CompTIA

Exam Questions N10-009

CompTIA Network+ Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 1)
A company built a new building at its headquarters location. The new building is connected to the company's LAN via fiber-optic cable. Multiple users in the new building are unable to access the company's intranet site via their web browser, but they are able to access internet sites. Which of the following describes how the network administrator can resolve this issue?

A. Correct the DNS server entries in the DHCP scope
B. Correct the external firewall gateway address
C. Correct the NTP server settings on the clients
D. Correct a TFTP Issue on the company's server

Answer: A

Explanation:
If multiple users in a new building are unable to access the company's intranet site via their web browser but are able to access internet sites, the network administrator can resolve this issue by correcting the DNS server entries in the DHCP scope. The DHCP scope is responsible for assigning IP addresses and DNS server addresses to clients. If the DNS server entries are incorrect, clients will not be able to access intranet sites.
References:
> CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 4: Network Implementations, Objective 4.4: Explain the purpose and properties of DHCP.

NEW QUESTION 2
- (Exam Topic 1)
An administrator is writing a script to periodically log the IPv6 and MAC addresses of all the devices on a network segment. Which of the following switch features will MOST likely be used to assist with this task?

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

Answer: B

Explanation:
Short explanation
The switch feature that is most likely to be used to assist with logging IPv6 and MAC addresses of devices on a network segment is Neighbor Discovery Protocol (NDP). NDP is used by IPv6 to discover and maintain information about other nodes on the network, including their IPv6 and MAC addresses. By periodically querying NDP, the administrator can log this information for auditing purposes.
References:
> CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.1: Compare and contrast TCP and UDP ports, protocols, and their purposes.

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

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

Answer: B

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

NEW QUESTION 4
- (Exam Topic 1)
Wireless users are reporting intermittent internet connectivity. Connectivity is restored when the users disconnect and reconnect, utilizing the web authentication process each time. The network administrator can see the devices connected to the APs at all times. Which of the following steps will MOST likely determine the cause of the issue?

A. Verify the session time-out configuration on the captive portal settings
B. Check for encryption protocol mismatch on the client's wireless settings
C. Confirm that a valid passphrase is being used during the web authentication
D. Investigate for a client's disassociation caused by an evil twin AP

Answer: A

Explanation:
A captive portal is a web page that requires users to authenticate before they can access the internet. If the session time-out configuration is too short, users may experience intermittent internet connectivity and have to reconnect using the web authentication process each time. The network administrator can verify the session time-out configuration on the captive portal settings and adjust it if needed. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 1.0 Network Architecture, Objective 1.8 Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 5
- (Exam Topic 1)
Which of the following DNS records works as an alias to another record?

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

Answer: B

Explanation:
The DNS record that works as an alias to another record is called CNAME (Canonical Name). CNAME records are used to create an alias for a domain name that points to another domain name.
References:
> CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.3: Given a scenario, implement and configure the
appropriate addressing schema.

NEW QUESTION 6
- (Exam Topic 1)
A workstation is configured with the following network details:

IP address	Subnet mask	Default gateway
10.1.2.23	10.1.2.0/27	10.1.2.1

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

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

Answer: D

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

NEW QUESTION 7
- (Exam Topic 1)
The management team needs to ensure unnecessary modifications to the corporate network are not permitted and version control is maintained. Which of the following documents would BEST support this?

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

Answer: C

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

NEW QUESTION 8
- (Exam Topic 1)
A network engineer performs the following tasks to increase server bandwidth: Connects two network cables from the server to a switch stack
Configure LACP on the switchports
Verifies the correct configurations on the switch interfaces Which of the following needs to be configured on the server?

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

Answer: C

Explanation:
NIC teaming is a technique that combines two or more network interface cards (NICs) on a server into a single logical interface that can increase bandwidth, provide redundancy, and balance traffic. NIC teaming can be configured with different modes and algorithms depending on the desired outcome. Link Aggregation Control Protocol (LACP) is a protocol that enables NIC teaming by dynamically bundling multiple links between two devices into one logical link. References:

https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming/nic-teaming

NEW QUESTION 9
- (Exam Topic 1)
Given the following information:

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

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

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

Answer: D

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

NEW QUESTION 10
- (Exam Topic 1)
A network administrator is configuring a load balancer for two systems. Which of the following must the administrator configure to ensure connectivity during a failover?

A. VIP
B. NAT
C. APIPA
D. IPv6 tunneling
E. Broadcast IP

Answer: A

Explanation:
A virtual IP (VIP) address must be configured to ensure connectivity during a failover. A VIP address is a single IP address that is assigned to a group of servers or network devices. When one device fails, traffic is automatically rerouted to the remaining devices, and the VIP address is reassigned to the backup device, allowing clients to continue to access the service without interruption.
References:
- CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 6: Network Servers, p. 300

NEW QUESTION 10
- (Exam Topic 1)
Which of the following is used to track and document various types of known vulnerabilities?

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

Answer: A

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

NEW QUESTION 15
- (Exam Topic 1)
After the A record of a public website was updated, some visitors were unable to access the website. Which of the following should be adjusted to address the issue?

A. TTL
B. MX
C. TXT
D. SOA

Answer: A

Explanation:

TTL (Time To Live) should be adjusted to address the issue of some visitors being unable to access the website after the A record was updated. TTL is a value that specifies how long a DNS record should be cached by DNS servers and clients before it expires and needs to be refreshed. If the TTL is too high, some DNS servers and clients may still use the old A record that points to the previous IP address of the website, resulting in connection failures. By lowering the TTL, the DNS servers and clients will update their cache more frequently and use the new A record that points to the current IP address of the website. References: https://www.cloudflare.com/learning/dns/dns-records/dns-ttl/

NEW QUESTION 19
- (Exam Topic 1)
Which of the following transceiver types can support up to 40Gbps?

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

Answer: B

Explanation:
QSFP+ is a transceiver type that can support up to 40Gbps. It stands for Quad Small Form-factor Pluggable Plus and uses four lanes of data to achieve high-speed transmission. It is commonly used for data center and high-performance computing applications. References: https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-6600

NEW QUESTION 23
- (Exam 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 25
- (Exam Topic 1)
A technician is searching for a device that is connected to the network and has the device’s physical network address. Which of the following should the technician review on the switch to locate the device’s network port?

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

Answer: C

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

NEW QUESTION 30
- (Exam Topic 1)
A technician is deploying a new switch model and would like to add it to the existing network monitoring software. The technician wants to know what metrics can be gathered from a given switch. Which of the following should the technician utilize for the switch?

