network to download inappropriate material. Which of the following can the administrator do to MOST easily mitigate this issue?

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

Answer: A

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

NEW QUESTION 9
- (Exam Topic 1)
A technician is installing multiple UPS units in a major retail store. The technician is required to keep track of all changes to new and old equipment. Which of the following will allow the technician to record these changes?

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

Answer: A

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

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

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

Answer: A

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

NEW QUESTION 10
- (Exam Topic 1)
A technician is configuring a network switch to be used in a publicly accessible location. Which of the following should the technician configure on the switch to prevent unintended connections?

A. DHCP snooping
B. Geofencing
C. Port security
D. Secure SNMP

Answer: C

Explanation:
Port security is a feature that restricts input to a switch port by limiting and identifying MAC addresses of the devices allowed to access the port. This prevents unintended connections from unauthorized devices or spoofed MAC addresses. Port security can also be configured to take actions such as shutting down the port or sending an alert when a violation occurs. References:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0),
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-10/configuration_guide/se

NEW QUESTION 12
- (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 17
- (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 20
- (Exam Topic 1)
According to troubleshooting methodology, which of the following should the technician do NEXT after determining the most likely probable cause of an issue?

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

Answer: A

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

NEW QUESTION 25
- (Exam Topic 1)
Within the realm of network security, Zero Trust:

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

Answer: A

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

NEW QUESTION 29
- (Exam Topic 1)
A technician is deploying a new switch model and would like to add it to the existing network monitoring software. The technician wants to know what metrics can be gathered from a given switch. Which of the following should the technician utilize for the switch?

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

Answer: A

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

NEW QUESTION 32
- (Exam Topic 1)
A network device is configured to send critical events to a syslog server; however, the following alerts are not being received:
Severity 5 LINK-UPDOWN: Interface 1/1, changed state to down Severity 5 LINK-UPDOWN: Interface 1/3, changed state to down
Which of the following describes the reason why the events are not being received?

A. The network device is not configured to log that level to the syslog server
B. The network device was down and could not send the event
C. The syslog server is not compatible with the network device
D. The syslog server did not have the correct MIB loaded to receive the message

Answer: A

Explanation:
The reason why the alerts are not being received is that the network device is not configured to log that level to the syslog server. The severity level for the events may need to be adjusted in order for them to be sent to the syslog server. References: Network+ Certification Study Guide, Chapter 8: Network Troubleshooting

NEW QUESTION 34
- (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 35
- (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 39
- (Exam Topic 1)
A website administrator is concerned the company's static website could be defaced by hacktivists or used as a pivot point to attack internal systems. Which of the following should a network security administrator recommend to assist with detecting these activities?

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

Answer: A

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

NEW QUESTION 41
- (Exam Topic 1)
A network administrator walks into a datacenter and notices an unknown person is following closely. The administrator stops and directs the person to the security desk. Which of the following attacks did the network administrator prevent?

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

Answer: B

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

NEW QUESTION 45
- (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 48
- (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 51
- (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 54
- (Exam Topic 1)
A network administrator redesigned the positioning of the APs to create adjacent areas of wireless coverage. After project validation, some users still report poor connectivity when their devices maintain an association to a distanced AP. Which of the following should the network administrator check FIRST?

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

Answer: A

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

NEW QUESTION 55
- (Exam Topic 1)
Which of the following would MOST likely be used to review previous upgrades to a system?

A. Business continuity plan
B. Change management
C. System life cycle
D. Standard operating procedures

Answer: B

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

NEW QUESTION 57
- (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 60
- (Exam Topic 1)
A network technician is manually configuring the network settings for a new device and is told the network block is 192.168.0.0/20. Which of the following subnets should the technician use?

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

Answer: C

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

NEW QUESTION 63
- (Exam Topic 1)
A network administrator needs to query the NSs for a remote application. Which of the following commands would BEST help the administrator accomplish this task?

