Number: N10-009
Passing Score: 800
Time Limit: 120
File Version: 41.0

Exam Code: N10-009

Exam Name: CompTIA Network+ Certification

Exam A

QUESTION 1
Which of the following network traffic type is sent to all nodes on the network?

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

Correct Answer: B
Section:
Explanation:
Broadcast traffic is sent to all nodes on the network. In a broadcast, a single packet is transmitted to all devices in the network segment. This is commonly used for tasks like ARP (Address Resolution Protocol) requests.
Broadcast Domain: All devices within the same broadcast domain will receive broadcast traffic.
Network Types: Ethernet networks commonly use broadcast traffic for certain functions, including network discovery and addressing.
IPv4 Broadcast: An IPv4 broadcast address (e.g., 255.255.255.255) ensures the packet is sent to all devices on the network.
Network

QUESTION 2
A client wants to increase overall security after a recent breach. Which of the following would be best to implement? (Select two.)

A. Least privilege network access
B. Dynamic inventeries
C. Central policy management
D. Zero-touch provisioning
E. Configuration drift prevention
F. Subnet range limits

Correct Answer: A, C
Section:
Explanation:
To increase overall security after a recent breach, implementing least privilege network access and central policy management are effective strategies.
Least Privilege Network Access: This principle ensures that users and devices are granted only the access necessary to perform their functions, minimizing the potential for unauthorized access or breaches. By limiting permissions, the risk of an attacker gaining access to critical parts of the network is reduced.
Central Policy Management: Centralized management of security policies allows for consistent and streamlined implementation of security measures across the entire network. This helps in quickly responding to security incidents, ensuring compliance with security protocols, and reducing the chances of misconfigurations.
Network

QUESTION 3
An administrator is configuring a switch that will be placed in an area of the office that is accessible to customers. Which of the following is the best way for the administrator to mitigate unknown devices from connecting to the network?

A. SSE
B. ACL
C. Perimeter network
D. 802.1x

Correct Answer: D
Section:
Explanation:
802.1x is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. This ensures that only authorized devices can access the network, making it ideal for mitigating the risk of unknown devices connecting to the network, especially in accessible areas.
802.1x Authentication: Requires devices to authenticate using credentials (e.g., username and password, certificates) before gaining network access.
Access Control: Prevents unauthorized devices from connecting to the network, enhancing security in public or semi-public areas.
Implementation: Typically used in conjunction with a RADIUS server to manage authentication requests.
Network

QUESTION 4
Which of the following is the most likely reason an insurance brokerage would enforce VPN usage?

A. To encrypt sensitive data in transit
B. To secure the endpoint
C. To maintain contractual agreements
D. To comply with data retentin requirements

Correct Answer: A
Section:
Explanation:
The most likely reason an insurance brokerage would enforce VPN usage is to encrypt sensitive data in transit. VPNs (Virtual Private Networks) create a secure tunnel between the user's device and the corporate network, ensuring that data is encrypted and protected from interception.
Encryption: VPNs encrypt data, preventing unauthorized access and ensuring data privacy during transmission over public or unsecured networks.
Data Protection: Essential for industries handling sensitive information, such as insurance brokerages, to protect customer data and comply with regulatory requirements.
Security: Enhances overall network security by providing secure remote access for employees.
Network

QUESTION 5
Which of the following steps in the troubleshooting methodology would be next after putting preventive measures in place?

A. Implement the solution.
B. Verify system functionality.
C. Establish a plan of action.
D. Test the theory to determine cause.

Correct Answer: B
Section:
Explanation:
After implementing a solution and putting preventive measures in place, the next step is to verify that the system is functioning correctly. This ensures that the issue has been fully resolved.

QUESTION 6
An organization wants to ensure that incoming emails were sent from a trusted source. Which of the following DNS records is used to verify the source?

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

Correct Answer: A
Section:

QUESTION 7
A network engineer configures a new switch and connects it to an existing switch for expansion and redundancy. Users immediately lose connectivity to the network. The network engineer notes the following spanning tree information from both switches:
Switch 1
Port State Cost
1 Forward 2
2 Forward 2
Switch 2
Port State Cost
1 Forward 2
2 Forward 2
Which of the following best describes the issue?

A. The port cost should not be equal.
B. The ports should use link aggregation.
C. A root bridge needs to be identified.
D. The switch should be configured for RSTP.

Correct Answer: C
Section:

QUESTION 8
A support agent receives a report that a remote user's wired devices are constantly disconnecting and have slow speeds. Upon inspection, the support agent sees that the user's coaxial modern has a signal power of -97dB.

A. Removing any spliters connecte to the line
B. Switching the devices to wireless
C. Moving the devices closer to the modern
D. Lowering the network speed

Correct Answer: A
Section:
Explanation:
A signal power of -97dB indicates a very weak signal, which can cause connectivity issues and slow speeds. Splitters on a coaxial line can degrade the signal quality further, so removing them can help improve the signal strength and overall connection quality.
Signal Quality: Splitters can reduce the signal strength by dividing the signal among multiple lines, which can be detrimental when the signal is already weak.
Direct Connection: Ensuring a direct connection from the modem to the incoming line can maximize signal quality and reduce potential points of failure.
Network

QUESTION 9
Which of the following technologies are X.509 certificates most commonly associated with?

A. PKI
B. VLAN tagging
C. LDAP
D. MFA

Correct Answer: A
Section:
Explanation:
X 509 certificates are most commonly associated with Public Key Infrastructure (PKI). These certificates are used for a variety of security functions, including digital signatures, encryption, and authentication. PKI: X.509 certificates are a fundamental component of PKI, used to manage encryption keys and authenticate users and devices. Digital Certificates: They are used to establish secure communications over networks, such as SSL/TLS for websites and secure email communication. Authentication and Encryption: X.509 certificates provide the means to securely exchange keys and verify identities in various applications, ensuring data integrity and confidentiality. Network
Reference: CompTIA Network+ N10-007 Official Certification Guide: Covers PKI and the role of X.509 certificates in network security. Cisco Networking Academy: Provides training on PKI, certificates, and secure communications. Network+ Certification All-in-One Exam Guide: Explains PKI, X.509 certificates, and their applications in securing network communications.

QUESTION 10
Which of the following attacks utilizes a network packet that contains multiple network tags?

A. MAC flooding
B. VLAN hopping
C. DNS spoofing
D. ARP poisoning

Correct Answer: B
Section:
Explanation:
VLAN hopping is an attack where an attacker crafts packets with multiple VLAN tags, allowing them to traverse VLAN boundaries improperly. This can result in gaining unauthorized access to network segments that are supposed to be isolated. The other options do not involve the use of multiple network tags. MAC flooding aims to overwhelm a switch's MAC address table, DNS spoofing involves forging DNS responses, and ARP poisoning involves sending fake ARP messages.
According to the CompTIA Network+ course materials, VLAN hopping exploits the tagging mechanism in network packets to gain unauthorized access.

