Number: N10-008
Passing Score: 800
Time Limit: 120
File Version: 41.0

Exam Code: N10-008
Exam Name: CompTIA Network+

Exam A

QUESTION 1
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

Correct Answer: A
Section:
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.

QUESTION 2
A network engineer is monitoring a fiber uplink to a remote office and notes the uplink has been operating at 100% capacity for a long duration. Which of the following performance metrics is MOST likely to be impacted with sustained link saturation?

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

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

QUESTION 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.

Correct Answer: B
Section:

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.

QUESTION 4
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.

Correct Answer: C
Section:
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.

QUESTION 5
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.

Correct Answer: C, E
Section:
Explanation:
To allow each device to access its expected network without additional connections, theadministrator needs to configure VLANs (virtual LANs) on the switch. VLANs are logical groupsof devices that share the same broadcast domain, regardless of their physical location orconnection. VLANs can improve network performance, security, and management by isolatingtraffic and reducing broadcast storms. To configure VLANs on the switch, the administratorneeds to assign each device port to a specific VLAN and set the VLAN tagging mode. VLANtagging is a method of adding a VLAN identifier to the Ethernet frames to indicate which VLANthey belong to. There are two types of VLAN tagging: untagged and tagged. Untagged VLANtagging means that the switch removes the VLAN identifier from the frames before sendingthem to the device port. This is suitable for end devices that do not support VLAN tagging, such as PCs, printers, etc. Tagged VLAN tagging means that the switch keeps the VLAN identifier onthe frames when sending them to the device port. This is suitable for devices that support VLANtagging, such as routers, servers, other switches, etc. To allow each device to access the rest ofthe network, the administrator needs to configure a trunk port on the switch that connects tothe uplink. A trunk port is a port that can carry traffic from multiple VLANs using tagged VLANtagging. This way, the switch can send and receive frames from different VLANs to and from therest of the network. Therefore, the administrator should do the

following to meet therequirements:Untag an individual VLAN per device port. This will assign each device port to a specific VLANand remove the VLAN identifier from the frames before sending them to the device port. Thiswill allow each device to access its expected network without additional connections.Tag the three VLANs across the uplink. This will configure a trunk port on the switch thatconnects to the uplink and add the VLAN identifier to the frames before sending them to theuplink. This will allow the switch to carry traffic from multiple VLANs to and from the rest of thenetwork.VLANs and TrunksVLAN Tagging Explained with DTP Protocol

QUESTION 6
Users are reporting poor wireless performance in some areas of an industrial plant The wireless controller is measuring a tow EIRP value compared to me recommendations noted on me most recent site survey. Which of the following should be verified or replaced for the EIRP value to meet the site survey's specifications? (Select TWO).

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

Correct Answer: A, E
Section:
Explanation:
AP transmit power: You should check if your APs have sufficient power output and adjust them if needed. You should also make sure they are not exceeding regulatory limits for your region. Antenna gain: You should check if your antennas have adequate gain for your coverage area and replace them if needed. You should also make sure they are aligned properly and not obstructed by any objects.
In the scenario described, the wireless controller is measuring a low EIRP value compared to the recommendations noted in the most recent site survey. EIRP is the combination of the power transmitted by the access point and the antenna gain. Therefore, to increase the EIRP value to meet the site survey's specifications, the administrator should verify or replace the AP transmit power (option A) and the antenna gain (option E). This can be achieved by adjusting the transmit power settings on the AP or by replacing the AP's antenna with one that has a higher gain

QUESTION 7
An administrator is setting up a multicast server on a network, but the firewall seems to be dropping the traffic. After logging in to the device, me administrator sees me following entries:

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

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

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

Correct Answer: B
Section:
Explanation:

QUESTION 8
A client recently added 100 users who are using VMs. All users have since reported slow or unresponsive desktops. Reports show minimal network congestion, zero packet loss, and acceptable packet delay. Which of the following metrics will MOST accurately show the underlying performance issues? (Choose two.)

A. CPU usage
B. Memory

C. Temperature
D. Bandwidth
E. Latency
F. Jitter

Correct Answer: A, B
Section:
Explanation:
The question asks about the metrics that will most accurately show the underlying performanceissues of slow or unresponsive desktops for users who are using VMs (virtual machines).VMs are software-based simulations of physical computers that run on a host system. Theyshare the resources of the host system, such as CPU, memory, disk space, etc.If the host system does not have enough resources to support the number of VMs running on it,the performance of the VMs will suffer. This is especially true if the VMs are running resource-intensive applications or tasks.Therefore, the metrics that will most accurately show the underlying performance issuesareCPU usageandmemory. These metrics indicate how much of the host system's resources arebeing consumed by the VMs and how much is available for other processes.The other metrics are not relevant to the question, as they are related to the networkperformance, not the host system performance. They are:Temperature: the measure of how hot the host system or its components are. Hightemperature can cause overheating and damage to the hardware, but it is not directly relatedto the performance of the VMs.Bandwidth: the measure of how much data can be transferred over a network connection in agiven time. Low bandwidth can cause network congestion and slow data transfer, but it is notdirectly related to the performance of the VMs.Latency: the measure of how long it takes for a data packet to travel from one point to antheron a network. High latency can cause delays and poor quality of service, but it is not directlyrelated to the performance of the VMs.Jitter: the measure of how much the latency varies over time on a network. High jitter cancause inconsistent and unpredictable network performance, but it is not directly related to theperformance of the VMs.
CompTIA Network+ N10-008 Study Guide, Chapter 1: Networking Concepts, Section 1.3:Virtualization and Network Storage Technologies, Pages 34-36Professor Messer's CompTIA N10-008 Network+ Course, Video 1.3: Virtualization and NetworkStorage Technologies, Part 1

QUESTION 9
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

Correct Answer: D
Section:
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.
Reference:
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

QUESTION 10
An administrator is writing a script to periodically log the IPv6 and MAC addresses of all the devices on a network segment. Which of the following switch features will MOST likely be used to assist with this task?

A. Spanning Tree Protocol
B. Neighbor Discovery Protocol
C. Link Aggregation Control Protocol
D. Address Resolution Protocol

Correct Answer: B
Section:
Explanation:
Short The switch feature that is most likely to be used to assist with logging IPv6 and MAC addresses of devices on a network segment is Neighbor Discovery Protocol (NDP). NDP is used by IPv6 to discover and maintain

information about other nodes on the network, including their IPv6 and MAC addresses. By periodically querying NDP, the administrator can log this information for auditing purposes.
Reference:
CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.1: Compare and contrast TCP and UDP ports, protocols, and their purposes.

QUESTION 11
Which of the following DNS records works as an alias to another record?

A. AAAA
B. CNAME
C. MX
D. SOA

Correct Answer: B
Section:
Explanation:
The DNS record that works as an alias to another record is called CNAME (Canonical Name). CNAME records are used to create an alias for a domain name that points to another domain name.
Reference:
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.

QUESTION 12
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

Correct Answer: A
Section:
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.
Reference:
CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 4: Network Implementations, Objective 4.4: Explain the purpose and properties of DHCP.

QUESTION 13
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

Correct Answer: A
Section:
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.
Reference:
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.

QUESTION 14
A technician is searching for a device that is connected to the network and has the device's physical network address. Which of the following should the technician review on the switch to locate the device's network port?

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

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

QUESTION 15
Which of the following provides redundancy on a file server to ensure the server is still connected to a LAN even in the event of a port failure on a switch?

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

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

QUESTION 16
An IT organization needs to optimize speeds for global content distribution and wants to reduce latency in high-density user locations. Which of the following technologies BEST meets the organization's requirements?

A. Load balancing
B. Geofencing

C. Public cloud
D. Content delivery network
E. Infrastructure as a service

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

QUESTION 17
A user reports being unable to access network resources after making some changes in the office. Which of the following should a network technician do FIRST?

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

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

QUESTION 18
A new cabling certification is being requested every time a network technician rebuilds one end of a Cat 6 (vendor-certified) cable to create a crossover connection that is used to connect switches. Which of the following would address this issue by allowing the use of the original cable?

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

Correct Answer: D
Section:
Explanation:
MDIX (medium-dependent interface crossover) is a feature that allows network devices to automatically detect and configure the appropriate cabling type, eliminating the need for crossover cables. By enabling MDIX on the switches, a technician can use the original Cat 6 cable to create a crossover connection.
Reference: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

QUESTION 19
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

Correct Answer: A
Section:
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.

QUESTION 20
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

Correct Answer: B
Section:
Explanation:
802.11a/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.
Reference: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

QUESTION 21
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

Correct Answer: C
Section:
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. Reference:
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/sec/b_1610_sec_9500_cg/b_1610_sec_9500_cg_chapter_0101010.html

QUESTION 22
Which of the following is used to track and document various types of known vulnerabilities?

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

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

QUESTION 23
The network administrator is informed that a user's email password is frequently hacked by brute- force programs. Which of the following policies should the network administrator implements to BEST mitigate this issue? (Choose two.)

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

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

QUESTION 24
A network engineer performs the following tasks to increase server bandwidth:
Connects two network cables from the server to a switch stack Configure LACP on the switchports
Verifies the correct configurations on the switch interfaces Which of the following needs to be configured on the server?

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

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

QUESTION 25
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

Correct Answer: C
Section:
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. Reference: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam- objectives-(2-0), https://www.techopedia.com/definition/950/subnet-mask

QUESTION 26
Which of the following is the LARGEST MTU for a standard Ethernet frame?

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

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

QUESTION 27
Given the following information:

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

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

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

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

QUESTION 28
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

Correct Answer: A
Section:
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.
Reference: 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

QUESTION 29
Which of the following BEST describes a network appliance that warns of unapproved devices that are accessing the network?

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

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

QUESTION 30
A technician is installing a cable modem in a SOHO. Which of the following cable types will the technician MOST likely use to connect a modem to the ISP?

A. Coaxial
B. Single-mode fiber
C. Cat 6e
D. Multimode fiber

Correct Answer: A
Section:
Explanation:
Coaxial cable is a type of cable that consists of a central copper conductor surrounded by an insulating layer and a braided metal shield. Coaxial cable is commonly used to connect a cable modem to an ISP by transmitting data over cable television networks. Coaxial cable can support high bandwidth and long distances with minimal interference or attenuation. Reference:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam- objectives-(2-0), https://www.techopedia.com/definition/4027/coaxial-cable

QUESTION 31
A network technician is reviewing the interface counters on a router interface. The technician is attempting to confirm a cable issue. Given the following information:

Metric	Value
Last cleared	7 minutes, 34 seconds
# of packets output	6915
# of packets input	270
CRCs	183
Giants	0
Runts	0
Multicasts	14

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

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

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

QUESTION 32
Which of the following is the physical topology for an Ethernet LAN?

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

Correct Answer: D
Section:
Explanation:
In a star topology, all devices on a network connect to a central hub or switch, which acts as a common connection point. Ethernet LANs typically use a star topology, with each device connected to a central switch. Reference:
Network+ N10-008 Objectives: 2.2 Explain common logical network topologies and their characteristics.

QUESTION 33
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

Correct Answer: E
Section:
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. Reference:
Network+ N10-008 Objectives: 1.5 Compare and contrast disaster recovery concepts and methodologies.

QUESTION 34
The management team needs to ensure unnecessary modifications to the corporate network are not permitted and version control is maintained. Which of the following documents would BEST support this?

A. An incident response plan
B. A business continuity plan
C. A change management policy
D. An acceptable use policy

Correct Answer: C
Section:
Explanation:
A change management policy is a document that outlines the procedures and guidelines for making changes to a network or system, including how changes are approved, tested, and implemented. By following a change management policy, organizations can ensure that unnecessary modifications to the network are not permitted and version control is maintained. Reference:
Network+ N10-008 Objectives: 1.6 Given a scenario, implement network configuration and change management best practices.

QUESTION 35
Which of the following is MOST likely to generate significant East-West traffic in a datacenter?

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

Correct Answer: B
Section:
Explanation:
East-West traffic refers to data flows between servers or devices within the same datacenter. When a hosted virtual server is duplicated to another physical server for redundancy, it generates significant East-West traffic as the data is replicated between the two servers. Reference:
Network+ N10-008 Objectives: 3.3 Given a scenario, implement secure network architecture concepts.

QUESTION 36
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

Correct Answer: B
Section:
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. Reference:
Network+ N10-008 Objectives: 2.1 Given a scenario, troubleshoot common physical connectivity issues.

QUESTION 37
A technician wants to deploy a new wireless network that comprises 30 WAPs installed throughout a three-story office building. All the APs will broadcast the same SSID for client access. Which of the following BEST describes this deployment?

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

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

QUESTION 38
A user tries to ping 192.168.1.100 from the command prompt on the 192.168.2.101 network but gets the following response: U.U.U.U. Which of the following needs to be configured for these networks to reach each other?

A. Network address translation
B. Default gateway
C. Loopback
D. Routing protocol

Correct Answer: B
Section:
Explanation:
A default gateway is a device that routes traffic from one network to another network, such as the Internet. A default gateway is usually configured on each host device to specify the IP address of the router that connects the host's network to other networks. In this case, the user's device and the destination device are on different networks (192.168.1.0/24 and 192.168.2.0/24), so the user needs to configure a default gateway on their device to reach the destination device. Reference:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam- objectives-(2-0), https://www.techopedia.com/definition/25761/default-gateway

QUESTION 39
A branch of a company recently switched to a new ISP. The network engineer was given a new IP range to assign. The ISP assigned 196.26.4.0/26, and the branch gateway router now has the following configurations on the interface that peers to the ISP:

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

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

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

Correct Answer: C
Section:
Explanation:
The IP address configured on the router interface is 196.26.4.1/26, which belongs to the IP range assigned by the ISP (196.26.4.0/26). However, this IP address is not valid for this interface because it is the network address of the subnet, which cannot be assigned to any host device. The network address is the first address of a subnet that identifies the subnet itself. The valid IP addresses for this subnet are from 196.26.4.1 to 196.26.4.62, excluding the network address (196.26.4.0) and the broadcast address (196.26.4.63). The router interface should be configured with a valid IP address within this range to restore Internet connectivity for all users. Reference: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam- objectives-(2-0), https://www.techopedia.com/definition/24136/network-address

QUESTION 40
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.

Correct Answer: A
Section:
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.
Reference: 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/

QUESTION 41
Which of the following service models would MOST likely be used to replace on-premises servers with a cloud solution?

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

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

QUESTION 42

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

Correct Answer: B
Section:
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. Reference:
Network+ Certification Study Guide, Chapter 5:
Network Security

QUESTION 43
Which of the following is used to prioritize Internet usage per application and per user on the network?

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

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

QUESTION 44
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

Correct Answer: A
Section:

QUESTION 45
A company wants to set up a backup data center that can become active during a disaster. The site needs to contain network equipment and connectivity. Which of the following strategies should the company employ?

A. Active-active
B. Warm
C. Cold

D. Cloud

Correct Answer: B
Section:
Explanation:
Active-active refers to more than one NIC being active at the same time. In my opinion, this question is referring to a recovery site (hot, warm, cold, cloud)

QUESTION 46
A small office has a wireless network with several access points that are used by mobile devices. Users occasionally report that the wireless connection drops or becomes very slow. Reports confirm that this only happens when the devices are connected to the office wireless network. Which of the following is MOST likely the cause?

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

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

QUESTION 47
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+

Correct Answer: A
Section:

QUESTION 48
A network attack caused a network outage by wiping the configuration and logs of the border firewall. Which of the following sources, in an investigation to determine how the firewall was compromised, can provide the MOST detailed data?

A. Syslog server messages
B. MIB of the attacked firewall
C. Network baseline reports
D. NetFlow aggregate data

Correct Answer: A
Section:

QUESTION 49
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

Correct Answer: A
Section:
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. Reference: Network+ Certification Study Guide, Chapter 3: Network Infrastructure

QUESTION 50
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

Correct Answer: B
Section:
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. Reference: Network+ Certification Study Guide, Chapter 8: Network Troubleshooting

QUESTION 51
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

Correct Answer: A
Section:
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. Reference: Network+ Certification Study Guide, Chapter 5:
Network Security

QUESTION 52
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

Correct Answer: A
Section:
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. Reference: Network+ Certification Study Guide, Chapter 8:
Network Troubleshooting

QUESTION 53
A network administrator is implementing OSPF on all of a company's network devices. Which of the following will MOST likely replace all the company's hubs?

A. A Layer 3 switch
B. A proxy server
C. A NGFW
D. A WLAN controller

Correct Answer: A
Section:
Explanation:
A Layer 3 switch will likely replace all the company's hubs when implementing OSPF on all of its network devices. A Layer 3 switch combines the functionality of a traditional Layer 2 switch with the routing capabilities of a router. By implementing OSPF on a Layer 3 switch, an organization can improve network performance and reduce the risk of network congestion. Reference: Network+ Certification Study Guide, Chapter 5: Network Security

QUESTION 54
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

Correct Answer: A
Section:
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. Reference: 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

QUESTION 55
A network administrator is designing a new datacenter in a different region that will need to communicate to the old datacenter with a secure connection. Which of the following access methods would provide the BEST security for this new datacenter?

A. Virtual network computing

B. Secure Socket Shell
C. In-band connection
D. Site-to-site VPN

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

QUESTION 56
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

Correct Answer: D
Section:
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. Reference: CompTIA Network+ Certification Study Guide, Chapter 6: Network Attacks and Mitigation.

QUESTION 57
Which of the following technologies provides a failover mechanism for the default gateway?

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

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

QUESTION 58
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

Correct Answer: A
Section:
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. Reference: CompTIA Network+ Certification Study Guide, Chapter 3: IP Addressing.

QUESTION 59
A technician needs to configure a Linux computer for network monitoring. The technician has the following information:
Linux computer details:

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

Switch mirror port details:

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

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

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

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

QUESTION 60
A network engineer is investigating reports of poor network performance. Upon reviewing a device configuration, the engineer finds that duplex settings are mismatched on both ends. Which of the following would be the MOST likely result of this finding?

A. Increased CRC errors
B. Increased giants and runts
C. Increased switching loops
D. Increased device temperature

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

QUESTION 61
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

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

QUESTION 62
Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

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

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

QUESTION 63
An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex. Which of the following is the MOST likely cause of this issue?

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

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

QUESTION 64
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

Correct Answer: A
Section:
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.
Reference:
CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 6: Network Servers, p. 300

QUESTION 65
A technician is troubleshooting a wireless connectivity issue in a small office located in a high-rise building. Several APs are mounted in this office. The users report that the network connections frequently disconnect and reconnect throughout the day. Which of the following is the MOST likely cause of this issue?

