CompTIA

Exam Questions N10-009

CompTIA Network+ Exam

NEW QUESTION 1
- (Topic 3)
A company is moving to a new building designed with a guest waiting area that has existing network ports. Which of the following practices would BEST secure the network?

A. Ensure all guests sign an NDA.
B. Disable unneeded switchports in the area.
C. Lower the radio strength to reduce Wi-Fi coverage in the waiting area.
D. Enable MAC filtering to block unknown hardware addresses.

Answer: B

Explanation:
 One of the best practices to secure the network would be to disable unneeded switchports in the guest waiting area. This will prevent unauthorized users from connecting to the network through these ports. It's important to identify which switchports are not in use and disable them, as this will prevent unauthorized access to the network. Other practices such as ensuring all guests sign an NDA, lowering the radio strength to reduce Wi-Fi coverage in the waiting area and enabling MAC filtering to block unknown hardware addresses are not as effective in securing the network as disabling unneeded switchports. Enforcing an NDA with guests may not stop a malicious user from attempting to access the network, reducing the radio strength only limits the Wi-Fi coverage, and MAC filtering can be easily bypassed by hackers.

NEW QUESTION 2
- (Topic 3)
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

Answer: A

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. References: CompTIA Network+ N10-008 Certification Study Guide, page 371; The Official CompTIA Network+ Student Guide (Exam N10-008), page 14-5.

NEW QUESTION 3
- (Topic 3)
Which of the following DNS records maps an alias to a true name?

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

Answer: D

Explanation:
A CNAME (Canonical Name) record is a type of DNS (Domain Name System) record that maps an alias name to a canonical or true domain name. For example, a CNAME record can map blog.example.com to example.com, which means that blog.example.com is an alias of example.com. A CNAME record is useful when you want to point multiple subdomains to the same IP address, or when you want to change the IP address of a domain without affecting the subdomains1.

NEW QUESTION 4
- (Topic 3)
Due to space constraints in an IDF, a network administrator can only a do a single switch to
accommodate three data networks. The administrator needs a configuration that will allow each device to access its expected network without additional connections. The configuration must also allow each device to access the rest of the network. Which of the following should the administrator do to meet these requirements? (Select TWO).

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

Answer: AC

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

NEW QUESTION 5
- (Topic 3)
Which of the following best describe the functions of Layer 2 of the OSI model? (Select two).

A. Local addressing
B. Error preventing
C. Logical addressing
D. Error detecting
E. Port addressing
F. Error correcting

Answer: AD

Explanation:
Layer 2 of the OSI model, also known as the data link layer, is responsible for physical addressing and error detecting. Physical addressing refers to the use of MAC addresses to identify and locate devices on a network segment. Error detecting refers to the use of techniques such as checksums and CRCs to identify and correct errors in the data frames.
References:
? OSI Model | Computer Networking | CompTIA1

NEW QUESTION 6
- (Topic 3)
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

Answer: AC

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.

NEW QUESTION 7
- (Topic 3)
Which of the following options represents the participating computers in a network?

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

Answer: A

NEW QUESTION 8
- (Topic 3)
A technician is investigating packet loss to a device that has varying data bursts throughout the day. Which of the following will the technician MOST likely configure to resolve the issue?

A. Flow control
B. Jumbo frames
C. Duplex
D. Port mirroring

Answer: A

Explanation:
Ethernet flow control is a mechanism for temporarily stopping the transmission of data on Ethernet family computer networks. The goal of this mechanism is to avoid packet loss in the presence of network congestion.
Flow control is a mechanism that allows a device to regulate the amount of data it receives from another device, ensuring that the receiving device is not overwhelmed with data. If the device experiencing packet loss is receiving large bursts of data at times when it is not able to process it quickly enough, configuring flow control could help prevent packets from being lost.
"In theory, flow control can help with situations like a host that can't keep up with the flow of traffic. It enables the host to send an Ethernet PAUSE frame, which asks the switch to hold up for some amount of time so the host can catch its breath. If the switch can, it'll buffer transmissions until the pause expires, and then start sending again. If the host catches up early, it can send another PAUSE frame with a delay of zero to ask the switch to resume. In practice, flow control can cause latency trouble for modern real-time applications such as VoIP, and the same needs are usually met by QoS"

NEW QUESTION 9
- (Topic 3)
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

Answer: B

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.
References: [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.