QUESTION 11
Which of the following describes the best reason for using BGP?

A. Preventing a loop within a LAN
B. Improving reconvergence times
C. Exchanging router updates with a different ISP
D. Sharing routes with a Layer 3 switch

Correct Answer: C
Section:
Explanation:

BGP (Border Gateway Protocol) is used for routing data between different ISPs, making it essential for the functioning of the internet. Its primary use is for exchanging routing information between autonomous systems, especially different ISPs. Preventing loops within a LAN is handled by protocols like Spanning Tree Protocol (STP), while improving reconvergence times and sharing routes with a Layer 3 switch are functions of other protocols or internal mechanisms.
The CompTIA Network+ training emphasizes BGP's role in the exchange of routing information across different ISPs and autonomous systems.

QUESTION 12
A company's marketing team created a new application and would like to create a DNS record for newapplication.comptia.org that always resolves to the same address as www.comptia.org. Which of the following records should the administrator use?

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

Correct Answer: C
Section:
Explanation:
A CNAME (Canonical Name) record is used in DNS to alias one domain name to another. This means that newapplication.comptia.org can be made to resolve to the same IP address as www.comptia.org by creating a CNAME record pointing newapplication.comptia.org to www.comptia.org. SOA (Start of Authority) is used for DNS zone information, MX (Mail Exchange) is for mail server records, and NS (Name Server) is for specifying authoritative DNS servers.
The DNS section of the CompTIA Network+ materials describes the use of CNAME records for creating domain aliases.

QUESTION 13
Which of the following is the most closely associated with segmenting compute resources within a single cloud account?

A. Network security group
B. laaS
C. VPC
D. Hybrid cloud

Correct Answer: C
Section:
Explanation:
A Virtual Private Cloud (VPC) is most closely associated with segmenting compute resources within a single cloud account. A VPC allows you to define a virtual network that closely resembles a traditional network, complete with subnets, route tables, and gateways. This segmentation enables the isolation of different parts of a network within a cloud environment, ensuring security and efficient resource management. VPCs are a key component in many cloud infrastructures, providing the flexibility to manage and control network settings and resources.
Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

QUESTION 14
A user connects to a corporate VPN via a web browser and is able to use TLS to access the internal financial system to input a time card. Which of the following best describes how the VPN is being used?

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

Correct Answer: A
Section:

Explanation:
The scenario describes a user connecting to a corporate VPN via a web browser using TLS to access an internal system. This setup is best described as a 'clientless' VPN. Clientless VPNs do not require a VPN client to be installed on the user's device; instead, they rely on a standard web browser to establish the connection. This method is particularly useful for providing secure, remote access to applications through a web interface without the need for additional software installations.
Reference: CompTIA Network+ Certification Exam Objectives - Remote Access Methods section.

QUESTION 15
A network engineer wants to implement a new IDS between the switch and a router connected to the LAN. The engineer does not want to introduce any latency by placing the IDS in line with the gateway. The engineer does want to ensure that the IDS sees all packets without any loss. Which of the following is the best way for the engineer to implement the IDS?

A. Use a network tap.
B. Use Nmap software.
C. Use a protocol analyzer.
D. Use a port mirror.

Correct Answer: D
Section:
Explanation:
To ensure that an IDS sees all packets without any loss and without introducing latency, the best approach is to use a port mirror, also known as a SPAN (Switched Port Analyzer) port. Port mirroring copies network packets seen on one switch port (or an entire VLAN) to another port where the IDS is connected. This method allows the IDS to monitor traffic passively without being in the direct path of network traffic, thus avoiding any additional latency.
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

QUESTION 16
Which of the following must be implemented to securely connect a company's headquarters with a branch location?

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

Correct Answer: D
Section:
Explanation:
Site-to-Site VPN: A site-to-site VPN is used to securely connect two networks, such as a company's headquarters and a branch location, over the internet. This type of VPN creates a secure tunnel for data transmission, ensuring confidentiality and integrity.
Split-tunnel VPN (A): Allows some traffic to bypass the VPN tunnel, which may not secure all communications.
Clientless VPN (B): Used for individual users to access the network without VPN client software.
Full-tunnel VPN (C): Typically used for individual user traffic rather than connecting two networks.

QUESTION 17
A network administrator needs to assign IP addresses to a newly installed network. They choose 192.168.1.0/24 as their network address and need to create three subnets with 30 hosts on each subnet. Which of the following is a valid subnet mask that will meet the requirements?

A. 255.255.255.128
B. 255.255.255.192
C. 255.255.255.224
D. 255.255.255.240

Correct Answer: B
Section:
Explanation:
To create three subnets with at least 30 hosts each:
Subnet Calculation: Each subnet must support 32 addresses (30 usable + 2 reserved for network and broadcast).
Bits for Subnets: Subnet mask 255.255.255.192 (/26) provides 64 addresses per subnet (4 subnets total).
Valid Subnets: Each subnet provides sufficient IPs to meet the requirement.
255.255.255.128 (A): Creates only 2 subnets, not enough for the requirement.
255.255.255.224 (C): Provides 8 subnets but only 30 addresses per subnet (28 usable), insufficient for hosts.
255.255.255.240 (D): Too restrictive, only 16 addresses per subnet (14 usable).

QUESTION 18
Network administrators are using the Telnet protocol to administer network devices that are on the 192.168.1.0/24 subnet. Which of the following tools should the administrator use to best identify the devices?

A. dig
B. runap
C. tracert
D. telnet

Correct Answer: D
Section:
Explanation:
Telnet: Telnet is a protocol used to establish remote connections to devices for administration. It directly communicates with devices on the network and is the best tool for identifying and accessing devices that support it on the subnet.
dig (A): Used for DNS queries, unrelated to Telnet.
runap (B): Not a recognized tool in this context.
tracert (C): Tracks the path to a host but does not establish direct connections.

QUESTION 19
Which of the following panels would be best to facilitate a central termination point for all network cables on the floor of a company building?

A. Patch
B. UPS
C. MDF
D. Rack

Correct Answer: A
Section:
Explanation:
A patch panel is the best choice to facilitate a central termination point for all network cables on the floor of a company building. Patch panels are used to manage and organize multiple network cables, providing a central point where all cables converge. This setup allows for easy management, troubleshooting, and reconfiguration of network connections. The other options, such as UPS (Uninterruptible Power Supply), MDF (Main Distribution Frame), and rack, serve different purposes and are not specifically designed for the central termination of network cables.
Reference: CompTIA Network+ Certification Exam Objectives - Network Installation section.

QUESTION 20
A customer needs six usable IP addresses. Which of the following best meets this requirement?