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

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

QUESTION 66
A network engineer configured new firewalls with the correct configuration to be deployed to each remote branch. Unneeded services were disabled, and all firewall rules were applied successfully. Which of the following should the network engineer perform NEXT to ensure all the firewalls are hardened successfully?

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

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

QUESTION 67
At which of the following OSI model layers would a technician find an IP header?

A. Layer 1

B. Layer 2
C. Layer 3
D. Layer 4

Correct Answer: C
Section:
Explanation:
An IP header can be found at the third layer of the OSI model, also known as the network layer. This layer is responsible for logical addressing, routing, and forwarding of data packets.
Reference:
CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: Network Models, p. 82

QUESTION 68
An engineer is configuring redundant network links between switches. Which of the following should the engineer enable to prevent network stability issues?

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

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

QUESTION 69
Several WIFI users are reporting the inability to connect to the network. WLAN users on the guest network are able to access all network resources without any performance issues. The following table summarizes the findings after a site survey of the area in question:

Location	AP 1	AP 2	AP 3	AP 4
SSID	Corp1	Corp1	Corp1/Guest	Corp1/Guest
Channel	2	1	5	11
RSSI	-81dBm	-82dBm	-44dBm	-41dBm
Antenna type	Omni	Omni	Directional	Directional

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

A. Reconfigure the channels to reduce overlap
B. Replace the omni antennas with directional antennas
C. Update the SSIDs on all the APs
D. Decrease power in AP 3 and AP 4

Correct Answer: A
Section:
Explanation:
The issue of WIFI users being unable to connect while WLAN users on the guest network canaccess all resources indicates a problem with channel overlap or interference. By reconfiguringthe channels, interference can be minimized, improving connectivity for WIFI users. Accordingto the table, AP 1 and AP 2 are using adjacent channels (2 and 1), which can cause interference.AP 3 and AP 4 are using non-overlapping channels (5 and 11), but they have very high RSSIvalues (-44dBm and -41dBm), which can also cause interference. A possible solution is to useonly non-overlapping channels (such as 1, 6, and 11) and adjust the power levels to avoidexcessive signal strength.Reference:Wireless Troubleshooting -- N10-008 CompTIA Network+ :5.4,Network Troubleshooting Methodology - N10-008 CompTIA Network+ : 5.1

QUESTION 70

Which of the following routing protocols is used to exchange route information between public autonomous systems?

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

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

QUESTION 71
A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

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

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

QUESTION 72
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

Correct Answer: B
Section:
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.
Reference:
Network+ N10-007 Certification Exam Objectives, Objective 4.2: Given a scenario, implement secure network administration principles.

QUESTION 73
A network technician is installing new software on a Windows-based server in a different geographical location. Which of the following would be BEST for the technician to use to perform this task?

A. RDP
B. SSH
C. FTP
D. DNS

Correct Answer: A
Section:
Explanation:
RDP (Remote Desktop Protocol) is the best option for a network technician to use when installing new software on a Windows-based server in a different geographical location. This protocol allows the technician to connect to the server remotely and control it as if they were physically present.
Reference:
Network+ N10-007 Certification Exam Objectives, Objective 2.2: Given a scenario, implement the appropriate network-based security and troubleshoot common connectivity issues.

QUESTION 74
Branch users are experiencing issues with videoconferencing. Which of the following will the company MOST likely configure to improve performance for these applications?

A. Link Aggregation Control Protocol
B. Dynamic routing
C. Quality of service
D. Network load balancer
E. Static IP addresses

Correct Answer: C
Section:
Explanation:
To improve performance for videoconferencing, the company should configure Quality of Service (QoS). This technology allows for the prioritization of network traffic, ensuring that videoconferencing traffic is given higher priority and therefore better performance. Link Aggregation Control Protocol (LACP), Dynamic routing, Network load balancer, and Static IP addresses are not directly related to improving performance for videoconferencing.
Reference:
Network+ N10-007 Certification Exam Objectives, Objective 2.6: Given a scenario, implement and configure the appropriate wireless security and implement the appropriate QoS concepts.

QUESTION 75
A technician is assisting a user who cannot connect to a network resource. The technician first checks for a link light. According to troubleshooting methodology, this is an example of:

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

Correct Answer: A
Section:
Explanation:

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

QUESTION 76
Which of the following transceiver types can support up to 40Gbps?

A. SFP+
B. QSFP+
C. QSFP
D. SFP

Correct Answer: B
Section:
Explanation:
QSFP+ is a transceiver type that can support up to 40Gbps. It stands for Quad Small Form-factor Pluggable Plus and uses four lanes of data to achieve high-speed transmission. It is commonly used for data center and high-performance computing applications. Reference:
https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver- modules/data_sheet_c78-660083.html

QUESTION 77
A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

A. nslookup
B. netstat -a
C. ipconfig /a
D. arp -a

Correct Answer: B
Section:
Explanation:
netstat -a is a command that displays information about active TCP connections and listening ports on a system. A network administrator can use netstat -a to check if the database engine is listening on a certain port, as well as verify if there are any connections established to or from that port.
Reference: https://www.comptia.org/blog/what-is-netstat

QUESTION 78
A technician is implementing a new wireless network to serve guests at a local office. The network needs to provide Internet access but disallow associated stations from communicating with each other. Which of the following would BEST accomplish this requirement?

A. Wireless client isolation
B. Port security
C. Device geofencing
D. DHCP snooping

Correct Answer: A
Section:
Explanation:
Wireless client isolation is a feature on wireless routers that limits the connectivity between wireless devices connected to the same network. It prevents them from accessing resources on other wireless or wired devices, as a security measure to reduce attacks and threats. This feature can be useful for guest and BYOD SSIDs, but it can also be disabled on the router's settings. Reference:

https://www.howtogeek.com/179089/lock-down-your-wi-fi-network-with-your-routers-wireless- isolation-option/

QUESTION 79
A company requires a disaster recovery site to have equipment ready to go in the event of a disaster at its main datacenter. The company does not have the budget to mirror all the live data to the disaster recovery site. Which of the following concepts should the company select?

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

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

QUESTION 80
An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch. Which of the following command-line tools should the technician use to determine where the incident is occurring?

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

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

QUESTION 81
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.

Correct Answer: D
Section:
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. Reference: https://www.comptia.org/blog/what-is-link-light

QUESTION 82
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

Correct Answer: B
Section:
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. Reference:
https://www.comptia.org/blog/what-is-iaas

QUESTION 83
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

Correct Answer: B
Section:
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. Reference: https://www.adobe.com/sign/esignature- resources/sign-nda.html

QUESTION 84
Two remote offices need to be connected securely over an untrustworthy MAN. Each office needs to access network shares at the other site. Which of the following will BEST provide this functionality?

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

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

Reference: https://www.comptia.org/blog/what-is-a-site-to-site-vpn

QUESTION 85
A network requirement calls for segmenting departments into different networks. The campus network is set up with users of each department in multiple buildings. Which of the following should be configured to keep the design simple and efficient?

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

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

QUESTION 86
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

Correct Answer: A
Section:
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. Reference:
https://www.comptia.org/blog/what-is-syslog

QUESTION 87
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

Correct Answer: C
Section:
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.

Reference: https://www.comptia.org/blog/what-is-firmware

QUESTION 88
A network technician is investigating an issue with handheld devices in a warehouse. Devices have not been connecting to the nearest APs, but they have been connecting to an AP on the far side of the warehouse. Which of the following is the MOST likely cause of this issue?

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

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

QUESTION 89
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

Correct Answer: C
Section:
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.

QUESTION 90
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

Correct Answer: A
Section:
Explanation:
Reference:
https://www.techtarget.com/searchnetworking/definition/OSI#:~:text=The%20session%20layer,and %20terminates%20conversations%20between%20applications.
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.

QUESTION 91
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

Correct Answer: C
Section:
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.

QUESTION 92
A network administrator decided to use SLAAC in an extensive IPv6 deployment to alleviate IP address management. The devices were properly connected into the LAN but autoconfiguration of the IP address did not occur as expected. Which of the following should the network administrator verify?

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

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

QUESTION 93
Which of the following is used to provide networking capability for VMs at Layer 2 of the OSI model?

A. VPN
B. VRRP
C. vSwitch
D. VIP

Correct Answer: C
Section:
Explanation:
A vSwitch (virtual switch) is a software-based switch that provides networking capability for VMs (virtual machines) at Layer 2 of the OSI model. It connects the VMs to each other or to external networks using virtual NICs (network interface cards). A VPN (virtual private network) is a technology that creates a secure tunnel over a public network for remote access or site-to-site connectivity. VRRP (Virtual Router Redundancy Protocol) is a protocol that provides high availability for routers by creating a virtual router with multiple physical routers. A VIP (virtual IP) is an IP address that can be shared by multiple servers or devices for load balancing or failover purposes.

QUESTION 94
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

Correct Answer: C
Section:
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.

QUESTION 95
Which of the following would be used to expedite MX record updates to authoritative NSs?

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

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

QUESTION 96
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

Correct Answer: B
Section:
Explanation:
255.255.252.0 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.

QUESTION 97
A company is being acquired by a large corporation. As part of the acquisition process, the company's address should now redirect clients to the corporate organization page. Which of the following DNS records needs to be created?

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

Correct Answer: C
Section:
Explanation:
Reference: https://www.namecheap.com/support/knowledgebase/article.aspx/9604/2237/types-of- domain-redirects-301-302-url-redirects-url-frame-and-cname/#:~:text=CNAME%20record%20is%20actually%20not,often%20mistakenly%20used%20as%2 0such.&text=In%20other%20words%2C%20CNAME%20record,address%20of%20the%20destination %20hostname
CNAME (Canonical Name) is a type of DNS record that maps an alias name to another name, which can be either another alias or the canonical name of a host or domain. A CNAME record can be used to redirect clients from one domain name to another domain name, such as from the company's address to the corporate organization page. SOA (Start of Authority) is a type of DNS record that specifies authoritative information about a DNS zone, such as the primary name server, contact email address, serial number, refresh interval, etc., which does not redirect clients to another domain name. NS (Name Server) is a type of DNS record that specifies which name server is authoritative for a domain or subdomain, which does not redirect clients to another domain name. TXT (Text) is a type of DNS record that provides arbitrary text information about a domain or subdomain, such as SPF (Sender Policy Framework) records or DKIM (DomainKeys Identified Mail) records, which does not redirect clients to another domain name.

QUESTION 98
A user is having difficulty with video conferencing and is looking for assistance. Which of the following would BEST improve performance?

A. Packet shaping
B. Quality of service
C. Port mirroring
D. Load balancing

Correct Answer: B
Section:
Explanation:
Quality of service (QoS) is a mechanism that prioritizes network traffic based on different criteria, such as application type, source and destination address, port number, etc., and allocates bandwidth and resources accordingly. QoS would best improve performance for video conferencing, as it would ensure that video traffic gets higher priority and lower latency than other types of traffic on the network. Packet shaping is a technique that controls the rate or volume of network traffic by delaying or dropping packets that exceed certain thresholds or violate certain policies, which may not improve performance for video conferencing if it causes packet loss or jitter. Port mirroring is a technique that copies traffic from one port to another port on a switch for monitoring or analysis purposes, which does not improve performance for video conferencing at all. Load balancing is a technique that distributes network traffic across multiple servers or devices for improved availability and scalability, which does not

QUESTION 99
A network technician is configuring a new firewall for a company with the necessary access requirements to be allowed through the firewall. Which of the following would normally be applied as the LAST rule in the firewall?

A. Secure SNMP
B. Port security
C. Implicit deny
D. DHCP snooping

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

QUESTION 100
A systems administrator is running a VoIP network and is experiencing jitter and high latency. Which of the following would BEST help the administrator determine the cause of these issues?

A. Enabling RADIUS on the network
B. Configuring SNMP traps on the network
C. Implementing LDAP on the network
D. Establishing NTP on the network

Correct Answer: B
Section:
Explanation:
SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate with a network management system (NMS) for monitoring and configuration purposes. SNMP traps are unsolicited messages sent by network devices to the NMS when certain events or conditions occur, such as errors, failures, or thresholds. Configuring SNMP traps on the network would best help the administrator determine the cause of jitter and high latency on a VoIP network, as they would provide real-time alerts and information about the network performance and status. Enabling RADIUS on the network is not relevant to troubleshooting VoIP issues, as RADIUS is a protocol that provides authentication, authorization, and accounting services for network access. Implementing LDAP on the network is also not relevant to troubleshooting VoIP issues, as LDAP is a protocol that provides directory services for storing and querying information about users, groups, devices, etc. Establishing NTP on the network is not directly related to troubleshooting VoIP issues, as NTP is a protocol that synchronizes the clocks of network devices.

QUESTION 101
The following instructions were published about the proper network configuration for a videoconferencing device:
"Configure a valid static RFC1918 address for your network. Check the option to use a connection over NAT."
Which of the following is a valid IP address configuration for the device?

A. FE80::1
B. 100.64.0.1
C. 169.254.1.2
D. 172.19.0.2
E. 224.0.0.12

Correct Answer: D
Section:
Explanation:
172.19.0.2 is a valid IP address configuration for the device that uses a static RFC1918 address for the network and allows for a connection over NAT (Network Address Translation). RFC1918 addresses are private IP addresses that are not routable on the public Internet and are used for internal networks. The RFC1918 address ranges are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. NAT is a technique that translates private IP addresses to public IP addresses when communicating with external networks, such as the Internet. FE80::1 is an IPv6 link-local address that is not a static RFC1918 address and does not allow for a connection over NAT. 100.64.0.1 is an IPv4 address that belongs to the shared address space range (100.64.0.0/10) that is used for carrier-grade NAT (CGN) between service providers and subscribers, which is not a static RFC1918 address and does not allow for a connection over NAT. 169.254.1.2 is an IPv4 link-local address that is automatically assigned by a device when it cannot obtain an IP address from a DHCP server or manual configuration, which is not a static RFC1918 address

and does not allow for a connection over NAT. 224.0.0.12 is an IPv4 multicast address that is used for VRRP (Virtual Router Redundancy Protocol), which is not a static RFC1918 address and does not allow for a connection over NAT.

QUESTION 102
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

Correct Answer: B
Section:
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.

QUESTION 103
A network administrator needs to implement an HDMI over IP solution. Which of the following will the network administrator MOST likely use to ensure smooth video delivery?

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

Correct Answer: C
Section:
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.
Topic 3, Exam Pool C

QUESTION 104
A company with multiple routers would like to implement an HA network gateway with the least amount of downtime possible. This solution should not require changes on the gateway setting of the network clients. Which of the following should a technician configure?

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

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

QUESTION 105
A technician performed a manual reconfiguration of a firewall, and network connectivity was reestablished. Some connection events that were previously sent to a syslog server are no longer being generated by the firewal Which of Vie following should the technician perform to fix the Issue?

A. Adjust the proper logging level on the new firewall.
B. Tune the filter for logging the severity level on the syslog server.
C. Activate NetFlow traffic between the syslog server and the firewall
D. Restart the SNMP service running on the syslog server.

Correct Answer: A
Section:
Explanation:
Logging level is a setting that determines what types of events are recorded by a device and sent to a syslog server. Different logging levels have different severity levels, ranging from emergency to debug. If the technician performed a manual reconfiguration of the firewall, it is possible that the logging level was changed or reset to a lower level that does not include the connection events that were previously sent to the syslog server. To fix the issue, the technician should adjust the proper logging level on the new firewall to match the desired level of detail and severity for the connection events. Reference: Network+ Study Guide Objective 3.4: Explain common scanning, monitoring and patching processes and summarize their expected outputs. Subobjective: Syslog.

QUESTION 106
Switch 3 was recently added lo an existing stack to extend connectivity to various parts of the network. After the update, new employees were not able to print to the main networked copiers from then workstations. Following are the port configurations for the switch stack in question:

Switch 1:

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

Switch 2:

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

Switch 3:

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

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

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

Correct Answer: A, E
Section:

QUESTION 107
Several end users viewing a training video report seeing pixelated images while watching. A network administrator reviews the core switch and is unable to find an immediate cause. Which of the following BEST explains what is occurring?

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

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

QUESTION 108
An administrator notices that after contact with several switches in an MDF they failed due to electrostatic discharge. Which of the Mowing sensors should the administrator deploy to BEST monitor static electricity conditions in the MDF?

A. Temperature
B. Humidity
C. Smoke
D. Electrical

Correct Answer: B
Section:
Explanation:
"Humidity control prevents the buildup of static electricity and reduces the chances of electronic components becoming vulnerable to damage from electrostatic shock; not only can very low humidity lead to increased static electricity, but it can also contribute to health problems, such as skin irritation."

QUESTION 109
A medical building offers patients Wi-Fi in the waiting room. Which of the following security features would be the BEST solution to provide secure connections and keep the medical data protected?

A. Isolating the guest network
B. Securing SNMP
C. MAC filtering

D. Disabling unneeded switchports

Correct Answer: A
Section:

QUESTION 110
A malicious user is using special software 10 perform an on-path attack. Which of the following best practices should be configured to mitigate this threat?

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

Correct Answer: A
Section:

QUESTION 111
A systems administrator wants to use the least amount of equipment to segment two departments that nave cables terminating in the same room. Which of the following would allow this to occur?

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

Correct Answer: C
Section:

QUESTION 112
Two network technicians are installing a fiber-optic link between routers. The technicians used a light meter to verify the correct fibers However, when they connect the fibers to the router interface the link does not connect. Which of the following would explain the issue? (Select TWO).

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

Correct Answer: A, B
Section:

QUESTION 113
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 EIRP power settings.
B. Switch to 802.11n. disable channel auto-selection, and enforce channel bonding on the configuration.
C. Set up the AP to perform a dynamic selection of the frequency according to regulatory requirements.
D. Deactivate the band 5GHz to avoid Interference with the government radio

Correct Answer: C
Section:
Explanation:
The question asks about the best configuration for the WLAN being tested, which involveschannel bonding on an 802.11ac AP.Channel bonding is a technique that combines two or moreadjacent channels into a wider channel to increase the bandwidth and throughput of thewireless network1.
The answer is to set up the AP to perform a dynamic selection of the frequency according toregulatory requirements.This means that the AP will automatically choose the best availablechannel and adjust the transmit power based on the local regulations and the interferencelevel2.This way, the AP can avoid using the channels that are occupied by the government radiosystem, which may have higher priority and authority over the spectrum3.Upgrading the equipment to an AP that supports manual configuration of the EIRP powersettings is not the best solution, because it does not address the channel selection issue. EIRPstands for Effective Isotropic Radiated Power, which is the total power radiated by the antennain all directions. Manual configuration of the EIRP may allow the administrator to increase ordecrease the signal strength, but it may also violate the regulatory limits or cause moreinterference with other devices.Switching to 802.11n, disabling channel auto-selection, and enforcing channel bonding on theconfiguration is also not the best solution, because it may degrade the performance andcompatibility of the WLAN. 802.11n is an older standard than 802.11ac, which has lowermaximum data rates and fewer features. Disabling channel auto-selection may prevent the APfrom adapting to the changing environment and finding the optimal channel. Enforcing channelbonding may increase the bandwidth, but it may also increase the interference and reduce thenumber of available channels.Deactivating the band 5GHz to avoid interference with the government radio is not the bestsolution, because it may limit the functionality and capacity of the WLAN. The 5GHz band hasmore channels and less congestion than the 2.4GHz band, which makes it suitable for high-performance applications and devices. Deactivating the band 5GHz may force the WLAN to useonly the 2.4GHz band, which may reduce the speed, range, and reliability of the wirelessnetwork.Reference:Channel BondingDynamic Frequency SelectionRadio Regulations[EIRP Calculator][EIRP and Regulatory Domains][802.11n vs 802.11ac][Channel Auto-Selection][Channel Bonding and Interference][5GHz vs 2.4GHz][5GHz Band Deactivation]

QUESTION 114
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

Correct Answer: C
Section:
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.