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

Answer: A

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

NEW QUESTION 66
- (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 67
- (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 69
- (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 73
- (Exam Topic 2)
A SaaS provider has decided to leave an unpatched VM available via a public DMZ port. With which of the following concepts is this technique MOST closely associated?

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

Answer: D

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

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 80
- (Exam Topic 2)
A network technician was troubleshooting an issue for a user who was being directed to cloned websites that were stealing credentials. The URLs were correct for the websites but an incorrect IP address was revealed when the technician used ping on the user's PC After checking the is setting, the technician found the DNS server address was incorrect Which of the following describes the issue?

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

Answer: C

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

NEW QUESTION 81
- (Exam Topic 2)
A network administrator wants to analyze attacks directed toward the company's network. Which of the following must the network administrator implement to assist in this goal?

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

Answer: A

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

NEW QUESTION 85
- (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 88
- (Exam Topic 2)
A lab environment hosts Internet-facing web servers and other experimental machines, which technicians use for various tasks A technician installs software on one of the web servers to allow communication to the company's file server, but it is unable to connect to it Other machines in the building are able to retrieve files from the file server. Which of the following is the MOST likely reason the web server cannot retrieve the files, and what should be done to resolve the problem?

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

Answer: B

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

NEW QUESTION 93
- (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 95
- (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 97
- (Exam Topic 2)
A network technician is installing an analog desk phone for a new receptionist After running a new phone line, the technician now needs to cnmp on a new connector. Which of the following connectors would MOST likely be used in this case?

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

Answer: B

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

NEW QUESTION 98
- (Exam Topic 2)
Which of the following is a system that is installed directly on a server's hardware and abstracts the hardware from any guest machines?

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

Answer: B

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

NEW QUESTION 99
- (Exam Topic 2)
Which of the following attacks encrypts user data and requires a proper backup implementation to recover?

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

Answer: C

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

NEW QUESTION 100
- (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 102
- (Exam Topic 2)
An IDS was installed behind the edge firewall after a network was breached. The network was then breached again even though the IDS logged the attack. Which of the following should be used in place of these devices to prevent future attacks?

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

Answer: C

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

NEW QUESTION 104
- (Exam Topic 2)
A network administrator is required to ensure that auditors have read-only access to the system logs, while systems administrators have read and write access to the system logs, and operators have no access to the system logs. The network administrator has configured security groups for each of these functional categories. Which of the following security capabilities will allow the network administrator to maintain these permissions with the LEAST administrative effort?

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

Answer: C

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

NEW QUESTION 108
- (Exam Topic 2)
A firewall administrator is implementing a rule that directs HTTP traffic to an internal server listening on a non-standard socket Which of the following types of rules is the administrator implementing?

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

Answer: B

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

NEW QUESTION 109
- (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 112
- (Exam Topic 2)
Which of the following technologies allows traffic to be sent through two different ISPs to increase performance?

A. Fault tolerance
B. Quality of service
C. Load balancing
D. Port aggregation

Answer: C

Explanation:
Load balancing is a technology that allows traffic to be sent through two different ISPs to increase performance. Load balancing is a process of distributing network traffic across multiple servers or links to optimize resource utilization, throughput, latency, and reliability. Load balancing can be implemented at different layers of the OSI model, such as layer 4 (transport) or layer 7 (application). Load balancing can also be used for outbound traffic by using multiple ISPs and routing protocols such as BGP (Border Gateway Protocol) to select the best path for each packet. References:
https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/border-gateway-protocol-bgp/prod_white_

NEW QUESTION 116
- (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 120
- (Exam Topic 2)
A technician is connecting DSL for a new customer. After installing and connecting the on-premises equipment, the technician verifies DSL synchronization. When connecting to a workstation, however, the link LEDs on the workstation and modem do not light up. Which of the following should the technician perform during troubleshooting?

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

Answer: D

Explanation:
If the link LEDs on the workstation and modem do not light up when connecting to a workstation, it could indicate a problem with the cable connecting them. The

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

NEW QUESTION 121
- (Exam Topic 2)
A client moving into a new office wants the IP network set up to accommodate 412 network-connected devices that are all on the same subnet. The subnet needs to be as small as possible. Which of the following subnet masks should be used to achieve the required result?