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

Answer: A

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

NEW QUESTION 32
- (Exam Topic 1)
A client recently added 100 users who are using VMs. All users have since reported slow or unresponsive desktops. Reports show minimal network congestion,

zero packet loss, and acceptable packet delay. Which of the following metrics will MOST accurately show the underlying performance issues? (Choose two.)

A. CPU usage
B. Memory
C. Temperature
D. Bandwidth
E. Latency
F. Jitter

Answer: AB

NEW QUESTION 33
- (Exam Topic 1)
An engineer is configuring redundant network links between switches. Which of the following should the engineer enable to prevent network stability issues?

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

Answer: B

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

NEW QUESTION 36
- (Exam Topic 1)
Which of the following is the physical topology for an Ethernet LAN?

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

Answer: D

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

NEW QUESTION 37
- (Exam Topic 1)
A user reports being unable to access network resources after making some changes in the office. Which of the following should a network technician do FIRST?

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

Answer: D

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

NEW QUESTION 41
- (Exam Topic 1)
A technician is assisting a user who cannot connect to a network resource. The technician first checks for a link light. According to troubleshooting methodology, this is an example of:

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

Answer: A

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

NEW QUESTION 42
- (Exam Topic 1)
Which of the following BEST describes a network appliance that warns of unapproved devices that are accessing the network?

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

Answer: D

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

NEW QUESTION 46
- (Exam Topic 1)
Which of the following would MOST likely be used to review previous upgrades to a system?

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

Answer: B

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

NEW QUESTION 48
- (Exam Topic 1)
The following configuration is applied to a DHCP server connected to a VPN concentrator:

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

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

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

Answer: A

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

NEW QUESTION 52
- (Exam Topic 1)
A network technician is manually configuring the network settings for a new device and is told the network block is 192.168.0.0/20. Which of the following subnets should the technician use?

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

Answer: C

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

NEW QUESTION 57
- (Exam Topic 1)

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

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

Answer: A

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

NEW QUESTION 59
- (Exam Topic 2)
A network engineer is designing a new secure wireless network. The engineer has been given the following requirements:
* 1 Must not use plaintext passwords
* 2 Must be certificate based
* 3. Must be vendor neutral
Which of the following methods should the engineer select?

A. TWP-RC4
B. CCMP-AES
C. EAP-TLS
D. WPA2

Answer: C

Explanation:
EAP-TLS is the method that should be selected to meet the requirements for designing a new secure wireless network. EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) is an authentication protocol that uses X.509 digital certificates for both clients and servers. It provides strong security and mutual authentication by using TLS encryption and public key cryptography. It does not use plaintext passwords or shared secrets that can be compromised or guessed. It is also an open standard that is vendor neutral and supported by most wireless devices1. References: https://www.securew2.com/blog/what-is-eap-tls 1

NEW QUESTION 62
- (Exam Topic 2)
A corporation has a critical system that would cause unrecoverable damage to the brand if it was taken offline. Which of the following disaster recovery solutions should the corporation implement?

A. Full backups
B. Load balancing
C. Hot site
D. Snapshots

Answer: C

Explanation:
A hot site is the disaster recovery solution that the corporation should implement for its critical system that would cause unrecoverable damage to the brand if it was taken offline. A hot site is a fully operational backup site that can take over the primary site’s functions in case of a disaster or disruption. A hot site has all the necessary hardware, software, data, network connections, and personnel to resume normal operations with minimal downtime. A hot site is suitable for systems that require high availability and cannot afford any data loss or interruption. References: https://www.enterprisestorageforum.com/management/disaster-recovery-site/ 1

NEW QUESTION 64
- (Exam Topic 2)
Which of the following is used to provide networking capability for VMs at Layer 2 of the OSI model?

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

Answer: C

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

NEW QUESTION 69
- (Exam Topic 2)
There are two managed legacy switches running that cannot be replaced or upgraded. These switches do not support cryptographic functions, but they are password protected. Which of the following should a network administrator configure to BEST prevent unauthorized access?

A. Enable a management access list
B. Disable access to unnecessary services.

C. Configure a stronger password for access
D. Disable access to remote management
E. Use an out-of-band access method.

Answer: E

Explanation:
Using an out-of-band access method is the best way to prevent unauthorized access to the legacy switches that do not support cryptographic functions. Out-of-band access is a method of accessing a network device through a dedicated channel that is separate from the main network traffic. Out-of-band access can use physical connections such as serial console ports or dial-up modems, or logical connections such as VPNs or firewalls. Out-of-band access provides more security and reliability than in-band access, which uses the same network as the data traffic and may be vulnerable to attacks or failures. References:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15mt/fundamentals-15-mt-book/

NEW QUESTION 70
- (Exam Topic 2)
Which of the following protocol types describes secure communication on port 443?

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

Answer: C

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

NEW QUESTION 74
- (Exam Topic 2)
An organization wants to implement a method of centrally managing logins to network services. Which of the following protocols should the organization use to allow for authentication, authorization and auditing?

A. MS-CHAP
B. RADIUS
C. LDAPS
D. RSTP

Answer: B

Explanation:
RADIUS (Remote Authentication Dial-In User Service) is a protocol that should be used by the organization to allow for authentication, authorization, and auditing of network services. RADIUS is an AAA (Authentication, Authorization, and Accounting) protocol that manages network access by verifying user credentials, granting access permissions, and logging user activities. RADIUS uses a client-server model where a RADIUS client (such as a router, switch, or VPN server) sends user information to a RADIUS server (such as an authentication server) for verification and authorization. The RADIUS server can also send accounting information to another server for billing or reporting purposes. References:
https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838

NEW QUESTION 78
- (Exam Topic 2)
A user reports a weak signal when walking 20ft (61 m) away from the WAP in one direction, but a strong signal when walking 20ft in the opposite direction The technician has reviewed the configuration and confirmed the channel type is correct There is no jitter or latency on the connection Which of the following would be the MOST likely cause of the issue?