QUESTION 115
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

Correct Answer: B
Section:

QUESTION 116
A technician removes an old PC from the network and replaces it with a new PC that is unable to connect to the LAN. Which of the Mowing is MOST likely the cause of the issue?

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

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

QUESTION 117
A network technician is having issues connecting an loT sensor to the internet The WLAN settings were enabled via a custom command line, and a proper IP address assignment was received on the wireless interlace. However, when trying to connect to the internet, only HTTP redirections are being received when data Is requested. Which of the following will point to the root cause of the Issue?

A. Verifying if an encryption protocol mismatch exists.
B. Verifying If a captive portal is active for the WLAN.
C. Verifying the minimum RSSI for operation in the device's documentation
D. Verifying EIRP power settings on the access point.

Correct Answer: C
Section:
Explanation:
A captive portal is a web page that is displayed to a user before they can access the internet or other network resources. This is often used in public or guest networks to present users with a login or terms and conditions page before they can access the internet. If a captive portal is active on the WLAN, it would explain why the IoT sensor is only receiving HTTP redirections when trying to connect to the internet.

QUESTION 118
A corporate client is experiencing global system outages. The IT team has identified multiple potential underlying causes throughout the enterprise Each team member has been assigned an area to trouble shoot. Which of the following approaches is being used?

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

Correct Answer: A
Section:

QUESTION 119
A network administrator is troubleshooting a connectivity performance issue. As part of the troubleshooting process, the administrator performs a traceout from the client to the server, and also from the server to the client. While comparing the outputs, the administrator notes they show different hops between the hosts. Which of the following BEST explains these findings?

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

Correct Answer: C
Section:

QUESTION 120
Which of the following describes the BEST device to configure as a DHCP relay?

A. Bridge
B. Router
C. Layer 2 switch
D. Hub

Correct Answer: B
Section:
Explanation:
Normally, routers do not forward broadcast traffic. This means that each broadcast domain must be served by its own DHCP server. On a large network with multiple subnets, this would mean provisioning and configuring many DHCP servers. To avoid this scenario, a DHCP relay agent can be configured to provide forwarding of DHCP traffic between subnets. Routers that can provide this type of forwarding are described as RFC 1542 compliant. The DHCP relay intercepts broadcast DHCP frames, applies a unicast address for the appropriate DHCP server, and forwards them over the interface for the subnet containing the server. The DHCP server can identify the original IP subnet from the packet and offer a lease from the appropriate scope. The DHCP relay also performs the reverse process of directing responses from the server to the appropriate client subnet.

QUESTION 121
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

Correct Answer: B
Section:

QUESTION 122
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

Correct Answer: A
Section:

QUESTION 123
Which of the following network devices can perform routing between VLANs?

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

D. Bridge

Correct Answer: B
Section:
Explanation:
https://www.practicalnetworking.net/stand-alone/routing-between- vlans/#:~:text=A%20router%20will%20perform%20the,to%20communicate%20with%20one%20anot her.

QUESTION 124
An international company is transferring its IT assets including a number of WAPs from the United States to an office in Europe for deployment. Which of the following considerations should the company research before Implementing the wireless hardware?

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

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

QUESTION 125
Network connectivity in an extensive forest reserve was achieved using fiber optics. A network fault was detected, and now the repair team needs to check the integrity of the fiber cable. Which of me following actions can reduce repair time?

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

Correct Answer: C
Section:

QUESTION 126
Which of the following would be used to enforce and schedule critical updates with supervisory approval and include backup plans in case of failure?

A. Business continuity plan
B. Onboarding and offboarding policies
C. Acceptable use policy
D. System life cycle
E. Change management

Correct Answer: A
Section:

QUESTION 127
Which of the following would be the MOST cost-effective recovery solution for a company's lower- priority applications?

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

Correct Answer: C
Section:

QUESTION 128
A technician is troubleshooting reports that a networked printer is unavailable. The printer's IP address is configured with a DHCP reservation, but the address cannot be pinged from the print server in the same subnet. Which of the following is MOST likely the cause of me connectivity failure?

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

Correct Answer: A
Section:
Explanation:
A VLAN is a virtual local area network that logically separates devices on the same physicalnetwork. VLANs can improve network performance, security, and management by reducingbroadcast domains and isolating traffic.
A DHCP reservation is a feature that allows a network administrator to assign a specific IPaddress to a device based on its MAC address. This ensures that the device always receives thesame IP address from the DHCP server, even if the lease expires or the device reboots.A networked printer is a device that can be shared by multiple users on the same network. Anetworked printer typically has a built-in network interface card (NIC) that allows it tocommunicate with other devices using TCP/IP protocols.A print server is a device or a software application that manages the printing requests frommultiple clients. A print server can also provide additional features such as print queuemanagement, printer driver installation, and printer status monitoring.A subnet is a logical division of an IP network that allows devices to communicate moreefficiently and securely. A subnet is defined by a network address and a subnet mask, whichdetermine the range of valid IP addresses within the subnet. Devices on the same subnet cancommunicate directly with each other without the need for a router.A ping is a network diagnostic tool that tests the connectivity and reachability between twodevices by sending and receiving echo packets. A ping request can fail for various reasons, suchas network congestion, firewall settings, routing issues, or device configuration errors.Based on the question, the networked printer is unavailable because it cannot be pinged fromthe print server in the same subnet. This means that there is a problem with the layer 2connectivity between the two devices, which is determined by the MAC addresses and theVLANs. The most likely cause of this problem is that the printer and the print server are ondifferent VLANs, which prevents them from communicating with each other. The other optionsare less likely because they affect the layer 3 connectivity, which is determined by the IPaddresses and the gateways. A DNS failure would not affect the ping request, since it uses IPaddresses and not hostnames. A DHCP scope exhaustion would not affect the printer, since ithas a DHCP reservation that guarantees its IP address. An incorrect gateway would not affectthe communication within the same subnet, since it is only used for routing packets to othernetworks.Reference:CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Devices and Technologies,Section 2.2: Network Device Functions and Features, Subsection: Print Servers, pp. 76-77.CompTIA Network+ N10-008 Study Guide, Chapter 3: Network Operations, Section 3.3:Network Configuration Management, Subsection: DHCP, pp. 144-146.CompTIA Network+ N10-008 Study Guide, Chapter 4: Network Security, Section 4.2: NetworkSegmentation and Isolation, Subsection: VLANs, pp. 202-204.Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 1.5: NetworkTroubleshooting Methodology, Subsection: Identify the Problem, pp. 16-17.
Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 2.2: Network Devices,Subsection: Print Servers, p. 28.Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 2.6: NetworkAddressing, Subsection: DHCP, p. 38.Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 2.7: NetworkAddressing, Subsection: Subnetting, p. 39.Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 3.5: NetworkSegmentation, Subsection: VLANs, p. 58.

QUESTION 129
Users are reporting intermittent Wi-Fi connectivity in specific parts of a building. Which of the following should the network administrator check FIRST when troubleshooting this issue? (Select TWO).

A. Site survey
B. EIRP
C. AP placement
D. Captive portal
E. SSID assignment
F. AP association time

Correct Answer: A, C
Section:

Explanation:
This is a coverage issue. WAP placement and power need to be checked. Site survey should be done NEXT because it takes a while.

QUESTION 130
A network manager is configuring switches in IDFs to ensure unauthorized client computers are not connecting to a secure wired network. Which of the following is the network manager MOST likely performing?

A. Disabling unneeded switchports
B. Changing the default VLAN
C. Configuring DHCP snooping
D. Writing ACLs to prevent access to the switch

Correct Answer: A
Section:
Explanation:
Disabling unneeded switchports is a securitybest practice that prevents unauthorized devices from connecting to the network andpotentially compromising its integrity or confidentiality. By disabling the switchports that arenot in use, the network manager reduces the attack surface and the risk of rogue devices, suchas laptops, printers, or cameras, from accessing the network. Disabling unneeded switchports
can also prevent MAC flooding attacks, which occur when an attacker sends a large number ofspoofed MAC addresses to a switch, causing it to overflow its MAC address table and forwardall traffic to all ports, effectively turning the switch into a hub. To disable a switchport, thenetwork manager can use the commandswitchport mode shutdownon the interfaceconfiguration mode of the switch. Changing the default VLAN, configuring DHCP snooping, andwriting ACLs are also security measures that can be applied to switches, but they are not themost likely ones in this scenario. Changing the default VLAN can prevent VLAN hopping attacks,which occur when an attacker sends frames with double 802.1Q tags to a switch, causing it toforward the frames to another VLAN. Configuring DHCP snooping can prevent DHCP spoofingattacks, which occur when an attacker sets up a rogue DHCP server on the network and offersfake IP addresses and gateway information to unsuspecting clients, redirecting their traffic tothe attacker's device. Writing ACLs can prevent unauthorized access to the switch or thenetwork resources, by filtering traffic based on source and destination IP addresses, ports,protocols, or other criteria.Reference: Network + N10-008 practice exam Flashcards | QuizletNetwork+ N10-008 Practice Test | CertBlaster | Free CompTIA Network+ Practice Test

QUESTION 131
Which of the following OSI model layers is where a technician would view UDP information?

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

Correct Answer: D
Section:

QUESTION 132
A technician installed an 8-port switch in a user's office. The user needs to add a second computer in the office, so the technician connects both PCs to the switch and connects the switch to the wall jack. However, the new PC cannot connect to network resources. The technician then observes the following:
• The new computer does not get an IP address on the client's VLAN.
• Both computers have a link light on their NICs.
• The new PC appears to be operating normally except for the network issue.
• The existing computer operates normally.
Which of the following should the technician do NEXT to address the situation?

A. Contact the network team to resolve the port security issue.
B. Contact the server team to have a record created in DNS for the new PC.
C. Contact the security team to review the logs on the company's SIEM.
D. Contact the application team to check NetFlow data from the connected switch.

Correct Answer: A
Section:

QUESTION 133
Which of the following devices have the capability to allow communication between two different subnetworks? (Select TWO).

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

Correct Answer: D, E
Section:

QUESTION 134
Which of the following describes traffic going in and out of a data center from the internet?

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

Correct Answer: B
Section:

QUESTION 135
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

Correct Answer: C
Section:

QUESTION 136
Which of the following is the MOST appropriate use case for the deployment of a clientless VPN?

A. Secure web access to internal corporate resources.
B. Upgrade security via the use of an NFV technology
C. Connect two data centers across the internet.
D. Increase VPN availability by using a SDWAN technology.

Correct Answer: A
Section:

QUESTION 137

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

Correct Answer: A
Section:

QUESTION 138
Which of the following options represents the participating computers in a network?

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

Correct Answer: A
Section:

QUESTION 139
A technician is trying to determine whether an LACP bundle is fully operational. Which of the following commands will the technician MOST likely use?

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

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/optical/cpt/r9_3/command/reference/cpt93_cr/cpt93_cr_c hapter_01000.html

QUESTION 140
Which of the following is conducted frequently to maintain an updated list of a system's weaknesses?

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

Correct Answer: D
Section:

QUESTION 141
Which of the following protocols is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links?

A. OSPF
B. RIPv2
C. QoS
D. STP

Correct Answer: A
Section:

QUESTION 142
A network administrator is planning a WLAN for a soccer stadium and was advised to use MU-MIMO to improve connection performance in high-density areas. The project requires compatibility with clients connecting using 2.4GHz or 5GHz frequencies. Which of the following would be the BEST wireless standard for this project?

A. 80211ac
B. 802.11ax
C. 802.11g
D. 80211n

Correct Answer: B
Section:

QUESTION 143
An auditor assessing network best practices was able to connect a rogue switch into a network Jack and get network connectivity. Which of the following controls would BEST address this risk?

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

Correct Answer: A
Section:

QUESTION 144
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

Correct Answer: A, B
Section:
Explanation:
A MAC address is a unique identifier assigned to a network interface card (NIC) that allows it tocommunicate on a physical network layer, such as Ethernet1.An IP address is a logical identifierassigned to a device that allows it to communicate on a network layer, such as IP2.A technician can use different methods to find the IP address of a device if they know its MACaddress. Two of the most common methods are looking at the ARP table and the DHCP leases.The ARP table is a data

structure that stores the mappings between IP addresses and MACaddresses on a device.ARP stands for Address Resolution Protocol, which is a network protocolthat enables devices to discover the MAC address of another device based on its IP address3.The ARP table is populated by sending ARP requests and receiving ARP replies, or byusing static ARP entries that are manually configured4.A technician can look at the ARP table of their own device or a nearby device, such as a routeror a switch, to find the IP address of a device with a known MAC address. For example, on aWindows device, the technician can use the commandarp -ato display the ARP table, and lookfor the entry that matches the MAC address. On a Cisco device, the technician can use thecommandshow ip arpto display the ARP table, and look for the entry that matches the MACaddress.The DHCP leases are the records of the IP addresses that are assigned by a DHCP server toDHCP clients. DHCP stands for Dynamic Host Configuration Protocol, which is a networkprotocol that enables devices to obtain IP addresses and other network configurationparameters automatically from a DHCP server. The DHCP leases contain information such as theIP address, the MAC address, the lease duration, and the expiration time of each DHCP client.A technician can look at the DHCP leases of the DHCP server that serves the network segmentwhere the device with the known MAC address is connected. For example, on a Windows DHCPserver, the technician can use the DHCP console to view the DHCP leases, and look for the entrythat matches the MAC address. On a Cisco DHCP server, the technician can use thecommandshow ip dhcp bindingto view the DHCP leases, and look for the entry that matches theMAC address.The other options are incorrect for the following reasons:C . IP route table is a data structure that stores the routes to different network destinations ona device. It does not store the MAC addresses of the devices on the network.D . DNS cache is a data structure that stores the mappings between domain names and IPaddresses on a device. DNS stands for Domain Name System, which is a network service thattranslates human-readable domain names into IP addresses. It does not store the MACaddresses of the devices on the network.E . MAC address table is a data structure that stores the mappings between MAC addresses andswitch ports on a switch. It does not store the IP addresses of the devices on the network.F . STP topology is a network design that uses the Spanning Tree Protocol (STP) to prevent loopsand create a loop-free logical topology on a switched network. It does not store the IPaddresses or the MAC addresses of the devices on the network.Reference:1: MAC address - Wikipedia2: IP address - Wikipedia

QUESTION 145
A technician needs to configure a routing protocol for an internet-facing edge router. Which of the following routing protocols will the technician MOST likely use?

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

Correct Answer: A
Section:

QUESTION 146
Which of the following compromises internet-connected devices and makes them vulnerable to becoming part of a botnet? (Select TWO)

A. Deauthentication attack
B. Malware infection
C. IP spoofing
D. Firmware corruption
E. Use of default credentials
F. Dictionary attack

Correct Answer: B, E
Section:
Explanation:
A botnet is a network of compromised devices that are remotely controlled by a maliciousactor, usually for the purpose of launching distributed denial-of-service (DDoS) attacks, sendingspam, stealing data, or performing other malicious activities1.A malware infection is a common way of compromising internet-connected devices and makingthem part of a botnet. Malware is any software that is designed to harm or exploit a device, anetwork, or a user.Malware can be delivered through various methods, such as phishing emails,malicious downloads, drive-by downloads, or removable media2.Malware can infect a deviceand allow a remote attacker to take control of it, monitor its activities, or use its resources3 The use of default credentials is another common way of compromising internet-connecteddevices and making them part of a botnet. Default credentials are the username and passwordcombinations that are preconfigured by the manufacturer or vendor of a device, such as arouter, a camera, or a printer. Default credentials are often easy to guess or find online, andmany users do not change them after setting up their devices. This makes the devicesvulnerable to unauthorized access and manipulation by attackers who can scan the internet fordevices with default credentials and add them to their botnet .A deauthentication attack is a type of wireless attack that aims to disconnect a legitimate userfrom a wireless network by sending spoofed deauthentication frames to the user's device orthe access point (AP). A deauthentication attack can cause a denial of service, disrupt networkcommunication, or facilitate other attacks, such as capturing the handshake during thereconnection process. However, a deauthentication attack does not compromise the device ormake it part of a botnet.IP spoofing is a technique of forging the source IP address of a packet to make it appear as if itcame from a different device or location. IP spoofing can be used to bypass security filters, hidethe identity of the attacker, or launch reflection or amplification attacks. However, IP spoofingdoes not compromise the device or make it part of a botnet, unless it is combined with othermethods, such as malware infection or exploitation of vulnerabilities.Firmware corruption is a condition where the firmware of a device, which is the software thatcontrols its basic functions and operations, becomes damaged or altered due to variousreasons, such as power surges, hardware failures, malicious attacks, or improper updates.Firmware corruption can cause the device to malfunction, lose data, or become inaccessible.However, firmware corruption does not compromise the device or make it part of a botnet,unless it is caused by a malicious attack that replaces the firmware with a malicious version.A dictionary attack is a type of brute-force attack that tries to guess the password of a user or adevice by using a list of common or likely passwords, such as those found in a dictionary, adatabase, or a previous breach. A dictionary attack can be used to compromise a device andmake it part of a botnet, but only if the device has a weak or predictable password. Therefore, adictionary attack is not a direct way of compromising a device, but rather a means of exploitingthe use of default or weak credentials.

QUESTION 147
Several employees have expressed concerns about the company monitoring their internet activity when they are working from home. The company wants to mitigate this issue and reassure employees that their private

internet activity is not being monitored. Which of the following would satisfy company and employee needs?

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

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

QUESTION 148
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

Correct Answer: C
Section:
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.