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

Answer: B

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

NEW QUESTION 126
- (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 127
- (Exam Topic 2)
A city has hired a new employee who needs to be able to work when traveling at home and at the municipal sourcing of a neighboring city that snares services. The employee is issued a laptop, and a technician needs to train the employee on the appropriate solutions for secure access to the network from all the possible locations On which of the following solutions would the technician MOST likely train the employee?

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

Answer: A

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

NEW QUESTION 132
- (Exam Topic 3)
A network administrator views a network pcap and sees a packet containing the following:

```
community: public
request-id: 13438
get-response 1.3.6.1.2.1.1.3.0 Value:206801150
```

Which of the following are the BEST ways for the administrator to secure this type of traffic? (Select TWO).

A. Migrate the network to IPv6.
B. Implement 802.1 X authentication
C. Set a private community siring
D. Use SNMPv3.
E. Incorporate SSL encryption
F. Utilize IPSec tunneling.

Answer: CD

Explanation:
The packet shown in the image is an SNMP (Simple Network Management Protocol) packet, which is used to monitor and manage network devices. SNMP uses community strings to authenticate requests and responses between SNMP agents and managers. However, community strings are sent in clear text and can be easily intercepted by attackers. Therefore, one way to secure SNMP traffic is to set a private community string that is not the default or well-known value. Another way to secure SNMP traffic is to use SNMPv3, which is the latest version of the protocol that supports encryption and authentication of SNMP messages.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.5: Given a scenario, use remote access methods.

NEW QUESTION 135
- (Exam Topic 3)
A technician is consolidating a topology with multiple SSlDs into one unique SSID deployment. Which of the following features will be possible after this new configuration?

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

Answer: A

NEW QUESTION 137
- (Exam Topic 3)
Which of the following is used to elect an STP root?

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

Answer: B

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

NEW QUESTION 140
- (Exam Topic 3)
An administrator is investigating reports of network slowness in a building. While looking at the uplink interface statistics In the switch's CLI, the administrator discovers the uplink Is at 100% utilization However, the administrator is unsure how to Identify what traffic is causing the saturation. Which of the following tools should the administrator utilize to identify the source and destination addresses of the traffic?

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

Answer: D

Explanation:
To identify the source and destination addresses of the traffic causing network saturation, the network administrator should use a network protocol analyzer that supports the NetFlow protocol. NetFlow is a network protocol that collects IP traffic information as it enters or exits an interface and sends it to a NetFlow collector for analysis. This data includes the source and destination addresses of the traffic, the ports used, and the number of bytes and packets transferred.
Therefore, the correct answer is option D, NetFlow.
Reference: CompTIA Network+ Study Guide, Exam N10-007, Fourth Edition, by Todd Lammle (Chapter 6: Network Devices)

NEW QUESTION 142
- (Exam Topic 3)
A company needs a redundant link to provide a channel to the management network in an incident response scenario. Which of the following remote access methods provides the BEST solution?

A. Out-of-band access
B. Split-tunnel connections
C. Virtual network computing
D. Remote desktop gateways

Answer: A

Explanation:
Out-of-band access is a remote access method that provides a separate, independent channel for accessing network devices and systems. Out-of-band access uses a dedicated network connection or a separate communication channel, such as a dial-up or cellular connection, to provide access to network devices and systems. This allows an administrator to access the management network even if the primary network connection is unavailable or impaired. Out-of-band access is a good solution for providing a redundant link to the management network in an incident response scenario because it can be used to access the network even if the primary connection is unavailable or impaired.

NEW QUESTION 146
- (Exam Topic 3)
A technician is checking network devices to look for opportunities to improve security Which of the following toots would BEST accomplish this task?