A. Antenna type
B. Power levels
C. Frequency
D. Encryption type

Answer: A

Explanation:
The antenna type affects the signal strength and coverage of a WAP. Different types of antennas have different radiation patterns and gain, which determine how far and wide the signal can reach. If the user experiences a weak signal in one direction but a strong signal in the opposite direction, it could mean that the antenna type is not suitable for the desired coverage area. The technician should consider changing the antenna type to one that has a more balanced or directional radiation pattern. References:
https://community.cisco.com/t5/wireless-small-business/wap200-poor-signal-strength/td-p/1565796

NEW QUESTION 81
- (Exam Topic 2)
A network technician is investigating an issue with a desktop that is not connecting to the network. The desktop was connecting successfully the previous day, and no changes were made to the environment. The technician locates the switchport where the device is connected and observes the LED status light on the switchport is not lit even though the desktop is turned on Other devices that arc plugged into the switch are connecting to the network successfully Which of the following is MOST likely the cause of the desktop not connecting?

A. Transceiver mismatch

B. VLAN mismatch
C. Port security
D. Damaged cable
E. Duplex mismatch

Answer: D

Explanation:
A damaged cable is most likely the cause of the desktop not connecting to the network. A damaged cable can cause physical layer issues such as loss of signal, attenuation, interference, or crosstalk. These issues can prevent the desktop from establishing a link with the switch and result in the LED status light on the switchport being off. Other possible causes of physical layer issues are faulty connectors, ports, or transceivers. References: https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/14119-37.html

NEW QUESTION 83
- (Exam Topic 2)
Given the following output:

```
192.168.22.1     00-13-5d-00-c6-23
192.168.22.15    00-15-88-00-58-00
192.168.22.10    00-13-5d-00-c6-23
192.168.22.100   00-13-5d-00-c6-23
```

Which of the following attacks is this MOST likely an example of?

A. ARP poisoning
B. VLAN hopping
C. Rogue access point
D. Amplified DoS

Answer: A

Explanation:
The output is most likely an example of an ARP poisoning attack. ARP poisoning, also known as ARP spoofing, is a type of attack that exploits the ARP protocol to associate a malicious device's MAC address with a legitimate IP address on a local area network. This allows the attacker to intercept, modify, or redirect network traffic between two devices without their knowledge. The output shows that there are multiple entries for the same IP address (192.168.1.1) with different MAC addresses in the ARP cache of the device. This indicates that an attacker has sent fake ARP replies to trick the device into believing that its MAC address is associated with the IP address of another device (such as the default gateway). References: https://www.cisco.com/c/en/us/about/security-center/arp-spoofing.html

NEW QUESTION 88
- (Exam Topic 2)
An IDS was installed behind the edge firewall after a network was breached. The network was then breached again even though the IDS logged the attack. Which of the following should be used in place of these devices to prevent future attacks?

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

Answer: C

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

NEW QUESTION 89
- (Exam Topic 2)
Which of the following technologies allows traffic to be sent through two different ISPs to increase performance?

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

Answer: C

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

NEW QUESTION 93
- (Exam Topic 2)
A technician is deploying a low-density wireless network and is contending with multiple types of building materials. Which of the following wireless frequencies would allow for the LEAST signal attenuation?

A. 2.4GHz
B. 5GHz
C. 850MHz
D. 900MHZ

Answer: A

Explanation:
* 2.4 GHz is the wireless frequency that would allow for the least signal attenuation when deploying a low-density wireless network with multiple types of building materials. Signal attenuation is the loss of signal strength or quality as it travels through a medium or over a distance. Signal attenuation can be affected by various factors such as distance, interference, reflection, refraction, diffraction, scattering, or absorption. Generally, lower frequencies have less signal attenuation than higher frequencies because they can penetrate obstacles better and travel farther. Therefore, 2.4GHz would have less signal attenuation than 5GHz, 850MHz, or 900MHz. References: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html

NEW QUESTION 96
- (Exam 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 99
- (Exam Topic 2)
A user recently made changes to a PC that caused it to be unable to access websites by both FQDN and IP Local resources, such as the file server remain accessible. Which of the following settings did the user MOST likely misconfigure?

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

Answer: B

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

NEW QUESTION 103
- (Exam Topic 2)
Which of the following would be used to expedite MX record updates to authoritative NSs?

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

Answer: D

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

NEW QUESTION 106
- (Exam Topic 2)
A network administrator is setting up several loT devices on a new VLAN and wants to accomplish the following
* 1. Reduce manual configuration on each system
* 2. Assign a specific IP address to each system
* 3. Allow devices to move to different switchports on the same VLAN
Which of the following should the network administrator do to accomplish these requirements?

A. Set up a reservation for each device
B. Configure a static IP on each device

C. Implement private VLANs for each device
D. Use DHCP exclusions to address each device

Answer: A

Explanation:
A reservation is a feature of DHCP that assigns a specific IP address to a device based on its MAC address. This way, the device will always receive the same IP address from the DHCP server, regardless of its location or connection time. A network administrator can set up a reservation for each loT device to accomplish the requirements of reducing manual configuration, assigning a specific IP address, and allowing devices to move to different switchports on the same VLAN.
References: https://www.comptia.org/blog/what-is-dhcp

NEW QUESTION 108
- (Exam Topic 3)
A network technician needs to ensure the company's external mail server can pass reverse lookup checks. Which of the following records would the technician MOST likely configure? (Choose Correct option and give explanation directly from CompTIA Network+ Study guide or documents)

A. PTR
B. AAAA
C. SPF
D. CNAME

Answer: A

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

NEW QUESTION 113
- (Exam Topic 3)
A technician is checking network devices to look for opportunities to improve security Which of the following toots would BEST accomplish this task?

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

Answer: B

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

NEW QUESTION 114
- (Exam Topic 3)
A non-employee was able to enter a server room. Which of the following could have prevented this from happening?

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

Answer: B

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

NEW QUESTION 119
- (Exam Topic 3)
A large number of PCs are obtaining an APIPA IP address, and a number of new computers were added to the network. Which of the following is MOST likely causing the PCs to obtain an APIPA address?

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

Answer: D

Explanation:

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

NEW QUESTION 123
- (Exam Topic 3)
A systems operator is granted access to a monitoring application, configuration application, and timekeeping application. The operator is denied access to the financial and project management applications by the system's security configuration. Which of the following BEST describes the security principle in use?

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

Answer: D

NEW QUESTION 126
- (Exam Topic 3)
A network manager is configuring switches in IDFs to ensure unauthorized client computers are not connecting to a secure wired network. Which of the following is the network manager MOST likely performing?

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

Answer: C

NEW QUESTION 130
- (Exam Topic 3)
An administrator is attempting to add a new system to monitoring but is unsuccessful. The administrator notices the system is similar to another one on the network; however, the new one has an updated OS version. Which of the following should the administrator consider updating?