QUESTION 149
Which of the following protocols would enable a company to upgrade its internet connection by acquiring its own public IP prefixes and autonomous system number?

A. EIGRP
B. BGP
C. IPv6
D. MPLS

Correct Answer: B
Section:
Explanation:
BGP is a routing protocol that is used to exchange routing information between different autonomous systems (ASes) on the internet. An autonomous system is a network or group of networks that is under the same administrative control and uses a common routing protocol. By acquiring its own public IP prefixes and autonomous system number, a company can use BGP to advertise these prefixes to other ASes and establish its own internet connection. This would enable the company to have more control over its internet connection and potentially improve its connectivity.EIGRP (Enhanced Interior Gateway Routing Protocol) is a routing protocol used within a single autonomous system, so it would not be used to establish a connection to the internet. IPv6 is a version of the Internet Protocol (IP) used to identify devices on a network. It is not a routing protocol and would not be used to establish an internet connection.MPLS (Multi-Protocol Label Switching) is a networking technology that is used to route packets between different networks. It is not a routing protocol and would not be used to establish an internet connection.

QUESTION 150
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

Correct Answer: E, F
Section:
Explanation:
A disaster recovery plan is a document that outlines the procedures and steps to restore thenormal operations of a network in the event of a disaster, such as a fire, flood, power outage,cyberattack, or human error. It includes the roles and responsibilities of the staff, the backupand recovery strategies, the communication channels, the testing and maintenance schedules,and the inventory of the network assets and resources. A disaster recovery plan needs to beupdated to reflect any changes in the network topology, configuration, or equipment, such asthe installation of an additional IDF (Intermediate Distribution Frame), which is a wiring closetthat connects the MDF (Main Distribution Frame) to the end devices. Updating the disasterrecovery plan ensures that the network administrator has the most accurate and currentinformation to restore the network in case of a disaster.A physical network diagram is a visual representation of the physical layout and connections ofthe network devices, such as routers, switches, firewalls, servers, workstations, printers, andcables. It shows the location, name, IP address, MAC address, and port number of each device,as well as the type, length, and color of each cable. A physical network diagram needs to beupdated to reflect any changes in the network infrastructure, such as the installation of anadditional IDF, which adds more devices and cables to the network. Updating the physicalnetwork diagram helps the network administrator to troubleshoot, monitor, and document thenetwork performance and status.
A data loss prevention policy is a document that defines the rules and guidelines to prevent theunauthorized access, disclosure, modification, or deletion of sensitive or confidential data onthe network. It includes the classification of the data, the encryption and backup methods, theaccess control and authentication mechanisms, the audit and logging procedures, and theincident response and reporting protocols. A data loss prevention policy does not need to beupdated to reflect the installation of an additional IDF, unless the IDF contains devices or cablesthat handle sensitive or confidential data, in which case the policy should specify the securitymeasures and controls for those devices or cables.A BYOD (Bring Your Own Device) policy is a document that regulates the use of personaldevices, such as smartphones, tablets, laptops, or USB drives, on the network. It includes therequirements and restrictions for the devices, the network access and security policies, the userrights and responsibilities, the support and maintenance services, and the legal and ethicalimplications. A BYOD policy does not need to be updated to reflect the installation of anadditional IDF, unless the IDF affects the network access or security of the personal devices, inwhich case the policy should clarify the impact and the actions for the users.An acceptable use policy is a document that specifies the rules and expectations for theappropriate and ethical use of the network resources and services by the users. It includes thepurpose and scope of the network, the acceptable and unacceptable behaviors and activities,the consequences and penalties for violations, and the user acknowledgment and agreement.An acceptable use policy does not need to be updated to reflect the installation of an additionalIDF, unless the IDF changes the purpose or scope of the network, in which case the policyshould inform the users of the changes and the implications.A non-disclosure agreement is a legal contract that binds the parties involved in the networkproject or service to keep the confidential information secret and not to share it with anyunauthorized third parties. It includes the definition and scope of the confidential information,the duration and termination of the agreement, the exceptions and exclusions, the remediesand damages, and the signatures and dates of the parties. A non-disclosure agreement doesnot need to be updated to reflect the installation of an additional IDF, unless the IDF involvesconfidential information that is not covered by the existing agreement, in which case theagreement should be amended or renewed to include the new information.

QUESTION 151
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

Correct Answer: D
Section:
Explanation:
VoIP phone is a device that uses voice over IP (VoIP) technology to transmit and receive voicecalls over a network. A VoIP phone typically has a built-in switch that allows a computer to beconnected to the same network port as the phone, sharing the same physical link andbandwidth.A VLAN tag is a piece of information that is added to the header of a network frame to indicatewhich virtual LAN (VLAN) it belongs to. A VLAN is a logical grouping of network devices thatshare the same broadcast domain, regardless of their physical location or connection. VLANscan help to isolate traffic, improve security, and reduce congestion on a network.A VLAN tag is required to provide network connectivity to the computer that is connected tothe VoIP phone, because the phone and the computer may belong to different VLANs. Forexample, the phone may belong to a voice VLAN that is dedicated for VoIP traffic, while thecomputer may belong to a data VLAN that is used for general network access. Without a VLANtag, the switch that connects to the VoIP phone would not be able to distinguish between theframes from the phone and the frames from the computer, and would not be able to forwardthem to the correct destination VLAN.Therefore, option D is the most likely answer, as the VLAN tags need to be configured correctlyto provide network connectivity to the computer. The switch port that connects to the VoIPphone needs to be configured as a trunk port, which can carry multiple VLANs, and the VoIPphone needs to be configured to add the appropriate VLAN tag to the frames from thecomputer.Option A is not a likely answer, as the port duplex settings determine the mode of datatransmission between the switch and the VoIP phone. The port duplex settings can be either
half-duplex, which means that data can be transmitted in one direction at a time, or full-duplex,which means that data can be transmitted in both directions simultaneously. The port duplexsettings do not affect the VLAN tags or the network

connectivity to the computer.Option B is also not a likely answer, as the port aggregation is a technique that combinesmultiple physical ports into a single logical port, increasing the bandwidth and redundancy ofthe link. The port aggregation does not affect the VLAN tags or the network connectivity to thecomputer.Option C is also not a likely answer, as the ARP settings are related to the address resolutionprotocol (ARP), which is a protocol that maps a network layer address, such as an IP address, toa data link layer address, such as a MAC address. The ARP settings do not affect the VLAN tagsor the network connectivity to the computer.Option E is also not a likely answer, as the MDIX settings are related to the medium dependentinterface crossover (MDIX), which is a feature that allows a switch to automatically detect thetype of cable that is connected to a port, and adjust the pinout accordingly. The MDIX settingsdo not affect the VLAN tags or the network connectivity to the computer.CompTIA Network+ N10-008 Study Guide, Chapter 3: Network Architecture, Section 3.1:Network Topologies and Technologies, Page 1361Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 3.1: Network Topologiesand Technologies, Page 232What is a VoIP Phone? | Definition and Examples3What is a VLAN Tag? | Definition and Examples4How to Configure VLANs on a VoIP Phone - Cisco5

QUESTION 152
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

Correct Answer: B
Section:
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.
Reference: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.2:
Given a scenario, use appropriate network hardening techniques.

QUESTION 153
Which of the following would be the BEST choice to connect branch sites to a main office securely?

A. VPN headend
B. Proxy server
C. Bridge
D. Load balancer

Correct Answer: A
Section:
Explanation:
Host-to-Site, or Client-to-Site, VPN allows for remote servers, clients, and other hosts to establish tunnels through a VPN gateway (or VPN headend) via a private network. The tunnel between the headend and the client host encapsulates and encrypts data.

QUESTION 154
A network administrator is designing a wireless network. The administrator must ensure a rented office space has a sufficient signal. Reducing exposure to the wireless network is important, but it is secondary to the primary objective. Which of the following would MOST likely facilitate the correct accessibility to the Wi-Fi network?

A. Polarization
B. Channel utilization
C. Channel bonding
D. Antenna type

E. MU-MIMO

Correct Answer: D
Section:
Explanation:
Theantenna typeis the factor that would most likely facilitate the correct accessibility to the Wi-Fi network, as it determines the shape, direction, and range of the wireless signal12.Differenttypes of antennas have different characteristics, such as gain, beamwidth, and polarization, thataffect how well they can cover a given area and overcome obstacles or interference12.Forexample, an omnidirectional antenna can radiate the signal in all directions, while a directionalantenna can focus the signal in a specific direction12. By choosing the appropriate antenna typefor the rented office space, the network administrator can ensure a sufficient signal and reduceexposure to the wireless network.Polarizationis the orientation of the electric field of the wireless signal, which can be eithervertical, horizontal, or circular12.Polarization affects the compatibility and performance of thewireless communication, as the transmitter and receiver antennas should have the samepolarization to avoid signal loss12.However, polarization alone would not facilitate the correctaccessibility to the Wi-Fi network, as it depends on the antenna type and the environment12.Channel utilizationis the measure of how much a wireless channel is occupied by datatransmission, management frames, or control frames13.Channel utilization affects theefficiency and throughput of the wireless network, as a high channel utilization can indicatecongestion, interference, or contention13.However, channel utilization alone would notfacilitate the correct accessibility to the Wi-Fi network, as it depends on the network design,configuration, and demand13.Channel bondingis the technique of combining two adjacent channels into one wider channel toincrease the bandwidth and throughput of the wireless network1.Channel bonding can improvethe performance of the wireless network, especially for applications that require high datarates, such as video streaming1.However, channel bonding alone would not facilitate the
correct accessibility to the Wi-Fi network, as it also introduces some challenges, such asincreased interference, reduced channel availability, and compatibility issues1.MU-MIMO(Multi-User Multiple Input Multiple Output) is a technology that allows a wirelessaccess point to transmit data to multiple devices simultaneously using multiple antennas andspatial streams1.MU-MIMO can enhance the capacity and efficiency of the wireless network,especially for high-density environments, such as offices, classrooms, or stadiums1.However,MU-MIMO alone would not facilitate the correct accessibility to the Wi-Fi network, as it alsorequires some conditions, such as compatible devices, sufficient signal strength, and optimalantenna placement1.1: CompTIA Network+ N10-008 Study Guide, Chapter 4: Wireless Technologies2: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 42: Wireless Antennas3: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 43: WirelessTroubleshooting: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 41: Wireless Channels: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 40: Wireless Technologies

QUESTION 155
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

Correct Answer: A
Section:

QUESTION 156
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

Correct Answer: C
Section:
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.

QUESTION 157
During a client audit, a network analyst is tasked with recommending changes to upgrade the client network and readiness. Afield technician has submitted the following report:

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

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

A. Electrical
B. Humidity
C. Flooding
D. Temperature

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

QUESTION 158
During an annual review of policy documents, a company decided to adjust its recovery time frames. The company agreed that critical applications can be down for no more than six hours, and the acceptable amount of data loss is no more than two hours. Which of the following should be documented as the RPO?

A. Two hours
B. Four hours
C. Six hours
D. Eight hours

Correct Answer: A
Section:
Explanation:
" RPO designates the variable amount of data that will be lost or will have to be re-entered during network downtime. RTO designates the amount of "real time" that can pass before the disruption begins to seriously and unacceptably impede the flow of normal business operations."

QUESTION 159
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

Correct Answer: A
Section:
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.

QUESTION 160
Which of the following would be BEST to install to find and block any malicious users within a network?

A. IDS
B. IPS
C. SCADA
D. ICS

Correct Answer: B
Section:
Explanation:
IPS takes action itself to block the attempted intrusion or otherwise remediate the incident. IDS is designed to only provide an alert about a potential incident, which enables a security operations center (SOC) analyst to investigate the event and determine whether it requires further action.

QUESTION 161
Which of the following records can be used to track the number of changes on a DNS zone?

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

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

QUESTION 162
A network technician is troubleshooting a new web server connectivity issue. The network technician discovers the following on the support ticket
• The server's IP address can be pinged from the client PCs,
• Access to the web resource works correctly when on the server's console.
• No clients can access the servers data via URL.
• The server does not have a firewall configured
• No ACLs are preventing connectivity from the client's network.
• All services on the server are operating normally,
which was confirmed by the server team.
Which of the following actions will resolve the issue?

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

Correct Answer: C
Section:

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

QUESTION 163
A Chief Executive Officer and a network administrator came to an agreement With a vendor to purchase new equipment for the data center A document was drafted so all parties would be Informed about the scope of the project before It started. Which of the following terms BEST describes the document used?

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

Correct Answer: B
Section:
Explanation:
The document used to inform all parties about the scope of the project before it starts is likely a project charter.
A project charter is a document that outlines the key aspects of a project, including the project's objectives, scope, stakeholders, and resources. It serves as a formal agreement between the project team and the stakeholders, and helps to define the project's goals and constraints.
A project charter typically includes information about the project's scope, including the specific deliverables that are expected and any constraints or limitations that may impact the project. It may also include details about the project team and stakeholders, the project schedule and budget, and the roles and responsibilities of each party.
By creating a project charter, the Chief Executive Officer and the network administrator can ensure that all parties involved in the project have a clear understanding of the project's goals and objectives, and can help to prevent misunderstandings or miscommunications during the project. What is in a project charter?
A project charter is a formal short document that states a project exists and provides project managers with written authority to begin work. A project charter document describes a project to create a shared understanding of its goals, objectives and resource requirements before the project is scoped out in detail.
What are the 5 elements of the project charter?
What Are the Contents of a Project Charter? A project charter should always include an overview, an outline of scope, an approximate schedule, a budget estimate, anticipated risks, and key stakeholders

QUESTION 164
A technician is trying to install a VoIP phone, but the phone is not turning on. The technician checks the cable gong from the phone to the switch, and the cable is good. Which of the following actions IS needed for this phone to work?

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

Correct Answer: A
Section:

QUESTION 165
Which of the following compromises internet-connected devices and makes them vulnerable to becoming part of a botnet? (Select TWO).

A. Deauthentication attack
B. Malware infection
C. IP spoofing
D. Firmware corruption
E. Use of default credentials

F. Dictionary attack

Correct Answer: B, E
Section:

QUESTION 166
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

Correct Answer: A
Section:

QUESTION 167
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

Correct Answer: C
Section:

QUESTION 168
A network administrator needs to configure a server to use the most accurate NTP reference available. Which of the following NTP devices should the administrator select?

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

Correct Answer: A
Section:
Explanation:
Stratum 1 devices are the most accurate ntp time sources accessible via a network connection. A Stratum 1 device would normally be synchronised via a Stratum 0 reference clock.
Reference: https://endruntechnologies.com/products/ntp-time-servers/stratum1

QUESTION 169
A Fortune 500 firm is deciding On the kind or data center equipment to install given its five-year budget Outlook. The Chief Information comparing equipment based on the life expectancy Of different models. Which Of the following concepts BEST represents this metric?

A. MTBF

B. MTRR
C. RPO
D. RTO

Correct Answer: A
Section:

QUESTION 170
While setting up a new workstation, a technician discovers that the network connection is only 100 full duplex (FD), although it is connected to a gigabit switch.
While reviewing the interface information in the switch CLI, the technician notes the port is operating at IOOFD but Shows many RX and TX errors. The technician moves the computer to another switchport and experiences the same issues.
Which of the following is MOST likely the cause of the low data rate and port errors?

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

Correct Answer: B
Section:

QUESTION 171
A network administrator wants to check all network connections and see the output in integer form. Which of the following commands should the administrator run on the command line?

A. netstat
B. netstat -a
C. netstat —e
D. netstat —n

Correct Answer: D
Section:
Explanation:
Thenetstat -ncommand displays active TCP connections, but addresses and port numbers areexpressed numerically and no attempt is made to determine names12.This option can be usefulfor checking the output in integer form, as well as for avoiding possible delays caused by nameresolution12.Thenetstatcommand without any parameters displays active TCP connections, but addressesand port numbers are resolved to their corresponding names, such as hostnames and servicenames12.This option can be less informative and more time-consuming than the -n option12

QUESTION 172
A Network engineer is investigating issues on a Layer 2 Switch. The department typically snares a Switchport during meetings for presentations, but atter the first user Shares, no Other users can connect. Which Of the following is MOST likely related to this issue?

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

Correct Answer: C
Section:

QUESTION 173
Which of the following would MOST likely utilize PoE?

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

Correct Answer: A
Section:
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.

QUESTION 174
An administrator is attempting to add a new system to monitoring but is unsuccessful. The administrator notices the system is similar to another one on the network; however, the new one has an updated OS version. Which of the following should the administrator consider updating?

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

Correct Answer: A
Section:

QUESTION 175
A network engineer needs to pass both data and telephony on an access port. Which or the following features should be configured to meet this requirement?

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

Correct Answer: A
Section:

QUESTION 176
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

Correct Answer: D
Section:
Explanation:
The end user can access local network shares and intranet pages, which means that the IPaddress and the subnet mask are configured correctly and the network interface is workingproperly.However, the end user is unable to access the internet or remote resources, which means thatthere is a problem with the name resolution or the routing of the traffic.The gateway address is responsible for routing the traffic to the destination network, whichcould be on the internet or another subnet. If the gateway address is incorrect, the end userwould not be able to reach any network outside the local subnet.The DNS servers are responsible for resolving the domain names to the IP addresses, which areneeded to communicate with the internet or remote resources. If the DNS servers are incorrect,the end user would not be able to resolve the names of the websites or servers they want toaccess.

QUESTION 177
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

Correct Answer: B, D
Section:

QUESTION 178
A technician wants to monitor and provide traffic segmentation across the network. The technician would like to assign each department a specific identifier. Which of the following will the technician MOST likely use?

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

Correct Answer: C
Section:
Explanation:
To monitor and provide traffic segmentation across the network, a technician may use the concept of VLANs (Virtual Local Area Networks). VLANs are a way of dividing a single physical network into multiple logical networks, each with its own unique identifier or "tag."
By assigning each department a specific VLAN identifier, the technician can segment the network traffic and ensure that the different departments' traffic is kept separate from one another. This can help to improve network security, performance, and scalability, as well as allowing for better monitoring and control of the network traffic.
To implement VLANs, the technician will need to configure VLAN tagging on the network devices, such as switches and routers, and assign each department's devices to the appropriate VLAN. The technician may also need to configure VLAN trunking to allow the different VLANs to communicate with each other.
By using VLANs, the technician can effectively monitor and segment the network traffic, providing better control and visibility into the network.

QUESTION 179
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

Correct Answer: B
Section:
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."

QUESTION 180
A network technician needs to ensure that all files on a company's network can be moved in a safe and protected manner without interception from someone who is not the intended recipient. Which of the following would allow the network technician to meet these requirements?