NEW QUESTION 10
- (Topic 3)
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+

Answer: D

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.

NEW QUESTION 11
- (Topic 3)
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

Answer: C

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.
References
? 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

NEW QUESTION 12
- (Topic 3)
A divide-and-conquer approach is a troubleshooting method that involves breaking a complex problem into smaller and more manageable parts, and then testing each part to isolate the cause of the problem. In this scenario, the technician is using a divide-and- conquer approach by pinging the default gateway and DNS server of the workstation, which are two possible sources of connectivity issues. By pinging these devices, the technician can determine if the problem is related to the local network or the external network.
Which of the following most likely requires the use of subinterfaces?

A. A router with only one available LAN port
B. A firewall performing deep packet inspection
C. A hub utilizing jumbo frames
D. A switch using Spanning Tree Protocol

Answer: A

Explanation:

Subinterfaces are logical divisions of a physical interface that allow a router to communicate with multiple networks using a single LAN port. Subinterfaces can have different IP addresses, VLANs, and routing protocols. They are useful for reducing the number of physical interfaces and cables needed, as well as improving network performance and security.
References:
? Subinterfaces - CompTIA Network+ N10-008 Domain 1.21 - YouTube1

? CompTIA Network+ Certification Exam Objectives, page 92

NEW QUESTION 13
- (Topic 3)
A technician is configuring a wireless access point in a public space for guests to use. Which of the following should the technician configure so that only approved connections are
allowed?

A. Geofencing
B. Captive portal
C. Secure SNMP
D. Private VLANs

Answer: B

Explanation:

A captive portal is a web page that requires users to authenticate or accept terms of service before they can access the internet through a wireless access point. A captive portal can be used to control who can use the wireless network, limit the bandwidth or time of usage, or display advertisements or information. A captive portal is a common feature of public wireless networks, such as those in hotels, airports, cafes, or libraries. A captive portal can prevent unauthorized or malicious users from accessing the network or consuming network resources.
ReferencesPublic Wireless Access Points Definition | Law InsiderAre Public Wi-Fi Networks Safe? What You Need To Know

NEW QUESTION 14
- (Topic 3)
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

Answer: A

NEW QUESTION 15
- (Topic 3)
An organization has experienced an increase in malicious spear-phishing campaigns and wants to mitigate the risk of hyperlinks from inbound emails.
Which of the following appliances would best enable this capability?

A. Email protection gateway
B. DNS server
C. Proxy server
D. Endpoint email client
E. Sandbox

Answer: A

Explanation:
An email protection gateway is an appliance that can filter and block malicious emails and attachments before they reach the recipients. An email protection gateway can mitigate the risk of hyperlinks from inbound emails by scanning the links for malicious content, rewriting the links to point to a safe domain, or blocking the links altogether. An email protection gateway can also perform other functions such as spam filtering, antivirus scanning, encryption, and data loss prevention. A DNS server, a proxy server, an endpoint email client, and a sandbox are not appliances that can enable this capability, as they have different purposes and functions.
References
? 1: CompTIA Network+ N10-008 Certification Study Guide, page 304
? 2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 15
? 3: CompTIA Network+ N10-008 Certification Practice Test, question 5
? 4: Email Protection Gateway – N10-008 CompTIA Network+ : 3.2

NEW QUESTION 16
- (Topic 3)
A store owner would like to have secure wireless access available for both business equipment and patron use. Which of the following features should be configured to allow different wireless access through the same equipment?

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

Answer: D

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

NEW QUESTION 17
- (Topic 3)
Which of the following should be used to associate an IPv6 address with a domain name?

A. AAAA
B. A
C. SOA
D. TXT

Answer: A

Explanation:
An AAAA record is a type of DNS record that maps a domain name to an IPv6 address. It is similar to an A record, which maps a domain name to an IPv4 address, but it uses a 128-bit address instead of a 32-bit one. An AAAA record allows a domain name to be resolved by both IPv4 and IPv6 clients, and it is necessary for accessing websites and services that use IPv6.

NEW QUESTION 18
- (Topic 3)
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

Answer: B

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. References: [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.)

NEW QUESTION 19
- (Topic 3)
An ISP configured an internet connection to provide 20Mbps, but actual data rates are occurring at 10Mbps and causing a significant delay in data transmission. Which of the following specifications should the ISP check?