A. Wi-Fi analyzer
B. Protocol analyzer
C. Nmap
D. IP scanner

Answer: B

Explanation:
A protocol analyzer is a tool that can capture and analyze network traffic and identify security issues such as unauthorized devices, malicious packets, or misconfigured settings.
A Wi-Fi analyzer is a tool that can measure the signal strength, interference, and channel usage of wireless networks, but it cannot provide detailed information about network security.
Nmap and IP scanner are tools that can scan network hosts and ports for open services, vulnerabilities, or operating systems, but they cannot monitor network traffic in real time.

NEW QUESTION 147
- (Exam Topic 3)
During a recent security audit, a contracted penetration tester discovered the organization uses a number of insecure protocols. Which of the following ports should be disallowed so only encrypted protocols are allowed? (Select TWO).

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

Answer: BC

NEW QUESTION 152
- (Exam Topic 3)
A non-employee was able to enter a server room. Which of the following could have prevented this from happening?

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

Answer: B

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

NEW QUESTION 153
- (Exam Topic 3)
Which of the following would MOST likely utilize PoE?

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

Answer: A

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

NEW QUESTION 156
- (Exam Topic 3)
A network is experiencing extreme latency when accessing a particular website. Which of the following commands will BEST help identify the issue?

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

Answer: C

NEW QUESTION 159
- (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 161
- (Exam Topic 3)
Which of the following is the MOST cost-effective alternative that provides proper cabling and supports gigabit Ethernet devices?

A. Twisted cable with a minimum Cat 5e certification
B. Multimode fiber with an SC connector
C. Twinaxial cabling using an F-type connector
D. Cable termination using TIA/EIA-568-B

Answer: A

Explanation:
twisted cable with a minimum Cat 5e certification is the MOST cost-effective alternative that provides proper cabling and supports gigabit Ethernet devices.

NEW QUESTION 165
- (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 169
- (Exam Topic 3)
A network administrator installed an additional IDF during a building expansion project. Which of the following documents need to be updated to reflect the change? (Select TWO).

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

Answer: BF

NEW QUESTION 174
- (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 176
- (Exam Topic 3)
A network technician is implementing a solution that will allow end users to gain access to multiple applications after logging on. Which of the following authentication methods would allow this type of access?

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

Answer: A

NEW QUESTION 181
- (Exam Topic 3)
A new global ISP needs to connect from central offices in North America to the United Kingdom. Which of the following would be the BEST cabling solution for this project?

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

Answer: A

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

NEW QUESTION 184
- (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 186
- (Exam Topic 3)
Users within a corporate network need to connect to the Internet, but corporate network policy does not allow direct connections. Which of the following is MOST likely to be used?

A. Proxy server
B. VPN client
C. Bridge
D. VLAN

Answer: A

NEW QUESTION 189
- (Exam Topic 3)
A technician knows the MAC address of a device and is attempting to find the device's IP address. Which of the following should the technician look at to find the IP address? (Select TWO).

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

Answer: BE

NEW QUESTION 193
- (Exam Topic 3)
Which of the following is used to provide disaster recovery capabilities to spin up an critical devices using internet resources?

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

Answer: A

NEW QUESTION 195
- (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 199
- (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 201
- (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 203
- (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 205
- (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 208
- (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 212
- (Exam Topic 3)
An employee working in a warehouse facility is experiencing interruptions in mobile applications while walking around the facility. According to a recent site survey, the WLAN comprises autonomous APs that are directly connected to the internet, providing adequate signal coverage. Which of the following is the BEST solution to improve network stability?

A. Implement client roaming using an extended service deployment employing a wireless controller.

B. Remove omnidirectional antennas and adopt a directional bridge.
C. Ensure all APs of the warehouse support MIMO and Wi-Fi 4.
D. Verify that the level of EIRP power settings is set to the maximum permitted by regulations.

Answer: A

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

NEW QUESTION 217
- (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 222
- (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 225
- (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 229
- (Exam Topic 3)
Which of the following can have multiple VLAN interfaces?

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

Answer: B

NEW QUESTION 234

- (Exam Topic 3)
Due to space constraints in an IDF, a network administrator can only a do a single switch to accommodate three data networks. The administrator needs a configuration that will allow each device to access its expected network without additional connections. The configuration must also allow each device to access the rest of the network. Which of the following should the administrator do to meet these requirements? (Select TWO).