A. 255.255.255.128

B. 255.255.255.192
C. 255.255.255.224
D. 255.255.255.240

Correct Answer: D
Section:
Explanation:
To meet the requirement of six usable IP addresses, the subnet mask 255.255.255.240 (also represented as /28) is the best fit. A /28 subnet provides 16 total IP addresses, out of which 14 are usable (the first address is the network address, and the last address is the broadcast address). This meets and exceeds the requirement for six usable IP addresses, ensuring there are enough addresses for future expansion if needed. The other options provide either too few or too many addresses for this specific requirement.
Reference: CompTIA Network+ Certification Exam Objectives - IP Addressing section.

QUESTION 21
A network administrator needs to connect two routers in a point-to-point configuration and conserve IP space. Which of the following subnets should the administrator use?

A. 724
B. /26
C. /28
D. /30

Correct Answer: D
Section:
Explanation:
Using a /30 subnet mask is the most efficient way to conserve IP space for a point-to-point connection between two routers. A /30 subnet provides four IP addresses, two of which can be assigned to the router interfaces, one for the network address, and one for the broadcast address. This makes it ideal for point-to-point links where only two usable IP addresses are needed.
Reference: CompTIA Network+ study materials and subnetting principles.

QUESTION 22
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 the best choice for the CTO's requirements. It allows the organization to run key services from the on-site data center while leveraging the cloud for enterprise services. This approach provides flexibility, scalability, and cost savings, while also minimizing disruptions to users by keeping critical services local. The hybrid model integrates both private and public cloud environments, offering the benefits of both.
Reference: CompTIA Network+ study materials and cloud computing principles.

QUESTION 23
A technician is troubleshooting a user's laptop that is unable to connect to a corporate server. The technician thinks the issue pertains to routing. Which of the following commands should the technician use to identify the issue?

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

Correct Answer: C
Section:
Explanation:
The tracert (Traceroute) command is used to determine the path packets take from the source to the destination. It helps in identifying routing issues by showing each hop the packets pass through, along with the time taken for each hop. This command can pinpoint where the connection is failing or experiencing delays, making it an essential tool for troubleshooting routing issues.
Reference: CompTIA Network+ study materials and common network troubleshooting commands.

QUESTION 24
Which of the following fiber connector types is the most likely to be used on a network interface card?

A. LC
B. SC
C. ST
D. MPO

Correct Answer: A
Section:
Explanation:
Definition of Fiber Connector Types:
LC (Lucent Connector): A small form-factor fiber optic connector with a push-pull latching mechanism, commonly used for high-density applications.
SC (Subscriber Connector or Standard Connector): A larger form-factor connector with a push-pull latching mechanism, often used in datacom and telecom applications.
ST (Straight Tip): A bayonet-style connector, typically used in multimode fiber optic networks.
MPO (Multi-fiber Push On): A connector designed to support multiple fibers (typically 12 or 24 fibers), used in high-density cabling environments.
Common Usage:
LC Connectors: Due to their small size, LC connectors are widely used in network interface cards (NICs) and high-density environments such as data centers. They allow for more connections in a smaller space compared to SC and ST connectors.
SC and ST Connectors: These are larger and more commonly used in patch panels and older fiber installations but are less suitable for high-density applications.
MPO Connectors: Primarily used for trunk cables in data centers and high-density applications but not typically on individual network interface cards.
Selection Criteria:
The small form-factor and high-density capabilities of LC connectors make them the preferred choice for network interface cards, where space and connection density are critical considerations.
CompTIA Network+ study materials on fiber optics and connector types.

QUESTION 25
A network engineer receives a vendor alert regarding a vulnerability in a router CPU. Which of the following should the engineer do to resolve the issue?

A. Update the firmware.
B. Replace the system board.
C. Patch the OS.
D. Isolate the system.

Correct Answer: A
Section:
Explanation:

Understanding the Vulnerability:
Vulnerabilities in the router CPU can be exploited to cause performance degradation, unauthorized access, or other security issues.
Firmware Update:
Firmware Role: The firmware is low-level software that controls the hardware of a device. Updating the firmware can address vulnerabilities by providing patches and enhancements from the manufacturer.
Procedure: Download the latest firmware from the vendor's website, follow the manufacturer's instructions to apply the update, and verify that the update resolves the vulnerability.
Comparison with Other Options:
Replace the System Board: This is a costly and often unnecessary step if the issue can be resolved with a firmware update.
Patch the OS: Patching the OS is relevant for devices with a full operating system but not directly applicable to addressing a CPU vulnerability on a router.
Isolate the System: Temporarily isolating the system can mitigate immediate risk but does not resolve the underlying vulnerability.
Best Practice:
Regularly check for and apply firmware updates to ensure that network devices are protected against known vulnerabilities.
CompTIA Network+ study materials on network security and device management.

QUESTION 26
A virtual machine has the following configuration:
* IPv4 address: 169.254.10.10
* Subnet mask: 255.255.0.0
The virtual machine can reach colocated systems but cannot reach external addresses on the Internet. Which of the following Is most likely the root cause?

A. The subnet mask is incorrect.
B. The DHCP server is offline.
C. The IP address is an RFC1918 private address.
D. The DNS server is unreachable.

Correct Answer: B
Section:
Explanation:
Understanding the 169.254.x.x Address:
An IPv4 address in the range of 169.254.x.x is an Automatic Private IP Addressing (APIPA) address, assigned when a DHCP server is unavailable.
DHCP Server Offline:
APIPA Assignment: When a device cannot obtain an IP address from a DHCP server, it assigns itself an APIPA address to enable local network communication. This allows communication with other devices on the same local subnet but not with external networks.
Resolution: Ensure the DHCP server is operational. Check for connectivity issues between the virtual machine and the DHCP server, and verify the DHCP server settings.
Comparison with Other Options:
The subnet mask is incorrect: The subnet mask 255.255.0.0 is appropriate for the 169.254.x.x range and does not prevent external access by itself.
The IP address is an RFC1918 private address: RFC1918 addresses are private IP ranges (10.x.x.x, 172.16.x.x-172.31.x.x, 192.168.x.x) but 169.254.x.x is not one of them.
The DNS server is unreachable: While this could affect name resolution, it would not prevent the assignment of a non-APIPA address or local network communication.
Troubleshooting Steps:
Verify the DHCP server's status and connectivity.
Restart the DHCP service if necessary.
Renew the IP lease on the virtual machine using commands such as ipconfig /renew (Windows) or dhclient (Linux).
CompTIA Network+ study materials on IP addressing and DHCP troubleshooting.

QUESTION 27
A network technician is troubleshooting a web application's poor performance. The office has two internet links that share the traffic load. Which of the following tools should the technician use to determine which link is being used for the web application?