A. FTP
B. TFTP
C. SMTP
D. SFTP

Correct Answer: D
Section:

QUESTION 181
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

Correct Answer: B
Section:
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.

QUESTION 182
Which of the following documents would be used to define uptime commitments from a provider, along with details on measurement and enforcement?

A. NDA
B. SLA
C. MOU
D. AUP

Correct Answer: B
Section:

Explanation:
A service level agreement (SLA) is a document that is used to define uptime commitments from a provider, along with details on measurement and enforcement. An SLA is a contract between a service provider and a customer that outlines the level of service that the provider is committed to providing and the terms under which that service will be delivered.

QUESTION 183
A company ranis out a largo event space and includes wireless internet access for each tenant. Tenants reserve a two-hour window from the company each week, which includes a tenant-specific SSID However, all users share the company's network hardware.

Wireless encryption	WPA2
Captive portal	Disabled
AP isolation	Enabled
Subnet mask	255.255.255.0
DNS server	10.0.0.1
Default gateway	10.1.10.1
DHCP scope begin	10.1.10.10
DHCP scope end	10.1.10.150
DHCP lease time	24 hours

The network support team is receiving complaints from tenants that some users are unable to connect to the wireless network Upon investigation, the support teams discovers a pattern indicating that after a tenant with a particularly large attendance ends its sessions, tenants throughout the day are unable to connect.
The following settings are common lo all network configurations:
Which of the following actions would MOST likely reduce this Issue? (Select TWO).

A. Change to WPA encryption
B. Change the DNS server to 10.1.10.1.
C. Change the default gateway to 10.0.0.1.
D. Change the DHCP scope end to 10.1.10.250
E. Disable AP isolation
F. Change the subnet mask lo 255.255.255.192.
G. Reduce the DHCP lease time to four hours.

Correct Answer: D, G
Section:

QUESTION 184
Which of the following would be increased by adding encryption to data communication across the network?

A. Availability
B. Integrity
C. Accountability
D. Confidentiality

Correct Answer: D
Section:
Explanation:
Confidentiality is the property of preventing unauthorized access or disclosure of data. Encryption is a method of transforming data into an unreadable format that can only be decrypted by authorized parties who have the correct key. Encryption can increase the confidentiality of data communication across the network by making it harder for attackers to intercept or eavesdrop on the data.
Reference: Network+ Study Guide Objective 4.1: Summarize the purposes of physical security devices. Subobjective: Encryption.

QUESTION 185
Which of the following uses the link-state routing algorithm and operates within a single autonomous system?

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

Correct Answer: B
Section:
Explanation:
OSPF uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks

QUESTION 186
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

Correct Answer: B
Section:

QUESTION 187
Which of the following layers of the OSI model receives data from the application layer and converts it into syntax that is readable by other devices on the network?

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

Correct Answer: C
Section:

QUESTION 188
During the troubleshooting of an E1 line, the point-to-point link on the core router was accidentally unplugged and left unconnected for several hours. However, the network management team was not notified. Which of the following could have been configured to allow early detection and possible resolution of the issue?

A. Traps
B. MIB
C. OID
D. Baselines

Correct Answer: A
Section:
Explanation:
Traps are unsolicited messages sent by network devices to a network management system (NMS) when an event or a change in status occurs. Traps can help notify the network management team of any issues or problems on the network, such as a link failure or a device reboot. Traps can also trigger actions or alerts on the NMS, such as sending an email or logging the event. MIB stands for Management Information Base and is a database of information that can be accessed and managed by an NMS using SNMP (Simple Network Management Protocol). OID stands for Object Identifier and is a unique name that identifies a specific variable in the MIB. Baselines are measurements of normal network performance and behavior that can be used for comparison and analysis.
Reference: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.5:
Given a scenario, use remote access methods.

QUESTION 189
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

Correct Answer: A
Section:

QUESTION 190
A technician is installing the Wi-Fi infrastructure for legacy industrial machinery at a warehouse. The equipment only supports 802.11a and 802.11b standards. Speed of transmission is the top business requirement. Which of the following is the correct maximum speed for this scenario?

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

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

QUESTION 191
A technician is deploying a new SSID for an industrial control system. The control devices require the network to use encryption that employs TKIP and a symmetrical password to connect. Which of the following should the technician configure to ensure compatibility with the control devices?

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

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

QUESTION 192
Which of the following ports should be used to securely receive mail that is synchronized across multiple devices?

A. 25
B. 110
C. 443
D. 993

Correct Answer: D
Section:

QUESTION 193
A technician is configuring a static IP address on a new device in a newly created subnet. The work order specifies the following requirements:
• The IP address should use the highest address available in the subnet.
• The default gateway needs to be set to 172.28.85.94.
• The subnet mask needs to be 255.255.255.224.
Which of the following addresses should the engineer apply to the device?

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

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

QUESTION 194
Which of the following is most likely to have the HIGHEST latency while being the most accessible?

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

Correct Answer: A
Section:

QUESTION 195
Which of the following commands can be used to display the IP address, subnet address, gateway address, and DNS address on a Windows computer?

A. netstat -a
B. ifconfig
C. ip addr
D. ipconfig /all

Correct Answer: D
Section:
Explanation:
The ipconfig command is a utility that allows you to view and modify the network configuration of a Windows computer. By running the command "ipconfig /all", you can view detailed information about the network configuration of your computer, including the IP address, subnet mask, default gateway, and DNS server addresses.
Option A (netstat -a) is a command that displays active network connections and their status, but it does not display IP address or other network configuration information. Option B (ifconfig) is a command used on Linux and Unix systems to view and modify network configuration, but it is not available on Windows. Option C (ip addr) is a command used on Linux and Unix systems to view and modify network configuration, but it is not available on Windows.

QUESTION 196
An office area contains two PoE-enabled WAPs. After the area was remodeled, new cable uplinks were installed in the ceiling above the fluorescent lights. However, after the WAPs were reconnected, users reported slowness and application errors. An intern reviewed the network and discovered a lot of CRC errors. A network engineer reviewed the intern's work and realized UTP cabling was used. Which of the following is the MOST likely cause of the CRC errors?

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

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

QUESTION 197
Several users with older devices are reporting intermittent connectivity while in an outdoor patio are a. After some research, the network administrator determines that an outdoor WAP might help with the issue. However, the company does not want the signal to bleed into the building and cause interference. Which of the following should the network administrator perform to BEST resolve the issue?

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

Correct Answer: C
Section:

QUESTION 198
A network engineer developed a plan of action to resolve an ongoing issue. Which of the following steps should the engineer take NEXT?

A. Verify full system functionality and implement preventative measures.
B. Implement the solution to resolve the problem.
C. Document findings, actions, outcomes, and lessons learned.
D. Establish a theory of probable cause.

Correct Answer: B
Section:
Explanation:
Network troubleshooting is a repeatable process, which means that you can break it down into clear steps that anyone can follow.
Identify the Problem. ...
Develop a Theory. ...
Test the Theory. ...
Plan of Action. ...
Implement the Solution. ...
Verify System Functionality. ...
Document the Issue.
Theory of probable cause is before Plan of action.
https://www.comptia.org/content/guides/a-guide-to-network-troubleshooting

QUESTION 199
Which of the following can have multiple VLAN interfaces?

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

Correct Answer: B
Section:

QUESTION 200
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

Correct Answer: A
Section:
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.

QUESTION 201

Which of the following is the IEEE link cost for a Fast Ethernet interface in STP calculations?

A. 2
B. 4
C. 19
D. 100

Correct Answer: D
Section:
Explanation:
The IEEE standard for link cost for a Fast Ethernet interface is 100, and for a Gigabit Ethernet interface is 19. These values are based on the bandwidth of the interface, with lower values indicating a higher-bandwidth interface.

QUESTION 202
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

Correct Answer: A
Section:
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.

QUESTION 203
A company is designing a SAN and would like to use STP as its medium for communication. Which of the following protocols would BEST suit me company's needs?

A. SFTP
B. Fibre Channel
C. iSCSI
D. FTP

Correct Answer: B
Section:
Explanation:
A SAN also employs a series of protocols enabling software to communicate or prepare data for storage. The most common protocol is the Fibre Channel Protocol (FCP), which maps SCSI commands over FC technology. The iSCSI SANs will employ an iSCSI protocol that maps SCSI commands over TCP/IP.
STP (Spanning Tree Protocol) is a protocol used to prevent loops in Ethernet networks, and it is not a medium for communication in a storage area network (SAN). However, Fibre Channel is a protocol that is specifically designed for high-speed data transfer in SAN environments. It is a dedicated channel technology that provides high throughput and low latency, making it ideal for SANs. Therefore, Fibre Channel would be the best protocol

for the company to use for its SAN. SFTP (Secure File Transfer Protocol), iSCSI (Internet Small Computer System Interface), and FTP (File Transfer Protocol) are protocols used for transferring files over a network and are not suitable for use in a SAN environment.

QUESTION 204
Given the following Information:

Connection	Cable length	Cable type	Configuration
PC A to switch 1	394ft (120m)	Cat 5	Straight through
Switch 1 to switch 2	3.3ft (1m)	Cat 6	Crossover
Switch 2 to PC B	16ft (5m)	Cat 5	Straight through

Which of the following would cause performance degradation between PC A and PC B'?

A. Attenuation
B. Interference
C. Decibel loss
D. Incorrect pinout

Correct Answer: A
Section:
Explanation:
Attenuation is the loss of signal strength as it travels over a distance or through a medium. It ismeasured in decibels (dB) and can affect the quality and reliability of network communication.In this scenario, the connection from PC A to switch 1 is using a Cat 5 cable with a length of394ft (120m), which exceeds the recommended maximum length of 328ft (100m) for twisted-pair cables. This can cause significant attenuation and performance degradation between PC Aand PC B.To solve this problem, the network technician should either reduce the cable length, use ahigher category cable, or insert a repeater or amplifier device to boost the signal strength.Interference is the unwanted noise or signal that affects the network communication. It can becaused by electromagnetic sources, such as power lines, motors, or wireless devices, or bycrosstalk, which is the interference between adjacent wires in a cable. Interference can alsoaffect the network performance, but it is not the most likely cause in this scenario, as it wouldaffect all the connections, not just the one with the excessive cable length.Decibel loss is another term for attenuation, so it is not a separate option. Incorrect pinout isthe wrong arrangement of wires in a cable connector, which can prevent the network devicesfrom communicating properly. However, this is not the most likely cause in this scenario, as thecable configuration is correct (straight through) for the connection from PC A to switch

QUESTION 205
A new office space is being designed. The network switches are up. but no services are running yet A network engineer plugs in a laptop configured as a DHCP client to a switch Which ol the following IP addresses should be assigned to the laptop?

A. 10.1.1.1
B. 169.254.1.128
C. 172 16 128 128
D. 192 168.0.1

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

QUESTION 206
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

Correct Answer: D
Section:
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)

QUESTION 207
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

Correct Answer: B
Section:
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.

QUESTION 208
The lack of a formal process to grant network permissions to different profiles of employees and contractors is leading to an increasing number of security incidents Non-uniform and overly permissive network accesses are being granted. Which of the following would be the MOST appropriate method to improve the security of the environment?

A. Change the default permissions to implicit deny
B. Configure uniform ACLs to employees and NAC for contractors.
C. Deploy an RDP server to centralize the access to the network
D. Implement role-based access control

Correct Answer: D
Section:
Explanation:
The most appropriate method to improve the security of the environment would be to implement role-based access control (RBAC). With RBAC, users are granted access to the network based on their role within the organization. This allows for more granular access control, as different roles may require different levels of access. Additionally, this ensures that users only have access to the resources they need and no more. This helps to reduce the risk of unauthorized access or misuse of the network. Reference and further information can be found in the CompTIA Network+ Study Manual, Chapter 8, Access Control.
RBAC is a method of restricting network access based on the roles of individual users within the organization. With RBAC, users are granted access only to the resources they need to perform their specific job functions. This approach reduces the risk of unauthorized access, provides greater visibility into user activity, and simplifies network management. Changing the default permissions to implicit deny may improve security, but it could also cause issues for legitimate users who require access to specific resources. Configuring uniform ACLs and NAC for contractors is a step in the right direction, but it may not be enough to address the overall lack of a formal process for granting network permissions. Deploying an RDP server to centralize access to the network is not a viable solution, as it would not address the root cause of the security incidents.
Therefore, the most appropriate option is to implement role-based access control. Reference:
CompTIA Network+ Study Guide, Fourth Edition, Chapter 7, section 7.4.

QUESTION 209
An ISP is providing Internet to a retail store and has terminated its point of connection using a standard Cat 6 pin-out Which of me following terminations should the technician use when running a cable from the ISP's port lo the front desk?

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

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

QUESTION 210
Which of the following BEST describes a spirt-tunnel client-to-server VPN connection?

A. The client sends an network traffic down the VPN tunnel
B. The client has two different IP addresses that can be connected to a remote site from two different ISPs to ensure availability
C. The client sends some network traffic down the VPN tunnel and other traffic to the local gateway.
D. The client connects to multiple remote sites at the same time

Correct Answer: C
Section:
Explanation:
In a split-tunnel VPN, the client can access both the local network and the remote network simultaneously, with some network traffic sent through the VPN tunnel and other traffic sent to the local gateway. This approach allows for more efficient use of bandwidth and reduces the load on the VPN server. It also allows the client to continue accessing local resources while connected to the remote network.

QUESTION 211
A network administrator is investigating a performance issue on a dual-link connection—VPN and MPLS—to a partner network. The MPLS is the primary path, and the VPN is used as a backup. While communicating, the delay is measured at 18ms, which is higher than the 6ms expected when the MPLS link is operational but lower than the 30ms expected tor the VPN connection. Which of the following will MOST likely point to the root cause of the Issue?

A. Checking the routing tables on both sides to ensure there is no asymmetric routing
B. Checking on the partner network for a missing route pointing to the VPN connection
C. Running iPerf on both sides to confirm the delay that Is measured is accurate
D. Checking for an incorrect VLAN assignment affecting the MPLS traffic

Correct Answer: A
Section:
Explanation:
Asymmetric routing can occur when two routers have different paths for the same two hosts, resulting in increased latency and possible packet loss. According to the CompTIA Network+ Study Manual, "If the path from the source to the destination is not the same in both directions, the packets will take different routes and the latency can increase significantly." To confirm this, the network administrator should check the routing tables on both sides of the connection and ensure that the same path is used in both directions.

QUESTION 212
A company has multiple offices around the world. The computer rooms in some office locations are too warm Dedicated sensors are in each room, but the process of checking each sensor takes a long time. Which of the following options can the company put In place to automate temperature readings with internal resources?

A. Implement NetFlow.
B. Hire a programmer to write a script to perform the checks

C. Utilize ping to measure the response.
D. Use SNMP with an existing collector server

Correct Answer: D
Section:
Explanation:
SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate with a management server. By using SNMP, the company can set up an SNMP agent on each sensor, which will report its temperature readings to an existing collector server. This will enable the company to monitor the temperatures of all their sensors in real-time without the need for manual checks. Additionally, SNMP's scalability means that even if the company adds more rooms or sensors, the existing system can be easily expanded to accommodate them.

QUESTION 213
Which of the following is a security flaw in an application or network?

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

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

QUESTION 214
Which of the following architectures is used for FTP?

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

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

QUESTION 215
A network technician is hired to review all the devices within a network and make recommendations to improve network efficiency. Which of the following should the technician do FIRST before reviewing and making any recommendations?

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

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

QUESTION 216
A network administrator is configuring logging on an edge switch. The requirements are to log each time a switch port goes up or down. Which of the following logging levels will provide this information?

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

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

QUESTION 217
A technician is investigating an issue with connectivity at customer's location. The technician confirms that users can access resources locally but not over the internet The technician theorizes that the local router has failed and investigates further. The technician's testing results show that the route is functional: however, users still are unable to reach resources on the internal. Which of the following describes what the technician should do NEXT?

A. Document the lessons learned
B. Escalate the issue
C. identify the symptoms.
D. Question users for additional information

Correct Answer: C
Section:
Explanation:
According to the CompTIA Network+ troubleshooting model123, this is the first step in troubleshooting a network problem. The technician should gather information about the current state of the network, such as error messages, device status, network topology, and user feedback. This can help narrow down the scope of the problem and eliminate possible causes.

QUESTION 218
A network technician 13 troubleshooting a network issue for employees who have reported Issues with speed when accessing a server in another subnet. The server is in another building that is 410ft (125m) away from the employees' building. The 10GBASE-T connection between the two buildings uses Cat 5e. Which of the following BEST explains the speed issue?

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

Correct Answer: D
Section:

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

QUESTION 219
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

Correct Answer: B
Section:
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.

QUESTION 220
Which of the following is an advanced distance vector routing protocol that automates routing tables and also uses some features of link-state routing protocols?

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

Correct Answer: C
Section:
Explanation:

QUESTION 221
A network resource was accessed by an outsider as a result of a successful phishing campaign. Which of the following strategies should be employed to mitigate the effects of phishing?

A. Multifactor authentication
B. Single sign-on
C. RADIUS
D. VPN

Correct Answer: A
Section:
Explanation:
Multifactor authentication is a security measure that requires users to provide multiple pieces of evidence before they can access a network resource. This could include requiring users to enter a username, password, and a code sent to the user's mobile phone before they are allowed access. This ensures that the user is who they say they are, reducing the risk of malicious actors gaining access to network resources as a result of a successful phishing campaign.

QUESTION 222
Which of the following devices would be used to extend the range of a wireless network?

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

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

QUESTION 223
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

Correct Answer: A
Section:
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."

QUESTION 224
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

Correct Answer: B
Section:
Explanation:
TACACS+ is used to authenticate users and authorize access to network resources. This protocol provides greater network security by encrypting the authentication credentials and reducing the risk of unauthorized access. According to the CompTIA Network+ Study Manual, “TACACS+ is an authentication protocol used to centralize authentication and authorization for network devices. It is a more secure alternative to Telnet for handling logins and for granting privileges to users.”

QUESTION 225
Which of the following OSI model layers would allow a user to access and download files from a remote computer?

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

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

QUESTION 226
All packets arriving at an interface need to be fully analyzed. Which of me following features should be used to enable monitoring of the packets?

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

Correct Answer: D
Section:
Explanation:

QUESTION 227
A PC user who is on a local network reports very slow speeds when accessing files on the network server The user's PC Is connecting, but file downloads are very slow when compared to other users' download speeds The PC's NIC should be capable of Gigabit Ethernet. Which of the following will MOST likely fix the issue?