A. Untag the three VLANs across the uplink
B. Tag an individual VLAN across the uplink
C. Untag an individual VLAN per device port
D. Tag an individual VLAN per device port
E. Tag the three VLANs across the uplink.
F. Tag the three VLANs per device port.

Answer: AC

Explanation:
To achieve this, you should do two things:
- Tag the three VLANs across the uplink port that connects to another switch or router. This will allow data packets from different VLANs to cross over into other networks.
- Untag an individual VLAN per device port that connects to an end device. This will assign each device to its expected network without additional connections.

NEW QUESTION 237
- (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 239
- (Exam Topic 3)
A switch is connected to another switch. Incompatible hardware causes a surge in traffic on both switches. Which of the following configurations will cause traffic to pause, allowing the switches to drain buffers?

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

Answer: B

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

NEW QUESTION 243
- (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 247
- (Exam Topic 3)
To comply with an industry regulation, all communication destined to a secure server should be logged and archived on a storage device. Which of the Mowing can be configured to fulfill this requirement?

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

Answer: B

NEW QUESTION 250
- (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 253
- (Exam Topic 3)
A Wi-Fi network was recently deployed in a new, multilevel budding. Several issues are now being reported related to latency and drops in coverage. Which of the following is the FIRST step to troubleshoot the issues?

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

Answer: A

NEW QUESTION 258
- (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 263
- (Exam Topic 3)
An engineer needs to verity the external record tor SMTP traffic. The engineer logged in to the server and entered the nslookup command. Which of the following commands should the engineer send before entering the DNS name?

A. set type=A
B. is -d company-mail.com
C. set domain=company.mail.com
D. set querytype=Mx

Answer: D

NEW QUESTION 265
- (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 267
- (Exam Topic 3)
A user calls the help desk to report being unable to reach a file server. The technician logs in to the user's computer and verifies that pings fall to respond back when trying to reach the file server. Which of the following would BEST help the technician verify whether the file server is reachable?

A. netstat
B. ipconfig
C. nslookup
D. traceroute

Answer: D

Explanation:
Traceroute is a network diagnostic tool that allows you to trace the path that network packets take from one device to another. By running traceroute to the file server, the technician can see the sequence of devices and networks that the packets pass through on their way to the file server. This can help the technician to determine if there is a problem with the network connection between the user's computer and the file server, or if the issue is with the file server itself.

NEW QUESTION 268
- (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 272
- (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 276
- (Exam Topic 3)
A network administrator is adding a new switch to the network. Which of the following network hardening techniques would be BEST to use once the switch is in production?

A. Disable unneeded ports
B. Disable SSH service
C. Disable MAC filtering
D. Disable port security

Answer: A

NEW QUESTION 280
- (Exam Topic 3)
A network technician is performing tests on a potentially faulty network card that is installed in a server. Which of the following addresses will MOST likely be used during traffic diagnostic tests?

A. 10.10.10.10
B. 127.0.0.1
C. 192.168.0.1
D. 255.255.255.0

Answer: B

Explanation:
* 127.1.1.1 is the loopback address, it is used to test the functionality of a network card by sending traffic to the card and then verifying that it is received properly. This address is used because it is guaranteed to always point to the local host, regardless of the network configuration. The IP address range for loopback addresses is 127.0.0.0/8.

NEW QUESTION 285
- (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 289
- (Exam Topic 3)
A network technician 13 troubleshooting a specific port on a switch. Which of the following commands should the technician use to see the port configuration?

A. show route
B. show Interface
C. show arp
D. show port

Answer: B

Explanation:
To see the configuration of a specific port on a switch, the network technician should use the "show interface" command. This command provides detailed information about the interface, including the current configuration, status, and statistics for the interface.