A. netstat
B. nslookup

C. ping
D. tracert

Correct Answer: D
Section:
Explanation:
Understanding Tracert:
Traceroute Tool: tracert (Windows) or traceroute (Linux) is a network diagnostic tool used to trace the path that packets take from a source to a destination. It lists all the intermediate routers the packets traverse.
Determining Traffic Path:
Path Identification: By running tracert to the web application's destination IP address, the technician can identify which route the traffic is taking and thereby determine which internet link is being used.
Load Balancing Insight: If the office uses load balancing for its internet links, tracert can help verify which link is currently handling the traffic for the web application.
Comparison with Other Tools:
netstat: Displays network connections, routing tables, interface statistics, and more, but does not trace the path of packets.
nslookup: Used for querying DNS to obtain domain name or IP address mapping, not for tracing packet routes.
ping: Tests connectivity and measures round-trip time but does not provide path information.
Implementation:
Open a command prompt or terminal.
Execute tracert [destination IP] to trace the route.
Analyze the output to determine the path and the link being used.
CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

QUESTION 28
A network administrator configured a router interface as 10.0.0.95 255.255.255.240. The administrator discovers that the router is not routing packets to a web server with IP 10.0.0.81/28. Which of the following is the best explanation?

A. The web server Is In a different subnet.
B. The router interface is a broadcast address.
C. The IP address space is a class A network.
D. The subnet is in a private address space.

Correct Answer: B
Section:
Explanation:
Understanding Subnetting:
The subnet mask 255.255.255.240 (or /28) indicates that each subnet has 16 IP addresses (14 usable addresses, 1 network address, and 1 broadcast address).
Calculating the Subnet Range:
Subnet Calculation: For the IP address 10.0.0.95 with a /28 subnet mask:
Network address: 10.0.0.80
Usable IP range: 10.0.0.81 to 10.0.0.94
Broadcast address: 10.0.0.95
Router Interface Configuration:
Broadcast Address Issue: The IP address 10.0.0.95 is the broadcast address for the subnet 10.0.0.80/28. Configuring a router interface with the broadcast address will cause routing issues as it is not a valid host address.
Comparison with Other Options:
The web server is in a different subnet: The web server (10.0.0.81) is within the same subnet range (10.0.0.80/28).
The IP address space is a class A network: While 10.0.0.0 is a Class A network, this does not explain the routing issue caused by the broadcast address.
The subnet is in a private address space: The private address space designation (RFC 1918) does not impact the routing issue related to the broadcast address configuration.
Resolution:
Reconfigure the router interface with a valid host IP address within the usable range, such as 10.0.0.94.
CompTIA Network+ study materials on subnetting and IP address configuration.

QUESTION 29
Which of the following does a full-tunnel VPN provide?

A. Lower bandwidth requirements
B. The ability to reset local computer passwords
C. Corporate Inspection of all network traffic
D. Access to blocked sites

Correct Answer: C
Section:
Explanation:
A full-tunnel VPN routes all of a user's network traffic through the corporate network. This means that the organization can inspect all network traffic for security and compliance purposes, as all data is tunneled through the VPN, allowing for comprehensive monitoring and inspection.
Reference: CompTIA Network+ study materials.

QUESTION 30
A customer is adding fiber connectivity between adjacent buildings. A technician terminates the multimode cable to the fiber patch panel. After the technician connects the fiber patch cable, the indicator light does not turn on. Which of the following should a technician try first to troubleshoot this issue?

A. Reverse the fibers.
B. Reterminate the fibers.
C. Verify the fiber size.
D. Examine the cable runs for visual faults.

Correct Answer: A
Section:
Explanation:
When working with fiber optic cables, one common issue is that the transmit (TX) and receive (RX) fibers might be reversed. The first step in troubleshooting should be to reverse the fibers at one end to ensure they are correctly aligned (TX to RX and RX to TX). This is a simple and quick step to rule out a common issue before moving on to more complex troubleshooting.
Reference: CompTIA Network+ study materials.

QUESTION 31
Which of the following protocols has a default administrative distance value of 90?

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

Correct Answer: B
Section:
Explanation:
EIGRP (Enhanced Interior Gateway Routing Protocol) has a default administrative distance (AD) value of 90 for internal routes. The administrative distance is used to rate the trustworthiness of routing information received from different routing protocols. EIGRP, developed by Cisco, has an AD of 90, which is lower than that of RIP (120) and OSPF (110), making it more preferred if multiple protocols provide a route to the same destination.
Reference: CompTIA Network+ study materials.

QUESTION 32
Which of the following is a cost-effective advantage of a split-tunnel VPN?

A. Web traffic is filtered through a web filter.
B. More bandwidth is required on the company's internet connection.
C. Monitoring detects insecure machines on the company's network.
D. Cloud-based traffic flows outside of the company's network.

Correct Answer: D
Section:
Explanation:
A split-tunnel VPN allows certain traffic (e.g., cloud-based services) to bypass the VPN and go directly to the Internet. This reduces the amount of traffic that needs to traverse the company's VPN and Internet connection, conserving bandwidth and reducing costs. It also means that not all traffic is subject to the same level of inspection or filtering, which can improve performance for cloud-based services.
Reference: CompTIA Network+ study materials.

QUESTION 33
Which of the following should be configured so users can authenticate to a wireless network using company credentials?

A. SSO
B. SAML
C. MFA
D. RADIUS

Correct Answer: D
Section:
Explanation:
RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. RADIUS is often used to manage access to wireless networks, enabling users to authenticate with their company credentials, ensuring secure access to the network.
Reference: CompTIA Network+ study materials.

QUESTION 34
Which of the following is most likely responsible for the security and handling of personal data in Europe?

A. GDPR
B. SCADA
C. SAML
D. PCI DSS

Correct Answer: A
Section:
Explanation:
Definition of GDPR:
General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.
Scope and Objectives:
GDPR aims to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
It enforces rules about data protection, requiring companies to protect the personal data and privacy of EU citizens for transactions that occur within EU member states.
Comparison with Other Options:
SCADA (Supervisory Control and Data Acquisition): Refers to control systems used in industrial and infrastructure processes, not related to personal data protection.
SAML (Security Assertion Markup Language): A standard for exchanging authentication and authorization data between parties, not specifically for personal data protection.

PCI DSS (Payment Card Industry Data Security Standard): A set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment, not specific to personal data protection in Europe.
Key Provisions:
GDPR includes provisions for data processing, data subject rights, obligations of data controllers and processors, and penalties for non-compliance.
CompTIA Network+ study materials on regulatory and compliance standards.

QUESTION 35
Users cannot connect to an internal website with an IP address 10.249.3.76. A network administrator runs a command and receives the following output:
1 3ms 2ms 3ms 192.168.25.234
2 2ms 3ms 1ms 192.168.3.100
3 4ms 5ms 2ms 10.249.3.1
4 *
5 '
6 *
7 *
Which of the following command-line tools is the network administrator using?