A. Releasing and renewing the PC's IP address
B. Replacing the patch cable
C. Reseating the NIC inside the PC
D. Flushing the DNS cache

Correct Answer: B
Section:
Explanation:
A slow download speed can be caused by a faulty patch cable, which is the cable used to connect the user's PC to the network server. If the patch cable is damaged, the connection will be slower than expected, resulting in slow download speeds. Replacing the patch cable is the most likely solution to this issue, as it will provide a new, reliable connection that should allow for faster download speeds.

QUESTION 228
An administrator would like to have two servers at different geographical locations provide fault tolerance and high performance while appearing as one URL to users. Which of the following should the administrator implement?

A. Load balancing

B. Multipathing
C. NIC teaming
D. Warm site

Correct Answer: B
Section:
Explanation:

QUESTION 229
AGRE tunnel has been configured between two remote sites. Which of the following features, when configured, ensures me GRE overhead does not affect payload?

A. jumbo frames
B. Auto medium-dependent Interface
C. Interface crossover
D. Collision detection

Correct Answer: A
Section:
Explanation:
One of the features that can be configured to ensure that GRE overhead does not affect payload is A. jumbo frames. Jumbo frames are Ethernet frames that have a payload size larger than 1500 bytes, which is the standard maximum transmission unit (MTU) for Ethernet. By using jumbo frames, more data can be sent in each packet, reducing the overhead ratio and improving efficiency. Auto medium-dependent interface (MDI), interface crossover, and collision detection are features related to Ethernet physical layer connectivity, but they do not affect GRE overhead or payload.

QUESTION 230
A network administrator views a network pcap and sees a packet containing the following:

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.

Correct Answer: C, D
Section:
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.
Reference: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.5:
Given a scenario, use remote access methods.

QUESTION 231
On a network with redundant switches, a network administrator replaced one of the switches but was unable to get a connection with another switch. Which of the following should the administrator chock after successfully

testing the cable that was wired for TIA/EIA-568A on both ends?

A. If MDIX is enabled on the new switch
B. If PoE is enabled
C. If a plenum cable is being used
D. If STP is disabled on the switches

Correct Answer: A
Section:
Explanation:
Auto-MDIX (or medium dependent interface crossover) is a feature that automatically detects the type of cable connection and configures the interface accordingly (i.e. straight-through or crossover). This ensures that the connection between the two switches is successful. This is referenced in the CompTIA Network+ Study Manual, page 519.

QUESTION 232
A coffee shop owner hired a network consultant to provide recommendations for installing a new wireless network. The coffee shop customers expect high speeds even when the network is congested. Which of the following standards should the consultant recommend?

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

Correct Answer: B
Section:
Explanation:
802.11ax is the latest and most advanced wireless standard, providing higher speeds, lower latency, and more capacity than previous standards. It also supports OFDMA, which allows multiple devices to share a channel and reduce congestion. The other options are older standards that have lower bandwidth, range, and efficiency than 802.11ax. Therefore, 802.11ax is the best option for the coffee shop owner who wants to provide high speeds even when the network is congested.

QUESTION 233
An IT technician successfully connects to the corporate wireless network at a hank. While performing some tests, the technician observes that the physical address of the DHCp server has changed even though the network connection has not been lost. Which of the following would BEST explain this change?

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

Correct Answer: D
Section:
Explanation:
A rogue server is a DHCP server on a network that is not under the administrative control of the network staff1. It may provide incorrect IP addresses or other network configuration information to devices on the network, causing them to lose connectivity or be vulnerable to attacks2. The physical address of the DHCP server may change if a rogue server takes over the role of assigning IP addresses to devices on the network. This can be detected by monitoring DHCP traffic or using tools such as RogueChecker2.

QUESTION 234
A network technician needs to ensure the company's external mail server can pass reverse lookup checks. Which of the following records would the technician MOST likely configure? (Choose Correct option and give explanation directly from CompTIA Network+ Study guide or documents)

A. PTR
B. AAAA
C. SPF
D.

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

QUESTION 235
A company wants to invest in new hardware for the core network infrastructure. The management team requires that the infrastructure be capable of being repaired in less than 60 minutes if any major part fails. Which of the following metrics is MOST likely associated with this requirement?

A. RPO
B. MTTR
C. FHRP
D. MTBF

Correct Answer: B
Section:
Explanation:
MTTR is directly related to how quickly a system can be repaired if any major part fails3. The management team requires that the infrastructure be capable of being repaired in less than 60 minutes, which means they have a low MTTR requirement.
MTTR stands for Mean Time To Repair and is a metric used to measure the average amount of time it takes to repair a failed component or system. In this case, the requirement is for the infrastructure to be capable of being repaired in less than 60 minutes if any major part fails, which means the MTTR should be less than 60 minutes.

QUESTION 236
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

Correct Answer: D
Section:
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.

QUESTION 237
A large number of PCs are obtaining an APIPA IP address, and a number of new computers were added to the network. Which of the following is MOST likely causing the PCs to obtain an APIPA address?

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

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

QUESTION 238
An organization would like to implement a disaster recovery strategy that does not require a facility agreement or idle hardware. Which of the following strategies MOST likely meets the organization's requirements?

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

Correct Answer: A
Section:
Explanation:
A cloud site is a type of disaster recovery site that uses cloud computing services to provide backup and recovery of data and applications in the event of a disaster1. A cloud site does not require a facility agreement or idle hardware, as the cloud provider manages the infrastructure and resources on demand. A cloud site can also offer scalability, flexibility, and cost-effectiveness compared to other types of disaster recovery sites.

QUESTION 239
A network engineer is investigating reports of poor performance on a videoconferencing application. Upon reviewing the report, the engineer finds that available bandwidth at the WAN connection is low.
Which Of the following is the MOST appropriate mechanism to handle this issue?

A. Traffic shaping
B. Flow control
C. NetFlow
D. Link aggregation

Correct Answer: A
Section:
Explanation:

Traffic shaping is a congestion management method that regulates network data transfer by delaying the flow of less important or less desired packets1. Traffic shaping can help to improve the performance of a videoconferencing application by prioritizing its packets over other types of traffic and smoothing out traffic bursts. Traffic shaping can also help to avoid packet loss and ensure fair allocation of bandwidth among different applications or users. Flow control is a mechanism that prevents a sender from overwhelming a receiver with more data than it can handle. Flow control can help to avoid buffer overflow and data loss, but it does not prioritize different types of traffic or smooth out traffic bursts. Flow control operates at the data link layer or the transport layer, while traffic shaping operates at the network layer or above. NetFlow is a protocol that collects and analyzes network traffic data for monitoring and troubleshooting purposes2. NetFlow can help to identify the sources, destinations, volumes, and types of traffic on a network, but it does not regulate or shape the traffic flow. NetFlow operates at the network layer or above.
Link aggregation is a technique that combines multiple physical links into one logical link for increased bandwidth, redundancy, and load balancing. Link aggregation can help to improve the performance of a videoconferencing application by providing more available bandwidth at the WAN connection, but it does not prioritize different types of traffic or smooth out traffic bursts. Link aggregation operates at the data link layer.

QUESTION 240
A network team is getting reports that air conditioning is out in an IDF. The team would like to determine whether additional network issues are occurring. Which of the following should the network team do?

A. Confirm that memory usage on the network devices in the IDF is normal.
B. Access network baseline data for references to an air conditioning issue.
C. Verify severity levels on the corporate syslog server.
D. Check for SNMP traps from a network device in the IDF.
E. Review interface statistics looking for cyclic redundancy errors.

Correct Answer: D
Section:
Explanation:
"Baselines play an integral part in network documentation because they let you monitor the network's overall performance. In simple terms, a baseline is a measure of performance that indicates how hard the network is working and where network resources are spent. The purpose of a baseline is to provide a basis of comparison. For example, you can compare the network's performance results taken in March to results taken in June, or from one year to the next. More commonly, you would compare the baseline information at a time when the network is having a problem to information recorded when the network was operating with greater efficiency. Such comparisons help you determine whether there has been a problem with the network, how significant that problem is, and even where the problem lies."

QUESTION 241
Which of the following is the NEXT step to perform network troubleshooting after identifying an issue?

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

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

QUESTION 242
Which of the following layers of the OSI model has new protocols activated when a user moves from a wireless to a wired connection?

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

Correct Answer: A
Section:
Explanation:
"The Data Link layer also determines how data is placed on the wire by using an access method. The wired access method, carrier-sense multiple access with collision detection (CSMA/CD), was once used by all wired Ethernet networks, but is automatically disabled on switched full-duplex links, which have been the norm for decades. Carrier-sense multiple access with collision avoidance (CSMA/CA) is used by wireless networks, in a similar fashion."

QUESTION 243
A network administrator is preparing answers for an annual risk assessment that is required for compliance purposes. Which of the following would be an example of an internal threat?

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

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

QUESTION 244
A company's primary ISP is experiencing an outage. However, the network administrator notices traffic continuing to flow through a secondary connection to the same ISP. Which of the following BEST describes this configuration?

A. Diverse paths
B. Load balancing
C. Multipathing
D. Virtual Router Redundancy Protocol

Correct Answer: A
Section:

QUESTION 245
Network users reported that a recent firmware upgrade to a firewall did not resolve the issue that prompted the upgrade. Which of the following should be performed NEXT?

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

Correct Answer: B
Section:

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

QUESTION 246
A technician manages a DHCP scope but needs to allocate a portion of the scope's subnet for statically assigned devices. Which of the following DHCP concepts would be BEST to use to prevent IP address conflicts?

A. Dynamic assignment
B. Exclusion range
C. Address reservation
D. IP helper

Correct Answer: B
Section:
Explanation:
To prevent IP address conflicts when allocating a portion of a DHCP scope's subnet for statically assigned devices, it is recommended to use the concept of DHCP exclusion ranges. DHCP exclusion ranges allow a DHCP administrator to specify a range of IP addresses within the scope that should not be assigned to DHCP clients. This can be useful in situations where some devices on the network need to be assigned static IP addresses, as it ensures that the statically assigned addresses do not overlap with addresses assigned by the DHCP server. To set up a DHCP exclusion range, the administrator needs to specify the start and end IP addresses of the range, as well as the subnet mask. The DHCP server will then exclude the specified range of addresses from its pool of available addresses, and will not assign them to DHCP clients. By using DHCP exclusion ranges, the technician can ensure that the statically assigned addresses do not conflict with addresses assigned by the DHCP server, and can prevent IP address conflicts on the network.
Anthony Sequeira
"Another frequent configuration you might make in a DHCP implementation is to configure an exclusion range. This is a portion of the address pool that you never want leased out to clients in the network. Perhaps you have numbered your servers 192.168.1.1–192.168.1.10. Because the servers are statically configured with these addresses, you exclude these addresses from the 192.168.1.0/24 pool of addresses."
Mike Meyers
"Exclusion ranges represent an IP address or range of IP addresses from the pool of addresses that are not to be given out by the DHCP server. Exclusions should be made for the static addresses manually configured on servers and router interfaces, so these IP addresses won't be offered to DHCP clients."

QUESTION 247
Which of the following protocols can be routed?

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

Correct Answer: C
Section:
Explanation:
iSCSI (Internet Small Computer System Interface) is a protocol that allows SCSI commands to be transported over IP networks1. iSCSI can be routed because it contains a network address and a device address, as required by a routable protocol2. iSCSI can be used to access block-level storage devices over a network, such as SAN (Storage Area Network).
FCoE (Fibre Channel over Ethernet) is a protocol that allows Fibre Channel frames to be encapsulated and transported over Ethernet networks1. FCoE cannot be routed because it does not contain a network address, only a

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

QUESTION 248
A technician thinks one of the router ports is flapping. Which of the following available resources should the technician use in order to determine if the router is flapping?

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

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

QUESTION 249
Which of the following technologies would MOST likely De used to prevent the loss of connection between a virtual server and network storage devices?

A. Multipathing
B. VRRP
C. Port aggregation
D. NIC teaming

Correct Answer: D
Section:
Explanation:
NIC teaming is a technology that allows multiple network interface cards (NICs) to work together as a single logical interface, providing redundancy and load balancing. This can prevent the loss of connection between a virtual server and network storage devices if one of the NICs fails or becomes disconnected. Reference: [CompTIA Network+ Certification Exam Objectives], Domain 2.0 Networking Concepts, Objective 2.5: Explain the purposes and use cases for advanced networking devices, Subobjective: NIC bonding/teaming

QUESTION 250
A network technician receives a support ticket concerning multiple users who are unable access the company's shared drive. The switch interface that the shared drive Is connected to is displaying die following:

```
GigabitEthernet0/9 is down, line protocol is down (notconnect)
        Hardware is Gigabit Ethernet, address is C800.84bf.9847 (via c800.84bf.9847)
        MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
        reliability 255/255. txload 1/255. rxload 1/255
        Encapsulation ARPA, loopback not set
```

Which of the following is MOST likely the Issue?

A. The switchport Is shut down
B. The cable Is not plugged In.
C. The loopoack Is not set
D. The bandwidth configuration is incorrect.

Correct Answer: A
Section:
Explanation:
The switchport is shut down, which means it is administratively disabled and cannot forward traffic.
The image shows that the switchport status is "down" and the protocol status is "down", indicating that there is no physical or logical connection. The cable is plugged in, as shown by the "connected" message under the interface name. The loopback is not set, as shown by the "loopback not set" message under the encapsulation type. The bandwidth configuration is correct, as shown by the "BW 10000 Kbit/sec" message under the MTU size.
Reference: [CompTIA Network+ Certification Exam
Objectives], Domain 3.0 Infrastructure, Objective 3.1: Given a scenario, use appropriate networking tools, Subobjective: Command line tools (ping, netstat, tracert, etc.)

QUESTION 251
Which of the following is the physical security mechanism that would MOST likely be used to enter a secure site?

A. A landing page
B. An access control vestibule
C. A smart locker
D. A firewall

Correct Answer: B
Section:
Explanation:
An access control vestibule is a physical security mechanism that consists of a small room or chamber with two doors, one leading to the outside and one leading to the secure site. The doors are controlled by an electronic system that verifies the identity and authorization of the person entering before allowing access to the next door. A landing page is a web page that appears when a user clicks on a link or advertisement. A smart locker is a physical security mechanism that allows users to store and retrieve items using a code or biometric authentication. A firewall is a network security device that monitors and filters incoming and outgoing traffic based on predefined rules. Reference:
[CompTIA Network+ Certification Exam Objectives], Domain 4.0 Network Operations, Objective 4.1:
Explain the importance of documentation and diagrams, Subobjective: Physical security devices (locks, cameras, etc.)

QUESTION 252
A network technician is troubleshooting a connection to a web server. The Technician Is unable to ping the server but is able to verify connectivity to the web service using Tenet. Which of the following protocols is being blocked by me firewall?

A. UDP
B. ARP

C. ICMP
D. TCP

Correct Answer: C
Section:
Explanation:
ICMP (Internet Control Message Protocol) is a protocol that is used to send error and control messages between network devices, such as ping requests and replies. ICMP is being blocked by the firewall, which prevents the network technician from pinging the web server. TCP (Transmission Control Protocol) is a protocol that provides reliable and ordered delivery of data between network devices, such as web service requests and responses using HTTP (Hypertext Transfer Protocol). TCP is not being blocked by the firewall, which allows the network technician to verify connectivity to the web service using Telnet. UDP (User Datagram Protocol) is a protocol that provides fast and efficient delivery of data between network devices, but does not guarantee reliability or order. UDP is used for applications such as streaming media or online gaming. ARP (Address Resolution Protocol) is a protocol that resolves IP addresses to MAC addresses on a local network. Reference: [CompTIA Network+ Certification Exam Objectives], Domain 2.0 Networking Concepts, Objective 2.1: Compare and contrast OSI and TCP/IP models, Subobjective: TCP/IP model layers (Application/Transport/Internet/Network Interface)

QUESTION 253
Which or the following devices and encapsulations are found at me data link layer? (Select TWO)

A. Session
B. Frame
C. Firewall
D. Switch
E. Packet
F. Router

Correct Answer: B, D
Section:
Explanation:
The data link layer is responsible for defining the format of data on the network and providing physical transmission of data. Devices that operate at this layer include switches and network interface cards (NICs). Encapsulations that are used at this layer include frames, which are units of data that contain a header, payload, and trailer. Frames are used to identify the source and destination of data on the network and to perform error detection. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 9; The Official CompTIA Network+ Student Guide (Exam N10-008), page 1-6.

QUESTION 254
Which of the following redundant devices creates broadcast storms when connected together on a high-availability network?

A. Switches
B. Routers
C. Access points
D. Servers

Correct Answer: A
Section:
Explanation:
Switches are devices that forward data based on MAC addresses. They create separate collision domains for each port, which reduces the chance of collisions on the network. However, if multiple switches are connected together without proper configuration, they can create broadcast storms, which are situations where broadcast frames are endlessly forwarded between switches, consuming network bandwidth and resources. Broadcast storms can be prevented by using protocols such as Spanning Tree Protocol (STP), which eliminates loops in the network topology. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 67; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-14.

QUESTION 255
A business purchased redundant internet connectivity from two separate ISPs. Which of the following is the business MOST likely implementing?

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

Correct Answer: C
Section:
Explanation:
Multipathing is a technique that allows a device to use more than one path to communicate with another device. This provides redundancy, load balancing, and fault tolerance for network connections. A business that purchased redundant internet connectivity from two separate ISPs is most likely implementing multipathing to ensure continuous access to the internet in case one ISP fails or becomes congested. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 437; The Official CompTIA Network+ Student Guide (Exam N10-008), page 16-8.

QUESTION 256
A network administrator is troubleshooting a PC that cannot connect to the LAN. The administrator runs the ipconfig command at the command prompt and gets the following output:

```
Ethernet Adapter:
Physical Address      AB-CD-EF-12-34-56
DHCP Enabled          No
IPV4 Address          192.168.1.55
Subnet Mask           225.225.225.224
Default Gateway       192.168.1.1
DHCP Server           192.168.1.1
DNS Server            192.168.1.1
```

Which of the following is misconfigured?

A. Subnet mask
B. Physical address
C. DNS server
D. DHCP server

Correct Answer: A
Section:
Explanation:
The subnet mask is a binary value that defines how many bits of an IP address are used to identify the network and how many bits are used to identify the host. The subnet mask also determines the size and number of subnets in a network. The ipconfig command shows the current IP configuration of a device, including the subnet mask. In this case, the subnet mask is misconfigured because it does not match the network address of the device. The device has an IP address of 192.168.1.55, which belongs to the network 192.168.1.0/24 (with a subnet mask of 255.255.255.0). However, the subnet mask is set to 225.225.225.224, which is an invalid value that does not correspond to any network prefix length. This causes the device to be unable to communicate with other devices on the same network or access the default gateway. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 109; The Official CompTIA Network+ Student Guide (Exam N10-008), page 5-4.