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

Answer: A

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

NEW QUESTION 20
- (Topic 3)
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

Answer: A

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.

NEW QUESTION 21
- (Topic 3)
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

Answer: B

NEW QUESTION 22
- (Topic 3)
While waking from the parking lot lo an access-controlled door an employee sees an authorized user open the door. Then the employee notices that another person catches the door before It closes and goes inside Which of the following attacks Is taking place?

A. Tailgating
B. Pipgybacking
C. Shoulder surfing
D. Phisning

Answer: A

Explanation:
 The difference between piggybacking and tailgaiting is that with piggybacking, the person is willfully and intentionally letting you in. In this particular case, the person caught the door before it closed, so it is tailgating.
Tailgating is a physical security attack that occurs when an unauthorized person follows an authorized person through a secured door or gate without their knowledge or consent. Tailgating can allow an attacker to bypass access control mechanisms and gain entry to restricted areas or resources. Tailgating can also pose a safety risk for the authorized person and other occupants of the facility.
Piggybacking is a physical security attack that occurs when an unauthorized person follows an authorized person through a secured door or gate with their knowledge or consent. Piggybacking can also allow an attacker to bypass access control mechanisms and gain entry to restricted areas or resources. Piggybacking can also violate security policies and compromise the accountability of the authorized person.
Shoulder surfing is a physical security attack that occurs when an unauthorized person observes or records an authorized person's confidential information, such as passwords, PINs, or credit card numbers. Shoulder surfing can allow an attacker to steal credentials and access sensitive data or systems. Shoulder surfing can also violate privacy and confidentiality rights of the authorized person.
Phishing is a cyber security attack that occurs when an unauthorized person sends fraudulent emails or messages that appear to come from legitimate sources, such as banks, companies, or government agencies. Phishing can trick recipients into clicking on malicious links, opening malicious attachments, or providing personal or financial information. Phishing can allow an attacker to install malware, steal credentials, or perform identity theft. Phishing does not involve physical access to secured doors or gates.

NEW QUESTION 23
- (Topic 1)
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

Answer: C

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.
References:
? 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.

NEW QUESTION 24
- (Topic 2)
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

Answer: B

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

NEW QUESTION 25
- (Topic 1)
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

Answer: D

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. References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 26
- (Topic 1)
Which of the following technologies provides a failover mechanism for the default gateway?

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

Answer: A

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

NEW QUESTION 27
- (Topic 1)
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

Answer: D

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.

NEW QUESTION 28
- (Topic 1)
A network administrator needs to query the NSs for a remote application. Which of the following commands would BEST help the administrator accomplish this task?

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

Answer: A

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

NEW QUESTION 29
- (Topic 1)
Access to a datacenter should be individually recorded by a card reader even when multiple employees enter the facility at the same time. Which of the following allows the enforcement of this policy?

A. Motion detection
B. Access control vestibules
C. Smart lockers
D. Cameras

Answer: B

Explanation:
The most effective security mechanism against physical intrusions due to stolen credentials would likely be a combination of several of these options. However, of the options provided, the most effective security mechanism would probably be an access control vestibule. An access control vestibule is a secure area that is

located between the outer perimeter of a facility and the inner secure area. It is designed to provide an additional layer of security by requiring that individuals pass through a series of security checks before being allowed access to the secure area. This could include biometric authentication, access card readers, and motion detection cameras.

Access control vestibules allow the enforcement of the policy that access to a datacenter should be individually recorded by a card reader even when multiple employees enter the facility at the same time. An access control vestibule is a physical security device that consists of two doors with an interlocking mechanism. Only one door can be opened at a time, and only one person can pass through each door. This prevents tailgating or piggybacking, where unauthorized persons follow authorized persons into a secure area. An access control vestibule can also be integrated with a card reader or other authentication system to record each individual's access. References: https://www.boonedam.us/blog/what-are-access-control-vestibules

NEW QUESTION 30
- (Topic 2)
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

Answer: B

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. References: https://www.comptia.org/blog/what-is-netstat

NEW QUESTION 31
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

N10-009 Practice Exam Features:

* N10-009 Questions and Answers Updated Frequently

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

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

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

100% Actual & Verified — Instant Download, Please Click
[Order The N10-009 Practice Test Here](https://www.surepassexam.com/N10-009-exam-dumps.html)