A. tracert
B. netstat
C. tcpdump
D. nmap

Correct Answer: A
Section:
Explanation:
Understanding Tracert:
tracert (Traceroute in Windows) is a command-line tool used to trace the path that packets take from the source to the destination. It records the route (the specific gateways at each hop) and measures transit delays of packets across an IP network.
Output Analysis:
The output shows a series of IP addresses with corresponding round-trip times (RTTs) in milliseconds.
The asterisks (*) indicate that no response was received from those hops, which is typical for routers or firewalls that block ICMP packets used by tracert.
Comparison with Other Tools:
netstat: Displays network connections, routing tables, interface statistics, and more, but does not trace packet routes.
tcpdump: Captures network packets for analysis, used for detailed network traffic inspection.
nmap: A network scanning tool used to discover hosts and services on a network, not for tracing packet routes.
Usage:
tracert helps identify the path to a destination and locate points of failure or congestion in the network.
CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

QUESTION 36
Which of the following attacks would most likely cause duplicate IP addresses in a network?

A. Rogue DHCP server
B. DNS poisoning
C. Social engineering
D. Denial-of-service

Correct Answer: A
Section:

Explanation:
Definition of a Rogue DHCP Server:
A rogue DHCP server is an unauthorized DHCP server on a network, which can assign IP addresses to devices without proper control, leading to IP address conflicts.
Impact of a Rogue DHCP Server:
IP Address Conflicts: Multiple devices may receive the same IP address from different DHCP servers, causing network connectivity issues.
Network Disruption: Devices may be assigned incorrect network configuration settings, disrupting network services and connectivity.
Comparison with Other Attacks:
DNS poisoning: Alters DNS records to redirect traffic to malicious sites, but does not cause IP address conflicts.
Social engineering: Involves manipulating individuals to gain unauthorized access or information, not directly related to IP address conflicts.
Denial-of-service (DoS): Floods a network or service with excessive traffic to disrupt operations, but does not cause duplicate IP addresses.
Prevention and Detection:
Implement network access control measures to prevent unauthorized devices from acting as DHCP servers.
Use DHCP snooping on switches to allow DHCP responses only from authorized DHCP servers.
CompTIA Network+ study materials on network security threats and mitigation techniques.

QUESTION 37
A network administrator is deploying a new switch and wants to make sure that the default priority value was set for a spanning tree. Which of the following values would the network administrator expect to see?

A. 4096
B. 8192
C. 32768
D. 36684

Correct Answer: C
Section:
Explanation:
Understanding Spanning Tree Protocol (STP):
STP is used to prevent network loops in Ethernet networks by creating a spanning tree that selectively blocks some redundant paths.
Default Priority Value:
Bridge Priority: STP uses bridge priority to determine which switch becomes the root bridge. The default bridge priority value for most switches is 32768.
Priority Range: The bridge priority can be set in increments of 4096, ranging from 0 to 61440.
Configuration and Verification:
When deploying a new switch, the network administrator can verify the bridge priority using commands such as show spanning-tree to ensure it is set to the default value of 32768.
Comparison with Other Values:
4096 and 8192: Lower than the default priority, indicating these would be manually configured for higher preference.
36684: A non-standard value, likely a result of specific configuration changes.
CompTIA Network+ study materials on Spanning Tree Protocol and network configuration.

QUESTION 38
Which of the following steps of the troubleshooting methodology should a technician take to confirm a theory?

A. Duplicate the problem.
B. Identify the symptoms.
C. Gather information.
D. Determine any changes.

Correct Answer: A
Section:
Explanation:

Troubleshooting Methodology:
Troubleshooting involves a systematic approach to diagnosing and resolving issues. It typically includes steps such as identifying symptoms, gathering information, formulating and testing theories, and implementing solutions.
Confirming a Theory:
Duplicate the Problem: To confirm a theory, the technician should reproduce the problem in a controlled environment. This helps verify that the identified cause actually leads to the observed issue.
Verification: By duplicating the problem, the technician can observe the issue firsthand, validate the hypothesis, and rule out other potential causes.
Comparison with Other Steps:
Identify the Symptoms: Initial step to understand what the problem is, not specifically for confirming a theory.
Gather Information: Involves collecting data and details about the issue, usually done before formulating a theory.
Determine Any Changes: Involves checking for recent changes that could have caused the issue, a part of the information-gathering phase.
Implementation:
Use similar equipment or software in a test environment to recreate the issue.
Observe the results to see if they match the original problem, thereby confirming the theory.
CompTIA Network+ study materials on troubleshooting methodologies and best practices.

QUESTION 39
Early in the morning, an administrator installs a new DHCP server. In the afternoon, some users report they are experiencing network outages. Which of the following is the most likely issue?

A. The administrator did not provision enough IP addresses.
B. The administrator configured an incorrect default gateway.
C. The administrator did not provision enough routes.
D. The administrator did not provision enough MAC addresses.

Correct Answer: A
Section:
Explanation:
When a DHCP server is installed and not enough IP addresses are provisioned, users may start experiencing network outages once the available IP addresses are exhausted. DHCP servers assign IP addresses to devices on the network, and if the pool of addresses is too small, new devices or those renewing their lease may fail to obtain an IP address, resulting in network connectivity issues.
Reference: CompTIA Network+ study materials.

QUESTION 40
Which of the following network topologies contains a direct connection between every node in the network?

A. Mesh
B. Hub-and-spoke
C. Star
D. Point-to-point

Correct Answer: A
Section:
Explanation:
In a mesh topology, every node is directly connected to every other node. This provides high redundancy and reliability, as there are multiple paths for data to travel between nodes. This topology is often used in networks where high availability is crucial.
Reference: CompTIA Network+ study materials.

QUESTION 41
A company receives a cease-and-desist order from its ISP regarding prohibited torrent activity. Which of the following should be implemented to comply with the cease-and-desist order?

A. MAC security
B. Content filtering
C. Screened subnet
D. Perimeter network

Correct Answer: B
Section:
Explanation:
Content filtering can be used to block or restrict access to websites and services that facilitate torrenting and other prohibited activities. By implementing content filtering, the company can comply with the ISP's cease-and-desist order and prevent users from accessing torrent sites and engaging in prohibited activities.
Reference: CompTIA Network+ study materials.

QUESTION 42
A network administrator is connecting two Layer 2 switches in a network. These switches must transfer data in multiple networks. Which of the following would fulfill this requirement?

A. Jumbo frames
B. 802.1Q tagging
C. Native VLAN
D. Link aggregation

Correct Answer: B
Section:
Explanation:
802.1Q tagging, also known as VLAN tagging, is used to identify VLANs on a trunk link between switches. This allows the switches to transfer data for multiple VLANs (or networks) over a single physical connection. This method ensures that traffic from different VLANs is properly separated and managed across the network.
Reference: CompTIA Network+ study materials.

QUESTION 43
A systems administrator is investigating why users cannot reach a Linux web server with a browser but can ping the server IP. The server is online, the web server process is running, and the link to the switch is up. Which of the following commands should the administrator run on the server first?