QUESTION 257
A customer runs a DNS lookup service and needs a network technician to reconfigure the network to improve performance. The customer wants to ensure that servers are accessed based on whichever one is topographically closest to the destination. If the server does not respond, then the next topographically closest server should respond Which of the following does the technician need to configure to meet the requirements?

A. Multicast addressing
B. Anycast addressing
C. Broadcast addressing
D. Unicast addressing

Correct Answer: B
Section:
Explanation:
Anycast addressing is a network addressing and routing methodology in which a single destination address has multiple routing paths to two or more endpoint destinations. Routers will select the desired path on the basis of number of hops, distance, lowest cost, latency measurements or based on the least congested route. Anycast addressing is designed to provide high availability and low latency for services that have multiple instances across the world, such as DNS servers. By using anycast addressing, the customer can ensure that servers are accessed based on whichever one is topographically closest to the destination. If the server does not respond, then the next topographically closest server should respond. Reference: [CompTIA Network+ Certification Exam Objectives], [Anycast - Wikipedia]

QUESTION 258
A help desk supervisor reviews the following excerpt of a call transcript:

```
Agent: Thanks for calling the help desk. What can I help you with today?
Customer: I have been trying to connect to www.awesome-website.com all morning, but I can't get to it.
Agent: Let me see if I can reach it from my end. Give me a moment, please.
Customer: Sure. Thanks for helping.
Agent: It's my pleasure. And indeed, it seems like I can't reach that website either.
Customer: I guess that means that it isn't just me, then.
```

Which of the following was the agent trying to accomplish with this exchange?

A. The agent was questioning the obvious.
B. The agent was verifying full system functionality
C. The agent was identifying potential effects.
D. The agent was trying to duplicate the problem.

Correct Answer: D
Section:
Explanation:
The agent was trying to duplicate the problem by asking the user to perform the same steps that led to the issue. This is a common troubleshooting technique that helps the agent to identify the root cause of the problem and verify if it is reproducible or intermittent. By duplicating the problem, the agent can also gather more information about the symptoms and error messages that the user encountered. Reference: [CompTIA Network+ Certification Exam Objectives], [Troubleshooting Methodology - CompTIA Network+ N10-007 - 1.4 | Professor Messer IT Certification Training Courses]

QUESTION 259
An infrastructure company is implementing a cabling solution to connect sites on multiple continents. Which of the following cable types should the company use for this project?

A. Cat 7
B. Single-mode
C. Multimode
D. Cat 6

Correct Answer: B
Section:
Explanation:
Single-mode fiber is a type of optical fiber that has a small core diameter and allows only one mode of light to propagate. This reduces signal attenuation and increases transmission distance, making it suitable for long-distance communication networks. Single-mode fiber can carry data over thousands of kilometers without requiring repeaters or amplifiers. Single-mode fiber is also immune to electromagnetic interference and has a higher bandwidth than multimode fiber. Therefore, single-mode fiber is the best cable type for connecting sites on multiple continents. Reference: [CompTIA Network+ Certification Exam Objectives], [Single-mode optical fiber - Wikipedia]
Single-mode fiber optic cable uses a single ray of light to transmit data. This allows it to achieve very low attenuation and high bandwidth.
Multimode fiber optic cable uses multiple rays of light to transmit data. This results in higher attenuation and lower bandwidth than single-mode cable.
Twisted pair copper cable uses two insulated copper wires to transmit data. It is less expensive than fiber optic cable, but it has higher attenuation and lower bandwidth.

When choosing a cable type for a long-distance application, it is important to consider the following factors:
Attenuation: The amount of signal loss that occurs over the length of the cable.
Bandwidth: The amount of data that can be transmitted over the cable per second.
Cost: The cost of the cable and installation.
Single-mode fiber optic cable is the best choice for long-distance applications because it has the lowest attenuation and highest bandwidth of any cable type. However, it is also the most expensive cable type.

QUESTION 260
A network technician wants to find the shortest path from one node to every other node in the network. Which of the following algorithms will provide the FASTEST convergence time?

A. A static algorithm
B. A link-state algorithm
C. A distance-vector algorithm
D. A path-vector algorithm

Correct Answer: B
Section:
Explanation:
A link-state algorithm is a routing algorithm that uses information about the state of each link in the network to calculate the shortest path from one node to every other node. A link-state algorithm requires each router to maintain a complete map of the network topology and exchange link-state advertisements with its neighbors periodically or when a change occurs. A link-state algorithm uses a mathematical formula called Dijkstra's algorithm to find the shortest path based on the link costs. A link-state algorithm provides the fastest convergence time because it can quickly detect and adapt to network changes. Reference: [CompTIA Network+ Certification Exam Objectives], [Link-state routing protocol - Wikipedia]

QUESTION 261
A customer reports there is no access to resources following the replacement of switches. A technician goes to the site to examine the configuration and discovers redundant links between two switches. Which of the following is the reason the network is not functional?

A. The ARP cache has become corrupt.
B. CSMA/CD protocols have failed.
C. STP is not configured.
D. The switches are incompatible models

Correct Answer: C
Section:
Explanation:
The reason the network is not functional is that STP (Spanning Tree Protocol) is not configured on the switches. STP is a protocol that prevents loops in a network topology by blocking redundant links between switches. If STP is not enabled, the switches will forward broadcast frames endlessly, creating a broadcast storm that consumes network resources and disrupts communication. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 67; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-14.

QUESTION 262
Which of the following BEST describes a north-south traffic flow?

A. A public internet user accessing a published web server
B. A database server communicating with another clustered database server
C. A Layer 3 switch advertising routes to a router
D. A management application connecting to managed devices

Correct Answer: A
Section:

Explanation:
A north-south traffic flow is a term used to describe the communication between a user or device outside the network and a server or service inside the network. For example, a public internet user accessing a published web server is a north-south traffic flow. This type of traffic flow typically crosses the network perimeter and requires security measures such as firewalls and VPNs. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 16; The Official CompTIA Network+ Student Guide (Exam N10-008), page 1-9.
North-south traffic flow refers to the flow of traffic between the internal network of an organization and the external world. This type of traffic typically flows from the internet to the organization's internal network, and back again.
Examples of north-south traffic flow include:
A public internet user accessing a published web server
A remote employee connecting to a VPN
An email client sending email to an external server
A customer connecting to an e-commerce website
Reference:
CompTIA Network+ N10-008 Exam Objectives, Version 5.0, August 2022, page 12
CompTIA Network+ Certification Study Guide, Seventh Edition, Todd Lammle, Sybex, 2022, page 17

QUESTION 263
A user is required to log in to a main web application, which then grants the user access to all other programs needed to complete job-related tasks. Which of the following authentication methods does this setup describe?

A. SSO
B. RADIUS
C. TACACS+
D. Multifactor authentication
E. 802.1X

Correct Answer: A
Section:
Explanation:
The authentication method that this setup describes is SSO (Single Sign-On). SSO is a technique that allows a user to log in once to a main web application and then access multiple other applications or services without having to re-enter credentials. SSO simplifies the user experience and reduces the number of passwords to remember and manage. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 371; The Official CompTIA Network+ Student Guide (Exam N10-008), page 14-5.

QUESTION 264
Which of the following is a valid alternative to maintain a deployed proxy technology while saving physical space in the data center by moving the network service to the virtualization infrastructure?

A. NFV
B. SDWAN
C. Networking as code
D. VIP

Correct Answer: A
Section:
Explanation:
The valid alternative to maintain a deployed proxy technology while saving physical space in the data center by moving the network service to the virtualization infrastructure is NFV (Network Function Virtualization). NFV is a technique that allows network functions, such as proxies, firewalls, routers, or load balancers, to be implemented as software applications running on virtual machines or containers. NFV reduces the need for dedicated hardware devices and improves scalability and flexibility of network services. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 440; The Official CompTIA Network+ Student Guide (Exam N10-008), page 16-11.
NFV can be used to virtualize a wide variety of network functions, including proxy servers. By virtualizing proxy servers, organizations can save physical space in the data center and improve the scalability and efficiency of their networks.

To virtualize a proxy server using NFV, an organization would need to deploy a virtualization platform, such as VMware ESXi or Microsoft Hyper-V. The organization would then need to install a virtual proxy server appliance on the virtualization platform.
Once the virtual proxy server appliance is installed, it can be configured and used just like a physical proxy server.
NFV is a relatively new technology, but it is quickly gaining popularity as organizations look for ways to improve the efficiency and scalability of their networks.

QUESTION 265
A SQL server connects over port:

A. 445.
B. 995
C. 1433.
D. 1521.

Correct Answer: C
Section:
Explanation:
A SQL server connects over port 1433. Port numbers are used to identify specific applications or services on a network device. Port 1433 is the default port for Microsoft SQL Server, which is a relational database management system that uses SQL (Structured Query Language) to store and manipulate data. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 147; The Official CompTIA Network+ Student Guide (Exam N10-008), page 6-4.

QUESTION 266
Which of the following is required when connecting an endpoint device with an RJ45 port to a network device with an ST port?

A. A media converter
B. A bridge
C. An MDIX
D. A load balancer

Correct Answer: A
Section:
Explanation:
The device that is required when connecting an endpoint device with an RJ45 port to a network device with an ST port is a media converter. A media converter is a device that converts signals between different types of media, such as copper and fiber. An RJ45 port is used for twisted-pair copper cables, while an ST port is used for fiber-optic cables. A media converter allows these two types of cables to interconnect and communicate. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 54; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-5.

QUESTION 267
After upgrading to a SOHO router that supports Wi-Fi 6, the user determines throughput has not increased. Which of the following is the MOST likely cause of the issue?

A. The wireless router is using an incorrect antenna type.
B. The user's workstation does not support 802.11 ax.
C. The encryption protocol is mismatched
D. The network is experiencing interference.

Correct Answer: B
Section:
Explanation:
The user's workstation does not support 802.11 ax, which is the technical name for Wi-Fi 6. Wi-Fi 6 is a new wireless standard that offers faster speeds, higher capacity, and lower latency than previous standards. However, to take advantage of these benefits, both the router and the workstation need to support Wi-Fi 6. If the workstation only supports an older standard, such as 802.11 ac or Wi-Fi 5, then the throughput will not increase even if

the router supports Wi-Fi 6. Reference: [CompTIA Network+ Certification Exam Objectives], What is Wi-Fi 6? Here's what you need to know | PCWorld

QUESTION 268
A company has a geographically remote office concern for this type of connection?

A. Duplex
B. Collisions
C. Jitter
D. Encapsulation

Correct Answer: C
Section:
Explanation:
Jitter is the variation in the delay of packets arriving at a destination. Jitter can cause problems for real-time applications, such as voice and video, that require consistent and smooth delivery of packets. A geographically remote office that connects to the main office via a WAN link may experience high jitter due to factors such as network congestion, routing changes, or link quality.
Jitter can be reduced by using quality of service (QoS) mechanisms that prioritize and shape traffic according to its importance and sensitivity. Reference: [CompTIA Network+ Certification Exam Objectives], What is Jitter? | Network Jitter Explained | SolarWinds

QUESTION 269
Which of the following demarcation connections would be MOST appropriate to use with a cable modem being installed in a SOHO situation?

A. RG6
B. Cat 6
C. RJ11
D. Multimode fiber

Correct Answer: A
Section:
Explanation:
RG6 is a type of coaxial cable that is commonly used for cable TV and internet services. A cable modem is a device that modulates and demodulates signals over a coaxial cable network to provide broadband internet access. A SOHO situation refers to a small office/home office environment that typically has a single cable modem connected to a single coaxial cable outlet. Therefore, RG6 is the most appropriate demarcation connection for a cable modem in a SOHO situation. Reference:
[CompTIA Network+ Certification Exam Objectives], What Is RG6 Cable? | Techwalla

QUESTION 270
A technician is investigating a SAN switch that has a high number of CRC errors. Which of the following is the MOST likely cause of the errors?

A. Break in the fiber
B. Bad switch port
C. Mismatched duplex
D. Memory errors

Correct Answer: B
Section:
Explanation:
A bad switch port is the most likely cause of CRC errors on a SAN switch. CRC stands for cyclic redundancy check, which is a method of detecting errors in data transmission. A SAN switch is a device that connects storage devices and servers in a storage area network (SAN), which is a high-performance network that provides block-level access to data. A bad switch port can cause CRC errors due to physical damage, faulty wiring, or misconfiguration. CRC errors can result in data corruption or loss, which can affect the performance and availability of the SAN. Reference:

QUESTION 271
An organization recently connected a new computer to the LAN. The user is unable to ping the default gateway. Which of the following is the most likely cause?

A. The DHCP server is not available.
B. An RFC1918 address is being used
C. The VLAN is incorrect.
D. A static IP is assigned.

Correct Answer: A
Section:
Explanation:
The DHCP server is not available is the most likely cause of the issue where a new computer is unable to ping the default gateway. DHCP stands for Dynamic Host Configuration Protocol, which is a network protocol that automatically assigns IP addresses and other configuration parameters to clients on a network. The default gateway is the IP address of the router or device that connects a local network to other networks, such as the internet. Pinging is a network utility that tests the connectivity and reachability between two devices by sending and receiving echo packets. If the DHCP server is not available, the new computer will not be able to obtain an IP address or other configuration parameters, such as the default gateway, from the DHCP server. This will prevent the new computer from communicating with other devices on the network or the internet, resulting in ping failure. Reference: [CompTIA Network+ Certification Exam Objectives], What Is DHCP? | How DHCP Works | SolarWinds MSP

QUESTION 272
A network technician is investigating a trouble ticket for a user who does not have network connectivity. All patch cables between the wall jacks and computers in the building were upgraded over the weekend from Cat 5 to Cat 6. The newly installed cable is crimped With a TIA/EIA 568A on one end and a TIA/EIA 568B on the other end. Which of the following should the technician do to most likely fix the issue?

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

Correct Answer: B
Section:
Explanation:
Crimping the cable as a straight-through cable is the most likely fix for the issue where users are unable to access any network resources after upgrading from Cat 5 to Cat 6 cables. Crimping is a process of attaching connectors to the ends of cables using a tool called a crimper. A straight-through cable is a type of twisted-pair cable that has the same wiring scheme on both ends, meaning that each pin on one end is connected to the same pin on the other end. A straight-through cable is used to connect devices that operate on different layers of the OSI model, such as a computer and a switch, or a switch and a router. If the newly installed cable is crimped with TIA/EIA 568A on one end and TIA/EIA 568B on the other end, it becomes a crossover cable. A crossover cable is a type of twisted-pair cable that has opposite wiring schemes on both ends, meaning that each pin on one end is connected to a different pin on the other end. A crossover cable is used to connect devices that operate on the same layer of the OSI model, such as two computers or two switches. Using a crossover cable instead of a straight-through cable can cause network communication errors or failures. Reference: [CompTIA Network+ Certification Exam Objectives], Straight Through vs Crossover Cable: What's The Difference?

QUESTION 273
A wireless technician is working to upgrade the wireless infrastructure for a company. The company currently uses the 802.11g wireless standard on all access points. The company requires backward compatibility and is requesting the least expensive solution. Which of the following should the technician recommend to the company?

A. 802.11a
B. 802.11ac
C. 802Hax
D. 802.11n

Correct Answer: D

Section:
Explanation:
802.11n is a wireless standard that supports data rates up to 600 Mbps and operates in both 2.4 GHz and 5 GHz frequency bands. 802.11n is backward compatible with 802.11g, which operates only in 2.4 GHz band. 802.11n is the least expensive solution that can upgrade the wireless infrastructure for the company, as it does not require replacing all the access points or wireless devices

QUESTION 274
A network technician is investigating why a core switch is logging excessive amounts of data to the syslog server. The running configuration of the switch showed the following logging information:

```
ip ssh logging events
logging level debugging
logging host 192.168.1.100
logging synchronous
```

Which of the following changes should the technician make to BEST fix the issue?

A. Update the logging host IP
B. Change lo asynchronous logging.
C. Stop logging SSH events.
D. Adjust the logging level.

Correct Answer: D
Section:
Explanation:
The logging level is set to debugging, which is the most verbose and detailed level of logging. This means that the switch will send a lot of information to the syslog server, which can cause excessive network traffic and storage consumption. To fix the issue, the technician should adjust the logging level to a lower value, such as informational or warning, which will reduce the amount of data logged

QUESTION 275
Two companies want to build an encrypted tunnel between them and use a PSK for initial authentication. Which of the following is the BEST protocol for the companies to use?

A. VPN
B. SSL
C. TLS
D. IPSec

Correct Answer: D
Section:
Explanation:
IPSec is a protocol that provides secure communication between two networks or hosts over an untrusted network, such as the Internet. IPSec uses encryption and authentication to protect the data from eavesdropping, tampering, and replay attacks. IPSec also supports pre-shared key (PSK) as one of the methods for initial authentication between the peers

QUESTION 276
Which of the following ports is a secure protocol?

A. 20
B. 23
C. 443
D. 445

Correct Answer: C
Section:

Explanation:
This is the port number for HTTPS, which stands for Hypertext Transfer Protocol Secure. HTTPS is a secure version of HTTP, which is the protocol used to communicate between web browsers and web servers. HTTPS encrypts the data sent and received using SSL/TLS, which are cryptographic protocols that provide authentication, confidentiality, and integrity. HTTPS is commonly used for online transactions, such as banking and shopping, where security and privacy are important

QUESTION 277
Which of the following indicates a computer has reached end-of-support?

A. The computer does not have any users.
B. The antivirus protection is expired.
C. The operating system license is expired.
D. No more patches or bug fixes are available indefinitely.

Correct Answer: D
Section:
Explanation:
No more patches or bug fixes are available indefinitely. This indicates that a computer has reached end-of-support, which means that the manufacturer or vendor of the hardware or software no longer provides technical assistance, updates, or security fixes for the product12. This can expose the computer to potential security risks and compatibility issues with newer technologies

QUESTION 278
A server application requires large amounts of data to be sent at a consistent rate. Which of the following should an engineer most likely configure to meet these requirements?

A. Link speed
B. Jumbo frames
C. Switch Virtual Interface
D. Spanning tree

Correct Answer: B
Section:
Explanation:
Jumbo frames are Ethernet frames that have a payload size greater than the standard 1500 bytes.
Jumbo frames can carry more data in each frame, which reduces the overhead and improves the throughput and efficiency of data transmission. Jumbo frames are commonly used in storage area networks (SANs), where large amounts of data need to be transferred between servers and storage devices

QUESTION 279
Which of the following is a document that states what the minimum performance expectations are within a network?