NEW QUESTION 290
- (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 293

- (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 294
- (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 299
- (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 302
- (Exam Topic 3)
A customer wants to log in t o a vendor's server using a web browser on a laptop. Which of the following would require the LEAST configuration to allow encrypted access to the server?

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

Answer: A

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

NEW QUESTION 304
- (Exam Topic 3)
A network administrator received a report staling a critical vulnerability was detected on an application that is exposed to the internet. Which of the following Is the appropriate NEXT step?

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

D. Deploy a new server to host the application.

Answer: A

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

NEW QUESTION 305
- (Exam Topic 3)
Two users on a LAN establish a video call. Which of the following OSI model layers ensures the initiation coordination, and termination of the call?

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

Answer: A

Explanation:
The OSI model layer that ensures the initiation, coordination, and termination of a video call is the session layer. The session layer is responsible for establishing, maintaining, and terminating communication sessions between two devices on a network.

NEW QUESTION 308
- (Exam Topic 3)
A company is utilizing multifactor authentication for data center access. Which of the following is the MOST effective security mechanism against physical intrusions due to stolen credentials?

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

Answer: C

NEW QUESTION 312
- (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 315
- (Exam Topic 3)
A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds hundreds of CRC errors on an interface. Which of the following is the MOST likely cause of these errors?

A. A bad wire on the Cat 5e cable
B. The wrong VLAN assignment to the switchport
C. A misconfigured QoS setting on the router
D. Both sides of the switch trunk set to full duplex

Answer: A

NEW QUESTION 319
- (Exam Topic 3)
Which of the following would be BEST suited for a long cable run with a 40Gbps bandwidth?

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

Answer: C

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

NEW QUESTION 324
- (Exam Topic 3)
Which of the following routing protocols is BEST suited for use on a perimeter router?

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

Answer: D

Explanation:
BGP stands for Border Gateway Protocol and it is used to exchange routing information between autonomous systems (AS) on the Internet. A perimeter router is a router that connects an AS to another AS or to the Internet. Therefore, BGP is the best suited routing protocol for a perimeter router.
References: Network+ Study Guide Objective 2.4: Compare and contrast the characteristics of network topologies, types and technologies.

NEW QUESTION 326
- (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 328
- (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 329
- (Exam Topic 3)
Which of the following describes when an active exploit is used to gain access to a network?

A. Penetration testing
B. Vulnerability testing
C. Risk assessment
D. Posture assessment
E. Baseline testing

Answer: A

Explanation:
Penetration testing is a type of security testing that is used to assess the security of a system or network by actively exploiting known vulnerabilities. It is used to simulate an attack on the system and identify any weaknesses that may be exploited by malicious actors. As stated in the CompTIA Security+ Study Guide, "penetration testing is a type of security assessment that attempts to gain unauthorized access to networks and systems by exploiting security vulnerabilities."

NEW QUESTION 331
- (Exam Topic 3)

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

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

Answer: B

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

NEW QUESTION 336
- (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 340
- (Exam Topic 3)
A security engineer is trying to determine whether an internal server was accessed by hosts on the internet. The internal server was shut down during the investigation Which of the following will the engineer review to determine whether the internal server had an unauthorized access attempt?

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

Answer: A

NEW QUESTION 342
- (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 343
- (Exam Topic 3)
A technician is equipped with a tablet, a smartphone, and a laptop to troubleshoot a switch with the help of support over the phone. However, the technician is having issues interconnecting all these tools in troubleshooting the switch. Which Of the following should the technician use to gain connectivity?

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

Answer: A

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

NEW QUESTION 345
- (Exam Topic 3)
Which of the following will reduce routing table lookups by performing packet forwarding decisions independently of the network layer header?

A. MPLS
B. mGRE
C. EIGRP
D. VRRP

Answer: A

Explanation:
Multiprotocol Label Switching, or MPLS, is a networking technology that routes traffic using the shortest path based on “labels,” rather than network addresses, to handle forwarding over private wide area networks. As a scalable and protocol-independent solution, MPLS assigns labels to each data packet, controlling the path the packet follows. MPLS greatly improves the speed of traffic, so users don’t experience downtime when connected to the network.