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

Answer: A

NEW QUESTION 131
- (Exam Topic 3)
Due to a surge in business, a company is onboarding an unusually high number of salespeople. The salespeople are assigned desktops that are wired to the network. The last few salespeople to be onboarded are able to access corporate materials on the network but not sales-specific resources. Which of the following is MOST likely the cause?

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

Answer: D

NEW QUESTION 132
- (Exam Topic 3)
Which of the following is the MOST cost-effective alternative that provides proper cabling and supports gigabit Ethernet devices?

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

Answer: A

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

NEW QUESTION 134
- (Exam Topic 3)
An engineer is gathering data to determine the effectiveness of UPSs in use at remote retail locations. Which of the following statistics can the engineer use to determine the availability of the remote network equipment?

A. Uptime

B. NetFlow baseline
C. SNMP traps
D. Interface statistics

Answer: A

Explanation:
Uptime is a statistic that can be used to determine the availability of the remote network equipment. Uptime is the amount of time that a device or system has been running without experiencing any failures or disruptions. It is commonly expressed as a percentage of total time, such as 99.99% uptime. By measuring the uptime of the network equipment at the remote retail locations, the engineer can determine how reliable and available the equipment is.

NEW QUESTION 136
- (Exam Topic 3)
A network administrator would like to purchase a device that provides access ports to endpoints and has the ability to route between networks. Which of the following would be BEST for the administrator to purchase?

A. An IPS
B. A Layer 3 switch
C. A router
D. A wireless LAN controller

Answer: B

NEW QUESTION 141
- (Exam Topic 3)
A network technician is implementing a solution that will allow end users to gain access to multiple applications after logging on. Which of the following authentication methods would allow this type of access?

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

Answer: A

NEW QUESTION 143
- (Exam Topic 3)
An administrator is setting up a multicast server on a network, but the firewall seems to be dropping the traffic. After logging in to the device, me administrator sees me following entries:

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

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

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

Answer: A

NEW QUESTION 145
- (Exam Topic 3)
Which of the following allows for an devices within a network to share a highly reliable time source?

A. NTP
B. SNMP
C. SIP
D. DNS

Answer: A

Explanation:
Network Time Protocol (NTP) is a protocol used to maintain a highly accurate and reliable clock time on all devices within a network. NTP works by synchronizing the time of all the devices within a network to a single, highly accurate time source. This allows for the time of all the devices to be kept in sync with each other, ensuring a consistent and reliable time source for all devices within the network.

NEW QUESTION 150
- (Exam 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 153
- (Exam Topic 3)
A technician knows the MAC address of a device and is attempting to find the device's IP address. Which of the following should the technician look at to find the IP address? (Select TWO).

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

Answer: BE

NEW QUESTION 158
- (Exam Topic 3)
Which of the following is used to provide disaster recovery capabilities to spin up an critical devices using internet resources?

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

Answer: A

NEW QUESTION 160
- (Exam Topic 3)
A network technician receives a report about a performance issue on a client PC that is connected to port 1/3 on a network switch. The technician observes the following configuration output from the switch:

1/1	Client PC	Connected	Full	1000
1/2	Client PC	Connected	Full	1000
1/3	Client PC	Connected	Full	10

Which of the following is a cause of the issue on port 1/3?

A. Speed
B. Duplex
C. Errors
D. VLAN

Answer: A

NEW QUESTION 162
- (Exam Topic 3)
An IT technician needs to increase bandwidth to a server. The server has multiple gigabit ports. Which of the following can be used to accomplish this without replacing hardware?

A. STP
B. 802. IQ
C. Duplex
D. LACP

Answer: D

Explanation:
LACP stands for Link Aggregation Control Protocol and is a protocol that allows multiple physical ports to be combined into a single logical port. This can increase bandwidth, redundancy, and load balancing for a server. LACP is part of the IEEE 802.3ad standard for link aggregation. STP stands for Spanning Tree Protocol and is a protocol that prevents loops in a network by blocking redundant links. 802.1Q is a standard for VLAN (Virtual Local Area Network) tagging, which allows multiple logical networks to share the same physical infrastructure. Duplex is a mode of communication that determines how data is transmitted and received on a link. Full duplex allows simultaneous transmission and reception, while half duplex allows only one direction at a time.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.5: Compare and contrast network cabling types, standards and speeds.

NEW QUESTION 164
- (Exam Topic 3)
Which of the following protocols is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links?

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

Answer: A

NEW QUESTION 168
- (Exam Topic 3)
A network technician is selecting a replacement for a damaged fiber cable that goes directly to an SFP transceiver on a network switch. Which of the following cable connectors should be used?

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

Answer: C

NEW QUESTION 169
- (Exam Topic 3)
A large metropolitan city is looking to standardize the ability tor police department laptops to connect to the city government's VPN The city would like a wireless solution that provides the largest coverage across the city with a minimal number of transmission towers Latency and overall bandwidth needs are not high priorities. Which of the following would BEST meet the city's needs?

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

Answer: B

NEW QUESTION 171
- (Exam Topic 3)
A network technician is attempting to increase throughput by configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch. Which of the following is the BEST choice concerning speed and duplex for all interfaces that are participating in the link aggregation?

A. Half duplex and 1GB speed
B. Full duplex and 1GB speed
C. Half duplex and 10OMB speed
D. Full duplex and 100MB speed

Answer: B

Explanation:
The best choice for configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch is to use full duplex and 1GB speed for all interfaces that are participating in the link aggregation. This will allow for maximum throughput, as the full duplex connection will enable simultaneous sending and receiving of data, and the 1GB speed will ensure that the data is transferred quickly.
According to the CompTIA Network+ Study Guide, “Full-duplex Ethernet allows the network adapter to transmit and receive data simultaneously, which can result in double the bandwidth of half-duplex Ethernet.” Additionally, the official text states, “Ethernet and Fast Ethernet use different speeds for data transmission, with Ethernet being 1,000 megabits (1 gigabit) per second and Fast Ethernet being 100 megabits per second.”

NEW QUESTION 173
- (Exam Topic 3)
Which of the following layers of the OSI model receives data from the application layer and converts it into syntax that is readable by other devices on the network?

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

Answer: C

NEW QUESTION 175
- (Exam Topic 3)
A network technician is having issues connecting an IoT sensor to the internet The WLAN settings were enabled via a custom command line, and a proper IP address assignment was received on the wireless interlace. However, when trying to connect to the internet, only HTTP redirections are being received when data Is requested. Which of the following will point to the root cause of the Issue?