A. traceroute
B. netstat
C. tcpdump
D. arp

Correct Answer: B
Section:
Explanation:
The netstat command provides information about network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. Running netstat on the server can help the administrator verify that the web server process is listening on the expected port (e.g., port 80 for HTTP or port 443 for HTTPS) and that there are no issues with network connections. This is a crucial first step in diagnosing why the web server is not accessible via a browser.
Reference: CompTIA Network+ study materials.

QUESTION 44
Which of the following best describes a group of devices that is used to lure unsuspecting attackers and to study the attackers' activities?

A. Geofencing

B. Honeynet
C. Jumpbox
D. Screened subnet

Correct Answer: B
Section:
Explanation:
A honeynet is a network of honeypots designed to attract and study attackers. Honeypots are decoy systems set up to lure cyber attackers and analyze their activities. A honeynet, being a collection of these systems, provides a broader view of attack methods and patterns, helping organizations improve their security measures.
Reference: CompTIA Network+ Exam Objectives and official study guides.

QUESTION 45
A customer recently moved into a new office and notices that some wall plates are not working and are not properly labeled Which of the following tools would be best to identify the proper wiring in the IDF?

A. Toner and probe
B. Cable tester
C. Visual fault locator
D. Network tap

Correct Answer: A
Section:
Explanation:
A toner and probe tool, also known as a tone generator and probe, is used to trace and identify individual cables within a bundle or to locate the termination points of cables in wiring closets and patch panels. It generates a tone that can be picked up by the probe, helping technicians quickly and accurately identify and label wall plates and wiring. This is the best tool for identifying proper wiring in the Intermediate Distribution Frame (IDF).
Reference: CompTIA Network+ Exam Objectives and official study guides.

QUESTION 46
A network administrator is planning to host a company application in the cloud, making the application available for all internal and third-party users. Which of the following concepts describes this arrangement?

A. Multitenancy
B. VPC
C. NFV
D. SaaS

Correct Answer: A
Section:
Explanation:
Multitenancy is a cloud computing architecture where a single instance of software serves multiple customers or tenants. Each tenant's data is isolated and remains invisible to other tenants. Hosting a company application in the cloud to be available for both internal and third-party users fits this concept, as it allows shared resources and infrastructure while maintaining data separation and security.
Reference: CompTIA Network+ Exam Objectives and official study guides.

QUESTION 47
A company wants to implement a disaster recovery site or non-critical applicance, which can tolerance a short period of downltime. Which of the followig type of sites should the company impelement to achive this goal?

A. Hot
B. Cold
C. Warm

D. Passive

Correct Answer: C
Section:
Explanation:
A warm site is a compromise between a hot site and a cold site, providing a balance between cost and recovery time. It is partially equipped with the necessary hardware, software, and infrastructure, allowing for a quicker recovery compared to a cold site but at a lower cost than a hot site.
Recovery Time: Warm sites can be operational within hours to a day, making them suitable for non-critical applications that can tolerate short downtimes.
Cost-Effectiveness: Warm sites are more economical than hot sites as they do not require all systems to be fully operational at all times.
Network

QUESTION 48
A user notifies a network administrator about losing access to a remote file server. The network administrator is able to ping the server and verifies the current firewall rules do not block access to the network fileshare. Which of the following tools wold help identify which ports are open on the remote file server?

A. Dig
B. Nmap
C. Tracert
D. nslookup

Correct Answer: B
Section:
Explanation:
Nmap (Network Mapper) is a powerful network scanning tool used to discover hosts and services on a computer network. It can be used to identify which ports are open on a remote server, which can help diagnose access issues to services like a remote file server.
Port Scanning: Nmap can perform comprehensive port scans to determine which ports are open and what services are running on those ports.
Network Discovery: It provides detailed information about the host's operating system, service versions, and network configuration.
Security Audits: Besides troubleshooting, Nmap is also used for security auditing and identifying potential vulnerabilities.
Network

QUESTION 49
A technician is planning an equipement installation into a rack in a data center that practices hot aisle/cold aise ventilation. Which of the following directions should the equipement exhaust face when installed in the rack?

A. Sides
B. Top
C. Front
D. Rear

Correct Answer: D
Section:
Explanation:
In a data center that practices hot aisle/cold aisle ventilation, equipment should be installed so that the exhaust faces the rear of the rack. This setup ensures that hot air is expelled into the hot aisle, maintaining proper airflow and cooling efficiency.
Hot Aisle/Cold Aisle Configuration: Equipment intake should face the cold aisle where cool air is supplied, and exhaust should face the hot aisle where hot air is expelled.
Cooling Efficiency: Proper orientation of equipment helps maintain an efficient cooling environment by segregating hot and cold air, preventing overheating and improving energy efficiency.
Network

QUESTION 50
Which of the following network cables involves bounding light off of protective cladding?

A. Twinaxial
B. Coaxial
C. Single-mode
D. Multimode

Correct Answer: D
Section:
Explanation:
Multimode fiber optic cables involve the transmission of light signals that bounce off the core's cladding as they travel down the fiber. This characteristic differentiates it from single-mode fiber, where the light travels directly down the fiber without reflecting off the cladding.
Here are some detailed points about multimode fiber cables:
Construction: Multimode fibers have a larger core diameter, typically 50 or 62.5 microns, compared to single-mode fibers, which have a core diameter of about 9 microns.
Light Propagation: The larger core of multimode fiber allows multiple light modes to propagate. These modes travel at different angles, leading to reflections off the core-cladding boundary.
Distance and Bandwidth: Due to modal dispersion, where different light modes arrive at the receiver at different times, multimode fibers are suited for shorter distance applications compared to single-mode fibers. Typical distances are up to 550 meters for 10 Gbps Ethernet using OM4 multimode fiber.
Applications: Multimode fibers are commonly used in LANs (Local Area Networks), data centers, and for shorter distance data transmission due to their cost-effectiveness and ease of installation.
Network

QUESTION 51
A network administrator performed upgrades on a server and installed a new NIC to improve performance. Following the upgrades, usera are unable to reach the server. Which of the following is the most likely reason.

A. The PoE power budget was exceeded.
B. TX/RX was transposed.
C. A port security violation occured.
D. An incorrect cable type was installed.

Correct Answer: D
Section:
Explanation:
When a network administrator installs a new Network Interface Card (NIC) and users are unable to reach the server, one of the common issues is the use of an incorrect cable type. Network cables must match the specifications required by the NIC and the network infrastructure (e.g., Cat5e, Cat6 for Ethernet).
NIC Compatibility: The new NIC might require a specific type of cable to function properly. Using a cable not rated for the NIC's required speeds or capabilities can result in connectivity issues.
Cable Standards: Different NICs and network devices might need different cabling standards (straight-through vs. crossover cables, or specific fiber optic types).
Connection Types: Ensuring that the cable connectors are appropriate for the NIC ports (e.g., RJ45 for Ethernet, LC connectors for fiber optics).
Network

QUESTION 52
Which of the following is a cost-effective advantage of a split-tunnel VPN?