NEW QUESTION 349
- (Exam Topic 3)
A technician is troubleshooting a connectivity issue with an end user. The end user can access local network shares and intranet pages but is unable to access the internet or remote resources. Which of the following needs to be reconfigured?

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

Answer: C

NEW QUESTION 351
- (Exam Topic 3)
A newly installed multifunction copier needs to be set up so scanned documents can be emailed to recipients. Which of the following ports from the copier's IP address should be allowed?

A. 22
B. 25
C. 53
D. 80

Answer: B

Explanation:
Port 25 is the port number that is commonly used for Simple Mail Transfer Protocol (SMTP), which is a protocol that allows sending and receiving email messages over a network1. Port 25 from the copier’s IP address should be allowed so that scanned documents can be emailed to recipients.
Port 22 is the port number that is commonly used for Secure Shell (SSH), which is a protocol that allows secure and encrypted remote access and control of a device over a network1. Port 22 from the copier’s IP address is not necessary for emailing scanned documents.
Port 53 is the port number that is commonly used for Domain Name System (DNS), which is a protocol that
allows resolving domain names to IP addresses and vice versa on a network1. Port 53 from the copier’s IP address is not necessary for emailing scanned documents.
Port 80 is the port number that is commonly used for Hypertext Transfer Protocol (HTTP), which is a protocol that allows transferring web pages and other resources over a network1. Port 80 from the copier’s IP address is not necessary for emailing scanned documents.

NEW QUESTION 354
- (Exam Topic 3)
A technician is tasked with setting up a mail server and a DNS server. The mail port should be secured and have the ability to transfer large files. Which of the following ports should be opened? (Select TWO).

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

Answer: BE

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

NEW QUESTION 357
- (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 359
- (Exam Topic 3)
A network engineer needs to reduce the overhead of file transfers. Which of the following configuration changes would accomplish that goal?

A. Link aggregation
B. Jumbo frames
C. Port security
D. Flow control
E. Lower FTP port

Answer: A

NEW QUESTION 361
- (Exam Topic 3)
A technician is consolidating a topology with multiple SSlDs into one unique SSiD deployment. Which of the following features will be possible after this new configuration?

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

Answer: A

NEW QUESTION 362
- (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 363
- (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 364
- (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 367
- (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 370
- (Exam Topic 3)
A network administrator is investigating a network event that is causing all communication to stop. The network administrator is unable to use SSH to connect to the switch but is able to gain access using the serial console port. While monitoring port statistics, the administrator sees the following:

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

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

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

Answer: B

NEW QUESTION 373
- (Exam Topic 3)
The following DHCP scope was configured for a new VLAN dedicated to a large deployment of 325 loT sensors:

```
DHCP network scope:      10.10.0.0/24
Exclusion range:         10.10.10.1-10.10.10.10
Gateway:                 10.10.0.1
DNS:                     10.10.0.2
DHCP option 66(TFTP):    10.10.10.4
DHCP option 4(NTP):      10.10.10.5
```

The first 244 loT sensors were able to connect to the TFTP server, download the configuration file, and register to an loT management system. The other sensors are being shown as offline. Which of the following should be performed to determine the MOST likely cause of the partial deployment of the sensors?

A. Check the gateway connectivity to the TFTP server.
B. Check the DHCP network scope.
C. Check whether the NTP server is online.
D. Check the loT devices for a hardware failure.

Answer: B

NEW QUESTION 376
- (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 381
- (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 385
- (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 389
- (Exam Topic 3)
An administrator wants to increase the availability of a server that is connected to the office network. Which of the following allows for multiple NICs to share a single IP address and offers maximum performance while providing fault tolerance in the event of a NIC failure?

A. Multipathing
B. Spanning Tree Protocol
C. First Hop Redundancy Protocol
D. Elasticity

Answer: A

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

NEW QUESTION 390
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

N10-009 Practice Exam Features:

* N10-009 Questions and Answers Updated Frequently

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

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

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