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

Answer: C

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

NEW QUESTION 180
- (Exam Topic 3)

A network administrator wants to test the throughput of a new metro Ethernet circuit to verify that its performance matches the requirements specified m the SLA. Which of the following would BEST help measure the throughput?

A. iPerf
B. Ping
C. NetFlow
D. Netstat

Answer: A

NEW QUESTION 184
- (Exam 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 188
- (Exam Topic 3)
A switch is connected to another switch. Incompatible hardware causes a surge in traffic on both switches. Which of the following configurations will cause traffic to pause, allowing the switches to drain buffers?

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

Answer: B

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

NEW QUESTION 192
- (Exam Topic 3)
After rebooting an AP a user is no longer able to conned to me enterprise LAN A technician plugs a laptop In to the same network jack and receives the IP 169.254 0 200. Which of the following is MOST likely causing the issue?

A. DHCP scope exhaustion
B. Signal attenuation
C. Channel overlap
D. Improper DNS configuration

Answer: A

Explanation:
DHCP scope exhaustion occurs when the number of available IP addresses to be leased from a DHCP server have been used up. This could be caused by a large number of clients on the network, or a misconfigured DHCP scope. When this happens, clients will be assigned an IP address from the APIPA range (169.254.0.0 to 169.254.255.255). To resolve this issue, the DHCP scope needs to be expanded or adjusted to accommodate the number of clients on the network.

NEW QUESTION 194

- (Exam Topic 3)
A new office space is being designed. The network switches are up. but no services are running yet A network engineer plugs in a laptop configured as a DHCP client to a switch Which ol the following IP addresses should be assigned to the laptop?

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

Answer: B

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

NEW QUESTION 198
- (Exam Topic 3)
An engineer needs to verity the external record tor SMTP traffic. The engineer logged in to the server and entered the nslookup command. Which of the following commands should the engineer send before entering the DNS name?

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

Answer: D

NEW QUESTION 203
- (Exam Topic 3)
Which of the following should be used to manage outside cables that need to be routed to various multimode uplinks?

A. Fiber distribution panel
B. 110 punchdown block
C. PDU
D. TIA/EIA-568A patch bay
E. Cat 6 patch panel

Answer: A

Explanation:
A fiber distribution panel is a device that provides a central location for connecting and managing fiber optic cables and optical modules. It can support various types and speeds of fiber optic links, including multimode uplinks. Therefore, a fiber distribution panel should be used to manage outside cables that need to be routed to various multimode uplinks.

NEW QUESTION 208
- (Exam Topic 3)
A new student is given credentials to log on to the campus Wi-Fi. The student stores the password in a laptop and is able to connect; however, the student is not able to connect with a phone when only a short distance from the laptop. Given the following information:

Signal strength	90%
Coverage	80%
Interference	15%
Number of connection attempts	10

Which of the following is MOST likely causing this connection failure?

A. Transmission speed
B. Incorrect passphrase
C. Channel overlap
D. Antenna cable attenuation/signal loss

Answer: B

NEW QUESTION 209
- (Exam Topic 3)
A technician is configuring a static IP address on a new device in a newly created subnet. The work order specifies the following requirements:
• The IP address should use the highest address available in the subnet.
• The default gateway needs to be set to 172.28.85.94.
• The subnet mask needs to be 255.255.255.224.
Which of the following addresses should the engineer apply to the device?

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

Answer: A

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

NEW QUESTION 210
- (Exam Topic 3)
Which of the following physical security methods Is the MOST effective to prevent tailgating?

A. Biometrics in an access control vestibule
B. IP cameras with motion detection
C. Smart lockers with tamper protection
D. Badge readers plus a PIN pad

Answer: A

Explanation:
Biometrics is a type of authentication that uses a person's physical characteristics, such as fingerprints, iris, or face, to verify their identity. An access control vestibule is a small room or area that separates two spaces and allows only one person to enter or exit at a time. Biometrics in an access control vestibule is the most effective physical security method to prevent tailgating, which is the unauthorized entry of a person behind another person who has legitimate access.
References: Network+ Study Guide Objective 5.1: Summarize the importance of physical security controls.

NEW QUESTION 213
- (Exam Topic 3)
A network engineer receives the following when connecting to a switch to configure a port:

```
telnet 10.1.200.1
Connecting to 10.1.200.1...Could not open connection to the host, on port 23: Connect failed.
```

Which of the following is the MOST likely cause for the failure?

A. The network engineer is using the wrong protocol
B. The network engineer does not have permission to configure the device
C. SNMP has been secured with an ACL
D. The switchport the engineer is trying to configure is down

Answer: D

NEW QUESTION 218
- (Exam Topic 3)
A client who shares office space and an IT closet with another company recently reported connectivity issues throughout the network. Multiple third-party vendors regularly perform on-site maintenance in the shared IT closet. Which of the following security techniques would BEST secure the physical networking equipment?

A. Disabling unneeded switchports
B. Implementing role-based access
C. Changing the default passwords
D. Configuring an access control list

Answer: B

Explanation:
Role-based access is a security technique that assigns permissions and privileges to users or groups based on their roles or functions within an organization. Role-based access can help secure the physical networking equipment by limiting who can access, modify, or manage the devices in the shared IT closet. Only authorized personnel with a valid role and credentials should be able to access the networking equipment. Disabling unneeded switchports is a security technique that prevents unauthorized devices from connecting to the network by turning off unused ports on a switch. Changing the default passwords is a security technique that prevents unauthorized access to network devices by replacing the factory-set passwords with strong and unique ones. Configuring an access control list is a security technique that filters network traffic by allowing or denying packets based on criteria such as source and destination IP addresses, ports, or protocols.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.2: Given a scenario, use appropriate network hardening techniques.

NEW QUESTION 219
- (Exam Topic 3)
Which of the following types of attacks can be used to gain credentials by setting up rogue APs with identical corporate SSIDs?

A. VLAN hopping
B. Evil twin
C. DNS poisoning
D. Social engineering

Answer: B

NEW QUESTION 222
- (Exam Topic 3)
A consultant is working with two international companies. The companies will be sharing cloud resources for a project. Which of the following documents would provide an agreement on how to utilize the resources?