A. Web traffic is filtered through a web filter.
B. More bandwidth is required on the company's internet connection.
C. Monitoring detects insecure machines on the company's network.
D. Cloud-based traffic flows outside of the company's network.

Correct Answer: D
Section:
Explanation:
A split-tunnel VPN allows some traffic to be routed through the VPN while other traffic goes directly to the internet. This setup offers several advantages, with a primary one being cost-effectiveness due to cloud-based traffic not consuming company bandwidth.
Bandwidth Utilization: Split-tunnel VPNs reduce the amount of traffic passing through the company's network, freeing up bandwidth for other uses.
Performance: By allowing internet-bound traffic to bypass the VPN, it can reduce latency and improve the performance for users accessing cloud services directly.
Cost Savings: Reduced load on the company's VPN infrastructure can lead to lower costs in terms of both hardware and bandwidth.
Network

QUESTION 53
A network technician needs to install patch cords from the UTP patch panel to the access switch for a newly occupied set of offices. The patch panel is not labeled for easy jack identification. Which of the following tools provides the easiest way to identify the appropriate patch panel port?

A. Toner
B. Laptop
C. Cable tester
D. Visual fault locator

Correct Answer: A
Section:
Explanation:
A toner probe, often referred to as a toner and probe kit, is the easiest and most effective tool for identifying individual cables in a bundle, especially in situations where the patch panel is not labeled. The toner sends an audible tone through the cable, and the probe detects the tone at the other end, allowing the technician to quickly identify the correct cable.
Functionality: The toner generates a tone that travels along the cable. When the probe is placed near the correct cable, it detects the tone and emits a sound.
Ease of Use: Toner probes are straightforward to use, even in environments with many cables, making them ideal for identifying cables in unlabeled patch panels.
Efficiency: This method is much faster and more reliable than manual tracing, especially in complex setups.
Network

QUESTION 54
A newtwork administrator needs to create an SVI on a Layer 3-capable device to separate voice and data traffic. Which of the following best explains this use case?

A. A physical interface used for trunking logical ports
B. A physical interface used for management access
C. A logical interface used for the routing of VLANs
D. A logical interface used when the number of physical ports is insufficent.

Correct Answer: C
Section:
Explanation:
An SVI (Switched Virtual Interface) is a logical interface on a Layer 3-capable switch used to route traffic between VLANs. This is particularly useful in environments where voice and data traffic need to be separated, as each type of traffic can be assigned to different VLANs and routed accordingly.
SVI (Switched Virtual Interface): A virtual interface created on a switch for inter-VLAN routing.
VLAN Routing: Enables the routing of traffic between VLANs on a Layer 3 switch, allowing for logical separation of different types of traffic, such as voice and data.
Use Case: Commonly used in scenarios where efficient and segmented traffic management is required, such as in VoIP implementations.
Network

QUESTION 55
A storage network requires reduced overhead and increased efficiency for the amout of data being sent. Which of the following should an engineer likely configure to meet these requirements>?

A. Link speed
B. Jumbo frames
C. QoS
D. 802.1q tagging

Correct Answer: B
Section:
Explanation:
Jumbo frames are Ethernet frames with a payload greater than the standard maximum transmission unit (MTU) of 1500 bytes. Configuring jumbo frames can reduce overhead and increase efficiency in storage networks by allowing more data to be sent in each frame, thus reducing the number of frames needed to transmit the same amount of data.
Reduced Overhead: By sending larger frames, the relative overhead for headers and acknowledgments is reduced.
Increased Efficiency: Larger frames mean fewer packets to process, leading to better utilization of network bandwidth and improved performance in high-throughput environments like storage networks.
Configuration: Requires support from all devices in the network path, including switches and network interface cards (NICs).
Network

QUESTION 56
A network administrator is in the process of installing 35 PoE security cameras. After the administrator installed and tested the new cables, the administrator installed the cameras. However, a small number of the cameras do not work. Which of the following is the most reason?

A. Incorrect wiring standard
B. Power budget exceeded
C. Signal attenuation
D. Wrong voltage

Correct Answer: B
Section:
Explanation:
When installing multiple Power over Ethernet (PoE) devices like security cameras, it is crucial to ensure that the total power requirement does not exceed the power budget of the PoE switch. Each PoE switch has a maximum power capacity, and exceeding this capacity can cause some devices to fail to receive power.
PoE Standards: PoE switches conform to standards such as IEEE 802.3af (PoE) and 802.3at (PoE+), each with specific power limits per port and total power capacity.
Power Calculation: Adding up the power requirements of all connected PoE devices can help determine if the total power budget of the switch is exceeded.
Symptoms: When the power budget is exceeded, some devices, typically those farthest from the switch or connected last, may not power up or function correctly.
Network

QUESTION 57
A company is hosting a secure that requires all connections to the server to be encrypted. A junior administrator needs to harded the web server. The following ports on the web server. The following ports on the web server are open:

443
80
22
587

Which of the following ports should be disabled?

A. 22

B. 80
C. 443
D. 587

Correct Answer: B
Section:
Explanation:
For a web server that requires all connections to be encrypted, port 80 (HTTP) should be disabled. Port 80 is used for unencrypted web traffic, whereas port 443 is used for HTTPS, which provides encrypted communication.
Port 80 (HTTP): This port is used for unsecured web traffic. Disabling this port ensures that all web traffic must use HTTPS, which encrypts the data in transit.
Port 443 (HTTPS): This port is used for secure web traffic via SSL/TLS encryption. Keeping this port open ensures that secure connections can be made to the web server.
Other Ports:
Port 22: Used for SSH, providing secure remote access and file transfers.
Port 587: Used for secure email submission (SMTP) with encryption.
Network

QUESTION 58
A network administrator is planning to implement device monitoring to enhance network visibility. The security that the solution provies authentication and encryption. Which of the following meets these requirements?

A. SIEM
B. Syslog
C. NetFlow
D. SNMPv3

Correct Answer: D
Section:
Explanation:
SNMPv3 (Simple Network Management Protocol version 3) provides device monitoring with authentication and encryption. This enhances network visibility and security by ensuring that monitoring data is securely transmitted and access to network devices is authenticated.
Authentication: SNMPv3 includes robust mechanisms for authenticating users accessing network devices.
Encryption: It provides encryption to protect the integrity and confidentiality of the data being transmitted.
Network Management: SNMPv3 allows for detailed monitoring and management of network devices, ensuring better control and security.
Network

QUESTION 59
A network administrator needs to change where the outside DNS records are hosted. Which of the following records should the administrator change the registrar to accomplish this task?

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

Correct Answer: A
Section:
Explanation:
To change where the outside DNS records are hosted, the network administrator needs to update the NS (Name Server) records at the domain registrar. NS records specify the authoritative name servers for a domain, directing where DNS queries should be sent.