A. Memorandum of understanding
B. Service-level agreement
C. Non-disclosure agreement
D. Baseline metrics

Correct Answer: B
Section:
Explanation:
A service-level agreement (SLA) is a document that states what the minimum performance expectations are within a network, such as uptime, throughput, latency, and security. An SLA is usually signed between a service provider and a customer, and it specifies the penalties or remedies if the service level is not met

QUESTION 280
To reduce costs and increase mobility, a Chief Technology Officer (CTO) wants to adopt cloud services for the organization and its affiliates. To reduce the impact for users, the CTO wants key services to run from the on-site data center and enterprise services to run in the cloud. Which of the following deployment models is the best choice for the organization?

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

Correct Answer: B
Section:
Explanation:
A hybrid cloud deployment model is a combination of on-premise and cloud solutions, where some resources are hosted in-house and some are hosted by a cloud provider. A hybrid cloud model can offer the benefits of both public and private clouds, such as scalability, cost-efficiency, security, and control12. A hybrid cloud model can also reduce the impact for users, as they can access the key services from the on-site data center and the enterprise services from the cloud

QUESTION 281
A user reports having intermittent connectivity issues to the company network. The network configuration for the user reveals the following:
IP address: 192.168.1.10
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.254
The network switch shows the following ARP table:

MAC address	IP address	Interface	VLAN
0c00.1134.0001	192.168.1.10	eth4	10
0c00.1983.210a	192.168.2.13	eth5	11
0c00.1298.d239	192.168.1.10	eth6	10
0c00.a291.c113	192.168.2.12	eth7	11
0c00.923b.2391	192.168.1.11	eth8	10
feff.2391.1022	192.168.1.254	eth1	10

Which of the following is the most likely cause of the user's connection issues?

A. A port with incorrect VLAN assigned
B. A switch with spanning tree conflict
C. Another PC with manually configured IP
D. A router with overlapping route tables

Correct Answer: C
Section:
Explanation:
This is the most likely cause of the user's connection issues, because the ARP table of the switch shows that there are two devices with the same IP address of 192.168.1.10, but different MAC addresses. This indicates that there is an IP address conflict on the network, where two devices are trying to use the same IP address. This can cause intermittent connectivity issues, as the switch may not be able to forward packets to the correct destination .

QUESTION 282
A sales team at a company uses a SaaS solution primarily for videoconferencing and a CRM application that connects to a database server in the corporate data center. Which of the following VPN solutions would allow

secure, remote access for sales staff to the CRM application without impacting videoconferencing traffic?

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

Correct Answer: A
Section:
Explanation:

QUESTION 283
A network administrator is configuring a firewall to allow for a new cloud-based email server. The company standard is to use SMTP to route email traffic. Which of the following ports, by default, should be reserved for this purpose?

A. 23
B. 25
C. 53
D. 110

Correct Answer: B
Section:
Explanation:
Port 25, by default, should be reserved for SMTP traffic to allow for a new cloud-based email server.
SMTP stands for Simple Mail Transfer Protocol, which is a network protocol that enables email communication between mail servers and clients. SMTP uses port 25 as its default port for sending and receiving email messages over TCP/IP networks. A cloud-based email server is an email server that is hosted on a cloud service provider's infrastructure, rather than on-premise or in-house. A cloud-based email server can offer advantages such as scalability, reliability, security, and cost-effectiveness. To allow for a new cloud-based email server, a firewall should be configured to open port 25 for SMTP traffic. Reference: [CompTIA Network+ Certification Exam Objectives], What Is SMTP? | Mailtrap Blog, Cloud Email Server: What Is It & How Does It Work? | Zoho Mail

QUESTION 284
A network administrator is concerned about a rainbow table being used to help access network resources. Which of the following must be addressed to reduce the likelihood of a rainbow table being effective?

A. Password policy
B. Remote access policy
C. Acceptable use policy
D. Data loss prevention policy

Correct Answer: A
Section:
Explanation:
A password policy must be addressed to reduce the likelihood of a rainbow table being effective. A rainbow table is a precomputed table of hashed passwords and their corresponding plaintext values.
A rainbow table can be used to crack hashed passwords by performing a reverse lookup of the hash value in the table. A password policy is a set of rules and guidelines that define how passwords should be created, used, and managed in an organization. A password policy can help prevent rainbow table attacks by enforcing strong password requirements, such as length, complexity, expiration, and history. A strong password is one that is hard to guess or crack by using common methods such as brute force or dictionary attacks. Reference: [CompTIA Network+ Certification Exam Objectives], What Is Rainbow Table Attack? | Kaspersky, Password Policy Best Practices | Thycotic

QUESTION 285

Which of the following would MOST likely be used to review disaster recovery information for a system?

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

Correct Answer: A
Section:
Explanation:
The document that would most likely be used to review disaster recovery information for a system is a business continuity plan (BCP). A BCP is a document that outlines the procedures and resources needed to maintain or resume critical business functions in the event of a disaster or disruption. A BCP typically includes a disaster recovery plan (DRP), which is a subset of the BCP that focuses on restoring IT systems and data after a disaster. A BCP also covers other aspects of business continuity, such as risk assessment, business impact analysis, emergency response, crisis management, and testing. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 346; The Official CompTIA Network+ Student Guide (Exam N10-008), page 13-9.

QUESTION 286
Which of the following policies outlines the software and hardware requirements for using personally owned devices to conduct business?

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

Correct Answer: C
Section:
Explanation:
The policy that outlines the software and hardware requirements for using personally owned devices to conduct business is BYOD (Bring Your Own Device). BYOD is a practice that allows employees to use their own devices, such as laptops, tablets, or smartphones, to access corporate resources and applications. BYOD can offer benefits such as increased productivity, flexibility, and satisfaction for employees, as well as reduced costs for employers. However, BYOD also poses challenges and risks, such as security, compatibility, and support issues. Therefore, a BYOD policy is needed to define the rules and expectations for using personal devices in a business environment. A BYOD policy typically covers topics such as device eligibility, security requirements, acceptable use, data ownership, privacy, and liability. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 362; The Official CompTIA Network+ Student Guide (Exam N10-008), page 14-2.

QUESTION 287
A network architect needs to create a wireless field network to provide reliable service to public safety vehicles. Which of the following types of networks is the best solution?

A. Mesh
B. Ad hoc
C. Point-to-point
D. Infrastructure

Correct Answer: A
Section:
Explanation:
A mesh network is the best solution for creating a wireless field network to provide reliable service to public safety vehicles. A mesh network is a type of wireless network that consists of multiple nodes that communicate with each other directly or through intermediate nodes, forming a web-like topology. A mesh network does not rely on a central access point or router, but rather on the cooperation and coordination of the nodes themselves. A mesh network has several advantages for public safety applications, such as12:
High availability and resilience: A mesh network can automatically route around failures or congestion, ensuring that the network remains operational even if some nodes are damaged or disconnected. A mesh network can also self-heal and self-configure, adapting to changes in the network topology or environment.

Extended coverage and scalability: A mesh network can extend the wireless signal beyond the range of a single node, by using other nodes as relays or repeaters. A mesh network can also accommodate more nodes and devices, by adding more links and paths between them.
Low cost and easy deployment: A mesh network can reduce the cost and complexity of installing and maintaining a wireless infrastructure, by eliminating the need for expensive cabling, towers, or antennas. A mesh network can also be deployed quickly and flexibly, by simply adding or removing nodes as needed.
A mesh network is especially suitable for public safety vehicles, because it can provide reliable wireless communication in challenging scenarios, such as12:
Disaster response: A mesh network can be deployed rapidly in areas where the existing wireless infrastructure is damaged or unavailable, such as after an earthquake, flood, or fire. A mesh network can also support emergency services, such as fire fighting, search and rescue, or medical assistance, by enabling data, voice, and video transmission among the responders and command centers.
Mobile surveillance: A mesh network can enable real-time monitoring and control of public safety vehicles, such as police cars, ambulances, or drones, by providing high-bandwidth and low-latency wireless connectivity. A mesh network can also support video streaming, location tracking, remote sensing, or analytics applications for public safety purposes.
Event management: A mesh network can enhance the security and efficiency of large-scale events, such as concerts, festivals, or parades, by providing wireless coverage and capacity for the event organizers and participants. A mesh network can also support crowd management, traffic control, or public announcement applications for event management.
The other options are not the best solutions for creating a wireless field network to provide reliable service to public safety vehicles. An ad hoc network is a type of wireless network that consists of devices that communicate with each other directly without any central coordination or infrastructure. An ad hoc network is simple and flexible, but it has limited scalability and performance3. A point-to-point network is a type of wireless network that consists of two devices that communicate with each other over a single link. A point-to-point network is fast and secure, but it has limited coverage and functionality. An infrastructure network is a type of wireless network that consists of devices that communicate with each other through an access point or router. An infrastructure network is stable and robust, but it has high cost and complexity.

QUESTION 288
Users ate moving back into an office that had been vacant for awhile. Ten workstations are hooked up in the office, but one workstation cannot obtain a link with (he switch. A network engineer checks the documentation and cable labeling, and everything is hooked up as expected. The engineer moves the connection lo a different switchport. but a link still cannot be obtained. When the engineer puts a tone generator on (he infrastructure cable, no tone is heard at the far end. Which of the following issues is the engineer MOST likely trying to find?

A. A bad switchport
B. A break in the cable
C. A cable short
D. Cable interference

Correct Answer: B
Section:
Explanation:
A break in the cable means that there is no electrical continuity between the two ends of the cable, which prevents the signal from reaching the switch. A tone generator is a device that sends an audible signal through the cable, and if no tone is heard at the far end, it indicates a break in the cable.

QUESTION 289
A network administrator is working to configure a new device to provide Layer 2 connectivity to various endpoints including several WAPs. Which of the following devices will the administrator MOST likely configure?

A. WLAN controller
B. Cable modem
C. Load balancer
D. Switch
E. Hub

Correct Answer: D
Section:
Explanation:
A switch is a device that provides Layer 2 connectivity to various endpoints by forwarding frames based on MAC addresses. A switch can also connect to several WAPs (wireless access points) to provide wireless connectivity to wireless devices.

QUESTION 290

A network deployment engineer is deploying a new single-channel 10G optical connection. Which of the following optics should the engineer MOST likely use to satisfy this requirement?

A. QSFP
B. QSFP+
C. SFP
D. SFP+

Correct Answer: D
Section:
Explanation:
SFP+ is a type of optical transceiver that supports 10G single-channel transmission over fiber optic cables. SFP+ stands for small form-factor pluggable plus, and it is compatible with SFP slots on switches and routers.

QUESTION 291
A technician is troubleshooting network connectivity from a wall jack. Readings from a multimeter indicate extremely low ohmic values instead of the rated impedance from the switchport. Which of the following is the MOST likely cause of this issue?

A. Incorrect transceivers
B. Faulty LED
C. Short circuit
D. Upgraded OS version on switch

Correct Answer: C
Section:
Explanation:
A short circuit is a condition where two conductors in a circuit are connected unintentionally, creating a low resistance path for the current. This causes the voltage to drop and the current to increase, which can damage the circuit or cause a fire. A multimeter can measure the resistance or impedance of a circuit, and if it shows extremely low values, it indicates a short circuit.

QUESTION 292
A technician is troubleshooting a user's connectivity issues and finds that the computer's IP address was changed to 169.254.0.1.
Which of the following is the most likely reason?

A. Two or more computers have the same IP address in the ARP table.
B. The computer automatically set this address because the DHCP was not available.
C. The computer was set up to perform as an NTP server.
D. The computer is on a VPN and is the first to obtain a different IP address in that network.

Correct Answer: B
Section:
Explanation:
IP addresses beginning with 169.254.are calledlink-local addressesorAPIPA (Automatic Private IP Addressing)1.They are assigned by the computer itself when it cannot reach a DHCP server to obtain a valid IP address from the network2.This can happen for several reasons, such as a faulty router, a misconfigured network, or a disconnected cable3.
To troubleshoot this issue, the technician should check the network settings, the router configuration, and the physical connection of the computer. The technician should also try to renew the IP address by using the commandipconfig /renewin Windows ordhclientin Linux. If the problem persists, the technician may need to contact the network administrator or the ISP for further assistance.

QUESTION 293
A company's publicly accessible servers are connected to a switch between the company's ISP-connected router and the firewall in front of the company network. The firewall is stateful, and the router is running an ACL.
Which of the following best describes the area between the router and the firewall?

A. Untrusted zone
B. Screened subnet
C. Trusted zone
D. Private VLAN

Correct Answer: B
Section:
Explanation:
A screened subnet is a network segment that is isolated from both the internal and external networks by firewalls or routers. It is used to host publicly accessible servers that need some protection from external attacks, but also need to be separated from the internal network for security reasons.
Reference
1: Seven-Second Subnetting -- N10-008 CompTIA Network+ : 1.4
2: CompTIA Network+ Study Guide: Exam N10-008, 5th Edition, page 56
3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 22

QUESTION 294
A network manager wants to view network traffic for devices connected to a switch. A network engineer connects an appliance to a free port on the switch and needs to configure the switch port connected to the appliance. Which of the following is the best option for the engineer to enable?

A. Trunking
B. Port mirroring
C. Full duplex
D. SNMP

Correct Answer: B
Section:
Explanation:
Port mirroring is a feature that allows a switch to copy the traffic from one or more ports to another port, where a network analyzer or a monitoring device can capture and analyze the traffic. Port mirroring is useful for troubleshooting and security purposes, as it allows the network engineer to see the traffic that is passing through the switch without affecting the normal operation of the network.
Reference
1: Port Mirroring - CompTIA Network+ Certification (N10-008): The Total Course [Video]
2: CompTIA Network+ Certification Exam Objectives, page 5
3: CompTIA Network+ N10-005: 2.1 -- Port Mirroring - Professor Messer IT Certification Training Courses
4: CompTIA Network+ N10-005: 1.4 -- Port Mirroring

QUESTION 295
Which of the following protocols should be used when Layer 3 availability is of the highest concern?

A. LACP
B. LDAP
C. FHRP
D. DHCP

Correct Answer: C
Section:
Explanation:
FHRP stands for First Hop Redundancy Protocol, which is a group of protocols that allow routers or switches to provide backup or failover for the default gateway in a network. FHRP ensures that the network traffic can reach its destination even if the primary gateway fails or becomes unavailable. Some examples of FHRP protocols are HSRP, VRRP, and GLBP.

Reference
1: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 18
2: CompTIA Network+ N10-008 Certification Practice Test, question 9
3: CompTIA Network+ Study Guide: Exam N10-008, 5th Edition, page 263
4: CompTIA Network+ (N10-008) Practice Exam w/PBQ & Solution, question 5
5: What's on the CompTIA Network+ 008 certification? | CompTIA, section 3.1

QUESTION 296
The cybersecurity department needs to monitor historical IP network traffic on the WAN interface of the outside router without installing network sensors. Which of the following would be best to allow the department to complete this task?

A. Enabling NetFlow on the interface
B. Enabling SSH on the Interface
C. Enabling SNMP on the interlace
D. Enabling 802.1Q on the Interface

Correct Answer: A
Section:
Explanation:
NetFlowis a protocol that collects and analyzes network traffic data. It provides information about the source and destination of traffic, the volume of data, and other relevant details.
By enabling NetFlow on the WAN interface, the cybersecurity department can monitor historical traffic patterns without additional hardware or sensors.
Professor Messer's Network+ Study Guide

QUESTION 297
A company is implementing a secure remote access solution for multiple employees. Which of the following should the company use?

A. Remote desktop connection
B. Virtual desktop
C. Site-to-site VPN
D. Client-to-site VPN

Correct Answer: D
Section:
Explanation:
A client-to-site VPN is a secure remote access solution that allows individual employees to connect to the company's network from remote locations1.This type of VPN creates a secure tunnel from the user's location to the company's network, ensuring that the data transmitted is secure and private

QUESTION 298
Which of the following is a hybrid routing protocol?

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

Correct Answer: D
Section:
Explanation:

Enhanced Interior Gateway Routing Protocol (EIGRP) is a hybrid routing protocol23.It combines the features of Distance Vector Routing Protocol (DVRP) and Link State Routing Protocol (LSRP), making it an effective solution for larger networks that require scalable and efficient routing

QUESTION 299
A network administrator wants all outgoing traffic to the internet to flow through a single device for web content inspection. Which of the following devices is the most appropriate?

A. VPN headend
B. Router
C. Proxy server
D. Load balancer

Correct Answer: C
Section:
Explanation:
A proxy server is the most appropriate device for inspecting all outgoing traffic to the internet5.It acts as an intermediary between users and the internet, allowing the network administrator to inspect and control the content accessed by the users

QUESTION 300
Which of the following is the most accurate NTP time source that is capable of being accessed across a network connection?

A. Stratum 0 device
B. Stratum 1 device
C. Stratum 7 device
D. Stratum 16 device

Correct Answer: B
Section:
Explanation:
The most accurate NTP (Network Time Protocol) time source that can be accessed across a network connection is theStratum 1 device. Here's why:
Stratum 0 device: These are reference clocks, such as atomic clocks or GPS receivers, which directly measure time. They are not accessible over the network.
Stratum 1 device: These are servers that synchronize their time with Stratum 0 devices. They are highly accurate and can be accessed over the network.
Stratum 7 device: This is not a standard stratum level in NTP. The valid stratum levels are 0 to 16.
Stratum 16 device: This is a reserved value and not used in practice.
Therefore, the correct answer isB. Stratum 1 device1.

QUESTION 301
An organization needs a solution that will inspect network traffic, determine security threats using signature-based rules, and block the traffic in real time based on the security assessment. Which of the following network devices will support these requirements?

A. SIEM
B. VPN
C. IPS
D. DLP

Correct Answer: C
Section:
Explanation:
An Intrusion Prevention System (IPS) is designed to inspect network traffic, identify malicious activity using signature-based rules, and block potentially harmful traffic in real time. This aligns with the requirements stated in

the question.
CompTIA Network+ N10-008 Certification Study Guide1
CompTIA Network+ N10-007 vs.N10-008: What's New

QUESTION 302
Which of the following describes the differences between switches and hubs?

A. Switches operate on the physical layer, while hubs operate on the data link layer.
B. Switches operate on the session layer, while hubs operate on the transport layer.
C. Switches operate on the data link layer, while hubs operate on the physial layer.
D. Switches operate on the transport layer, while hubs operate on the data link layer.

Correct Answer: C
Section:
Explanation:
Switches operate at the data link layer (Layer 2) of the OSI model and make decisions based on MAC addresses. Hubs, on the other hand, operate at the physical layer (Layer 1) and simply repeat the signals they receive to all connected devices without any filtering or decision-making.
Networking Devices -- N10-008 CompTIA Network+ : 2.1