A. MOU

B. NDA
C. AUP
D. SLA

Answer: A

Explanation:
A memorandum of understanding (MOU) is a document that describes an agreement between two or more parties on how to utilize shared resources for a project. An MOU is not legally binding, but it outlines the expectations and responsibilities of each party involved in the collaboration. An MOU can be used when two international companies want to share cloud resources for a project without creating a formal contract. References: https://www.comptia.org/training/books/network-n10-008-study-guide (page 405)

NEW QUESTION 225
- (Exam Topic 3)
A PC user who is on a local network reports very slow speeds when accessing files on the network server The user's PC Is connecting, but file downloads are very slow when compared to other users' download speeds The PC's NIC should be capable of Gigabit Ethernet. Which of the following will MOST likely fix the issue?

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

Answer: B

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

NEW QUESTION 227
- (Exam Topic 3)
A technician is troubleshooting reports that a networked printer is unavailable. The printer's IP address is configured with a DHCP reservation, but the address cannot be pinged from the print server in the same subnet. Which of the following is MOST likely the cause of me connectivity failure?

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

Answer: D

NEW QUESTION 231
- (Exam Topic 3)
Which of the following would be increased by adding encryption to data communication across the network?

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

Answer: D

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

NEW QUESTION 233
- (Exam Topic 3)
A company's primary ISP is experiencing an outage. However, the network administrator notices traffic continuing to flow through a secondary connection to the same ISP. Which of the following BEST describes this configuration?

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

Answer: A

NEW QUESTION 236
- (Exam Topic 3)
A false camera is installed outside a building to assist with physical security. Which of the following is the device assisting?

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

Answer: A

NEW QUESTION 241
- (Exam Topic 3)
Which of the following is MOST appropriate for enforcing bandwidth limits when the performance of an application is not affected by the use of buffering but is heavily impacted by packet drops?

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

Answer: B

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

NEW QUESTION 246
- (Exam Topic 3)
A technician is configuring a wireless network and needs to ensure users agree to an AUP before connecting. Which of the following should be implemented to achieve this goal?

A. Captive portal
B. Geofencing
C. Wireless client isolation
D. Role-based access

Answer: A

NEW QUESTION 248
- (Exam Topic 3)
Which of the following is a requirement when certifying a network cabling as Cat 7?

A. Ensure the patch panel is certified for the same category.
B. Limit 10Gb transmissions to 180ft (55m).
C. Use F-type connectors on the network terminations.
D. Ensure the termination standard is TIA/EIA-568-A.

Answer: D

Explanation:
Category 7 (Cat 7) is a cabling standard that supports 10GBASE-T Ethernet connections up to 100 meters (328 feet). In order for a cabling system to be certified as Cat 7, all components, including the patch panel, must meet the TIA/EIA-568-A standard. This standard requires the use of shielded cables with F-type connectors for the network terminations. Reference: CompTIA Network+ Study Manual, 8th Edition, page 158.

NEW QUESTION 251
- (Exam Topic 3)
A network resource was accessed by an outsider as a result of a successful phishing campaign. Which of the following strategies should be employed to mitigate the effects of phishing?

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

Answer: A

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

NEW QUESTION 255
- (Exam Topic 3)
A security engineer is trying to determine whether an internal server was accessed by hosts on the internet. The internal server was shut down during the investigation Which of the following will the engineer review to determine whether the internal server had an unauthorized access attempt?

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

Answer: A

NEW QUESTION 257
- (Exam Topic 3)
Which of the following uses the link-state routing algorithm and operates within a single autonomous system?

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

Answer: B

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

NEW QUESTION 262
- (Exam Topic 3)
Which of the following would be used when connecting devices that have different physical characteristics?

A. A proxy server
B. An industrial control system
C. A load balancer
D. A media converter

Answer: D

NEW QUESTION 264
- (Exam Topic 3)
A technician is equipped with a tablet, a smartphone, and a laptop to troubleshoot a switch with the help of support over the phone. However, the technician is having issues interconnecting all these tools in troubleshooting the switch. Which Of the following should the technician use to gain connectivity?

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

Answer: A

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

NEW QUESTION 268
- (Exam Topic 3)
A network administrator is troubleshooting a connectivity performance issue. As part of the troubleshooting process, the administrator performs a traceout from the client to the server, and also from the server to the client. While comparing the outputs, the administrator notes they show different hops between the hosts. Which of the following BEST explains these findings?

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

Answer: C

NEW QUESTION 269
- (Exam Topic 3)
Which of the following will reduce routing table lookups by performing packet forwarding decisions independently of the network layer header?

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

Answer: A

Explanation:
Multiprotocol Label Switching, or MPLS, is a networking technology that routes traffic using the shortest path based on “labels,” rather than network addresses, to

handle forwarding over private wide area networks. As a scalable and protocol-independent solution, MPLS assigns labels to each data packet, controlling the path the packet follows. MPLS greatly improves the speed of traffic, so users don’t experience downtime when connected to the network.

NEW QUESTION 270
- (Exam Topic 3)
Which of the following would be used to enforce and schedule critical updates with supervisory approval and include backup plans in case of failure?

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

Answer: A

NEW QUESTION 273
- (Exam Topic 3)
An organization is interested in purchasing a backup solution that supports the organization's goals. Which of the following concepts would specify the maximum duration that a given service can be down before impacting operations?

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

Answer: B

Explanation:
The maximum duration that a given service can be down before it impacts operations is often referred to as the Recovery Time Objective (RTO). RTO is a key consideration in any backup and disaster recovery plan, as it determines how quickly the organization needs to be able to recover from a disruption or failure. It is typically expressed in terms of time, and it helps to inform the design and implementation of the backup solution. For example, if an organization has a critical service that must be available 24/7, it may have a very low RTO, requiring that the service be restored within a matter of minutes or even seconds. On the other hand, if the service can be down for a longer period of time without significantly impacting operations, the organization may have a higher RTO. When selecting a backup solution, it is important to consider the organization's RTO requirements and ensure that the solution is capable of meeting those needs. A solution that does not meet the organization's RTO requirements may not be sufficient to ensure the availability of critical services in the event of a disruption or failure.

NEW QUESTION 276
- (Exam Topic 3)
A newly installed multifunction copier needs to be set up so scanned documents can be emailed to recipients. Which of the following ports from the copier's IP address should be allowed?

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

Answer: B

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

NEW QUESTION 278
- (Exam Topic 3)
Which of the following describes traffic going in and out of a data center from the internet?

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

Answer: B

NEW QUESTION 279
- (Exam Topic 3)
An IT administrator received an assignment with the following objectives
• Conduct a total scan within the company's network tor all connected hosts
• Detect all the types of operating systems running on all devices
• Discover all services offered by hosts on the network
• Find open ports and detect security risks.
Which of the following command-line tools can be used to achieve these objectives?