NS (Name Server) Records: These records indicate the servers that are authoritative for a domain. Changing the NS records at the registrar points DNS resolution to the new hosting provider.
SOA (Start of Authority): Contains administrative information about the domain, including the primary name server.
PTR (Pointer) Records: Used for reverse DNS lookups, mapping IP addresses to domain names.
CNAME (Canonical Name) Records: Used to alias one domain name to another, not relevant for changing DNS hosting.
Network

QUESTION 60
Which of the following ports is used for secure email?

A. 25
B. 110
C. 143
D. 587

Correct Answer: D
Section:
Explanation:
Port 587 is used for secure email submission. This port is designated for message submission by mail clients to mail servers using the SMTP protocol, typically with STARTTLS for encryption.
Port 25: Traditionally used for SMTP relay, but not secure and often blocked by ISPs for outgoing mail due to spam concerns.
Port 110: Used for POP3 (Post Office Protocol version 3), not typically secured.
Port 143: Used for IMAP (Internet Message Access Protocol), which can be secured with STARTTLS or SSL/TLS.
Port 587: Specifically used for authenticated email submission (SMTP) with encryption, ensuring secure transmission of email from clients to servers.
Network

QUESTION 61
A company is implementing a wireless solution in a high-density environment. Which of the following 802.11 standards is used when a company is concerned about device saturation and converage?

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

Correct Answer: B
Section:
Explanation:
802.11ax, also known as Wi-Fi 6, is designed for high-density environments and improves device saturation and coverage compared to previous standards.
802.11ac: While it offers high throughput, it is not optimized for high-density environments as effectively as 802.11ax.
802.11ax (Wi-Fi 6): Introduces features like OFDMA, MU-MIMO, and BSS Coloring, which enhance performance in crowded environments, reduce latency, and increase the number of devices that can be connected simultaneously.
802.11g and 802.11n: Older standards that do not offer the same level of efficiency or support for high device density as 802.11ax.
Network
Reference:
CompTIA Network+ N10-007 Official Certification Guide: Covers the 802.11 standards and their capabilities.
Cisco Networking Academy: Provides training on Wi-Fi technologies and best practices for high-density deployments.

QUESTION 62
Which of the following appliances provides users with an extended footprint that allows connections from multiple devices within a designated WLAN?

A. Router
B. Switch
C. Access point
D. Firewall

Correct Answer: C
Section:
Explanation:
An access point (AP) provides users with an extended footprint that allows connections from multiple devices within a designated Wireless Local Area Network (WLAN).
Router: Typically used to connect different networks, not specifically for extending wireless coverage.
Switch: Used to connect devices within a wired network, not for providing wireless access.
Access Point (AP): Extends wireless network coverage, allowing multiple wireless devices to connect to the network.
Firewall: Primarily used for network security, controlling incoming and outgoing traffic based on security rules, not for providing wireless connectivity.
Network

QUESTION 63
Which of the following is an XML-based security concept that works by passing sensitve information about users, such as log-in information and attributes, to providers.

A. IAM
B. MFA
C. RADIUS
D. SAML

Correct Answer: D
Section:
Explanation:
Security Assertion Markup Language (SAML) is an XML-based standard used for exchanging authentication and authorization data between parties, particularly between an identity provider (IdP) and a service provider (SP).
SAML is commonly used in Single Sign-On (SSO) solutions to pass sensitive user information, such as login credentials and attributes, securely between the identity provider and the service provider.
SAML (Security Assertion Markup Language): Facilitates web-based authentication and authorization, allowing users to access multiple services with a single set of credentials.
XML-based: Uses XML to encode the authentication and authorization data, ensuring secure transmission of user information.
Identity Federation: Enables secure sharing of identity information across different security domains, making it ideal for enterprise SSO solutions.
Network

QUESTION 64
Which of the following facilities is the best example of a warm site in the event of information system disruption?

A. A combination of public and private cloud services to restore data
B. A partial infrastructure, software, and data on site
C. A full electrical infrastructure in place, but no customer devices on site
D. A full infrastructure in place, but no current data on site

Correct Answer: D
Section:
Explanation:
A warm site typically has a full infrastructure ready, but it lacks the most up-to-date data or is not immediately operational. It requires some configuration or data restoration to become fully functional.

QUESTION 65
Which of the following would be violated if an employee accidentally deleted a customer's data?

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

Correct Answer: D
Section:
Explanation:
Availability refers to ensuring that data is accessible when needed. If a customer's data is accidentally deleted, it impacts availability, as the data can no longer be accessed.

QUESTION 66
Which of the following is used to describe the average duration of an outage for a specific service?

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

Correct Answer: B
Section:
Explanation:
MTTR (Mean Time to Repair) is the average time it takes to repair a system or service after a failure. It helps in measuring the downtime and planning recovery processes.

QUESTION 67
A network consultant needs to decide between running an ethernet uplink or using the built-in 5GHz-to-point functionality on a WAP. Which of the following documents provides the best information to assist the consultant with this decision?

A. Site survey results
B. Physical diagram
C. Service-level agreement
D. Logical diagram

Correct Answer: A
Section:

QUESTION 68
An organizatin is struggling to get effective coverage using the wireless network. The organization wants to implement a solution that will allow for continous connectivity anywhere in the facility. Which of the following should the network administ rator suggest to ensure the best coverage?

A. Implementing additional ad hoc access points
B. Providing more Ethernet drops for user connections
C. Deploying a mesh network in the building
D. nl Changing the current frequency of the WI-FI

Correct Answer: C
Section:

QUESTION 69
A network engineer is completing a wireless installation in a new building. A requirement is that all clients be able to automatically connect to the fastest supported network. Which of the following best supports this requirement?

A. Enabling band steering
B. Disabling the 5GHz SSID
C. Adding a captive portal
D. Configuring MAC filtering

Correct Answer: A
Section:
Explanation:
Band Steering: This technology encourages capable devices to use the faster and less congested 5 GHz band. It ensures clients automatically connect to the most optimal frequency, enhancing speed and performance.
Disabling the 5GHz SSID (B): Prevents access to the fastest network, defeating the purpose.
Adding a captive portal (C): Captive portals control access but do not affect network speed.
Configuring MAC filtering (D): Restricts access but does not influence network selection.

QUESTION 70
A network engineer needs to virtualize network services, including a router at a remote branch location. Which of the following solutions meets the requirements?

A. NFV
B. VRF
C. VLAN
D. VPC

Correct Answer: A
Section:
Explanation:
Network Functions Virtualization (NFV): NFV is a technology that virtualizes network services like routing, firewalls, and load balancers. It allows these services to run on virtual machines rather than requiring dedicated hardware. This is ideal for remote branch locations where deploying physical devices is costly and complex.
VRF (B): Virtual Routing and Forwarding is used for segmenting routing tables but does not virtualize services.
VLAN (C): Virtual Local Area Networks help segregate broadcast domains but are unrelated to virtualizing network functions.
VPC (D): Virtual Private Cloud is used for cloud computing but does not pertain to virtualizing network services.