A. nmap
B. arp
C. netatat
D. tcpdump

Answer: A

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

NEW QUESTION 284
- (Exam Topic 3)
A network administrator is given the network 80.87.78.0/26 for specific device assignments. Which of the following describes this network?

A. 80.87.78 0 - 80.87.78.14
B. 80.87.78 0 - 80.87.78.110
C. 80.87.78 1 - 80.87.78.62
D. 80.87.78.1 - 80.87.78.158

Answer: C

Explanation:
The network 80.87.78.0/26 is a Class A network with a subnet mask of /26, which means that it contains 26 bits of network information and 6 bits of host information. The range of valid host addresses for this network is 80.87.78.1 to 80.87.78.62. Any addresses outside of this range are reserved for special purposes or are not used.

NEW QUESTION 285
- (Exam Topic 3)
Which of the following can be used to store various types of devices and provide contactless delivery to users?

A. Asset tags
B. Biometrics
C. Access control vestibules
D. Smart lockers

Answer: C

NEW QUESTION 288
- (Exam Topic 3)
A network engineer needs to reduce the overhead of file transfers. Which of the following configuration changes would accomplish that goal?

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

Answer: A

NEW QUESTION 289
- (Exam Topic 3)
A technician is consolidating a topology with multiple SSlDs into one unique SSiD deployment. Which of the following features will be possible after this new configuration?

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

Answer: A

NEW QUESTION 294
- (Exam Topic 3)
An engineer recently decided to upgrade the firmware on a router. During the upgrade, the help desk received calls about a network outage, and a critical ticket was opened. The network manager would like to create a policy to prevent this from happening in the future. Which of the following documents should the manager create?

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

Answer: A

NEW QUESTION 295
- (Exam Topic 3)
A company wants to set up a backup data center that can become active during a disaster. The site needs to contain network equipment and connectivity. Which of the following strategies should the company employ?

A. Active-active
B. Warm
C. Cold
D. Cloud

Answer: B

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

NEW QUESTION 298
- (Exam Topic 3)
Network traffic is being compromised by DNS poisoning every time a company's router is connected to the internet. The network team detects a non-authorized DNS server being assigned to the network clients and remediates the incident by setting a trusted DNS server, but the issue occurs again after internet exposure. Which of the following best practices should be implemented on the router?

A. Change the device's default password.
B. Disable router advertisement guard.
C. Activate control plane policing.
D. Disable unneeded network services.

Answer: A

NEW QUESTION 303
- (Exam Topic 3)
A malicious user is using special software 10 perform an on-path attack. Which of the following best practices should be configured to mitigate this threat?

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

Answer: A

NEW QUESTION 306
- (Exam Topic 3)
A technician uses a badge to enter a security checkpoint on a corporate campus. An unknown individual quickly walks in behind the technician without speaking. Which of the following types of attacks did the technician experience?

A. Tailgating
B. Evil twin
C. On-path
D. Piggybacking

Answer: A

Explanation:
Tailgating is a type of physical security attack where an unauthorized person follows an authorized person into a restricted area without their consent or knowledge. Tailgating can allow an attacker to bypass security measures and gain access to sensitive information or resources. In this scenario, the technician experienced tailgating when the unknown individual walked in behind the technician without speaking. Piggybacking is similar to tailgating, but it involves the consent or cooperation of the authorized person. Evil twin is a type of wireless network attack where an attacker sets up a rogue access point that mimics a legitimate one. On-path is a type of network attack where an attacker intercepts and modifies traffic between two parties.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.2: Given a scenario, use appropriate network hardening techniques.

NEW QUESTION 311
- (Exam Topic 3)
A network administrator needs to monitor traffic on a specific port on a switch. Which of the following should the administrator configure to accomplish the task?

A. Port security
B. Port tagging
C. Port mirroring
D. Media access control

Answer: C

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

NEW QUESTION 313

- (Exam Topic 3)
Classification using labels according to information sensitivity and impact in case of unauthorized access or leakage is a mandatory component of:

A. an acceptable use policy.
B. a memorandum of understanding.
C. data loss prevention,
D. a non-disclosure agreement.

Answer: C

Explanation:
Data loss prevention (DLP) is a set of tools and processes that aim to prevent unauthorized access or leakage of sensitive information. One of the components of DLP is data classification, which involves labeling data according to its information sensitivity and impact in case of unauthorized disclosure. Data classification helps to identify and protect the most critical and confidential data and apply appropriate security controls and policies. References: Network+ Study Guide Objective 5.1: Explain the importance of policies, processes and procedures for IT governance. Subobjective: Data loss prevention.

NEW QUESTION 315
- (Exam Topic 3)
Which of the following protocols can be used to change device configurations via encrypted and authenticated sessions? (Select TWO).

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

Answer: BD

NEW QUESTION 316
- (Exam Topic 3)
A WAN technician reviews activity and identifies newly installed hardware that is causing outages over an eight-hour period. Which of the following should be considered FIRST?

A. Network performance baselines
B. VLAN assignments
C. Routing table
D. Device configuration review

Answer: D

NEW QUESTION 321
- (Exam Topic 3)
A network engineer is designing a wireless network that has the following requirements:
• Network speed must be higher than 100Mbps
• Must use the 2.4GHz and 5GHz bands
Which of the following 802.11 standards should the engineer select?

A. 802. lla
B. 802.11b
C. 802. 11g
D. 802.11 n

Answer: D

Explanation:
* 802.11 n is a wireless standard that supports up to 600 Mbps data rate and operates in both the 2.4 GHz and 5 GHz frequency bands. 802.11n uses multiple-input multiple-output (MIMO) technology to increase the number of spatial streams and improve the wireless performance and range. 802.11n meets the requirements of the wireless network design.
References: Network+ Study Guide Objective 1.6: Explain the functions of network services.

NEW QUESTION 323
- (Exam Topic 3)
A technician removes an old PC from the network and replaces it with a new PC that is unable to connect to the LAN. Which of the Mowing is MOST likely the cause of the issue?

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

Answer: A

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

NEW QUESTION 327
- (Exam Topic 3)
A corporate client is experiencing global system outages. The IT team has identified multiple potential underlying causes throughout the enterprise Each team member has been assigned an area to trouble shoot. Which of the following approaches is being used?

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

Answer: A

NEW QUESTION 332
- (Exam Topic 3)
An office area contains two PoE-enabled WAPs. After the area was remodeled, new cable uplinks were installed in the ceiling above the fluorescent lights. However, after the WAPs were reconnected, users reported slowness and application errors. An intern reviewed the network and discovered a lot of CRC errors. A network engineer reviewed the intern's work and realized UTP cabling was used. Which of the following is the MOST likely cause of the CRC errors?

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

Answer: C

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

NEW QUESTION 333
- (Exam Topic 3)
A technician is deploying a new SSID for an industrial control system. The control devices require the network to use encryption that employs TKIP and a symmetrical password to connect. Which of the following should the technician configure to ensure compatibility with the control devices?

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

Answer: C

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

NEW QUESTION 336
- (Exam Topic 3)
Users are reporting poor wireless performance in some areas of an industrial plant The wireless controller is measuring a tow EIRP value compared to me recommendations noted on me most recent site survey. Which of the following should be verified or replaced for the EIRP value to meet the site survey's specifications? (Select TWO).

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

Answer: AE

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

NEW QUESTION 341
- (Exam Topic 3)
A company is deploying a SAN at headquarters and a branch office 1, 000ml (1,609km) away that w« access small amounts of data. Which of the following types

of connections would be MOST cost effective to implement?

A. ISCSI
B. FCoE
C. Ethernet
D. FC

Answer: A

Explanation:
Mike Meyers
"Internet Small Computer Systems Interface (iSCSI) is built on top of TCP/IP, enabling devices that use the SCSI protocol to communicate across existing networks using cheap, readily available hardware."
Jason Dion "iSCSI (IP Small Computer System Interface)
- Lower cost, built using Ethernet switches (<10 Gbps)
- Relies on configuration allowing jumbo frames over the network"

NEW QUESTION 345
- (Exam Topic 3)
A network administrator is decommissioning a server. Which of the following will the network administrator MOST likely consult?

A. Onboarding and off boarding policies
B. Business continuity plan
C. Password requirements
D. Change management documentation

Answer: D

NEW QUESTION 346
- (Exam Topic 3)
A network team is getting reports that air conditioning is out in an IDF. The team would like to determine whether additional network issues are occurring. Which of the following should the network team do?

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

Answer: D

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

NEW QUESTION 349
- (Exam Topic 3)
While setting up a new workstation, a technician discovers that the network connection is only 100 full duplex (FD), although it is connected to a gigabit switch. While reviewing the interface information in the switch CLI, the technician notes the port is operating at IOOFD but Shows many RX and TX errors. The technician moves the computer to another switchport and experiences the same issues.
Which of the following is MOST likely the cause of the low data rate and port errors?

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

Answer: B

NEW QUESTION 351
- (Exam Topic 3)
A network administrator requires redundant routers on the network, but only one default gateway is configurable on a workstation. Which of the following will allow for redundant routers with a single IP address?

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

Answer: B

Explanation:
Virtual Router Redundancy Protocol (VRRP) is a protocol that allows for redundant routers on the network with a single IP address. VRRP works by creating a virtual router that consists of one master router and one or more backup routers. The virtual router has its own IP address and MAC address that are shared among the routers in the group. The master router responds to traffic sent to the virtual router's IP address, while the backup routers monitor the master router's

status. If the master router fails, one of the backup routers takes over as the new master router and continues to respond to traffic. This way, VRRP provides high availability and fault tolerance for the network. References:
https://www.comptia.org/training/books/network-n10-008-study-guide (page 230)

NEW QUESTION 356
- (Exam Topic 3)
A user reports that a crucial fileshare is unreachable following a network upgrade that was completed the night before. A network technician confirms the problem exists. Which of the following
troubleshooting Steps should the network technician perform NEXT?

A. Establish a theory of probable cause.
B. Implement a solution to fix the problem.
C. Create a plan of action to resolve the problem.
D. Document the problem and the solution.

Answer: A

Explanation:
s for the problem and testing them to verify or eliminate them. In this scenario, the network technician has confirmed the problem exists and should proceed to establish a theory of probable cause based on the information available, such as the network upgrade that was completed the night before.
Implementing a solution to fix the problem is the fifth step in the general troubleshooting process, after establishing a plan of action. Implementing a solution involves applying the chosen method or technique to resolve the problem and verifying its effectiveness. In this scenario, the network technician has not established a plan of action yet and should not implement a solution without knowing the cause of the problem.
Creating a plan of action to resolve the problem is the fourth step in the general troubleshooting process, after establishing a theory of probable cause. Creating a plan of action involves selecting the best method or technique to address the problem based on the available resources, constraints, and risks. In this scenario, the network technician has not established a theory of probable cause yet and should not create a plan of action without knowing the cause of the problem.
Documenting the problem and the solution is the seventh and final step in the general troubleshooting process, after implementing preventive measures. Documenting the problem and the solution involves recording the details of the problem, its symptoms, its cause, its solution, and its preventive measures for future reference and improvement. In this scenario, the network technician has not implemented preventive measures yet and should not document the problem and the solution without resolving and preventing it.

NEW QUESTION 360
- (Exam Topic 3)
A WAN technician reviews activity and identifies newly installed hardware that is causing outages over an eight-hour period. Which of the following should be considered FIRST?

A. Network performance baselines
B. VLAN assignments
C. Routing table
D. Device configuration review

Answer: D

Explanation:
The most likely cause of outages due to newly installed hardware is a misconfiguration of the device settings. Therefore, the first step should be to review the device configuration and check for any errors or inconsistencies that might affect the WAN connectivity.
References: Network+ Study Guide Objective 2.1: Explain the importance of network documentation.

NEW QUESTION 362
- (Exam Topic 3)
A network administrator is reviewing the following metrics from a network management system regarding a switchport. The administrator suspects an issue because users are calling in regards to the switchport's performance:

Metric	Value
Uptime	201 days, 3 hours, 18 minutes
MDIX	On
CRCs	0
Giants	2508
Output queue maximum	40
Packets input	136208849
Packets output	64458087024

Based on the information in the chart above, which of the following fs the cause of these performance issues?

A. The connected device is exceeding the configured MTU.
B. The connected device is sending too many packets
C. The switchport has been up for too long
D. The connected device is receiving too many packets.
E. The switchport does not have enough CRCs

Answer: A

NEW QUESTION 364
- (Exam Topic 3)
Which of the following attacks, if successful, would provide a malicious user who is connected to an isolated guest network access to the corporate network?

A. VLAN hopping
B. On-path attack
C. IP spoofing

D. Evil twin

Answer: A

Explanation:
The attack which, if successful, would provide a malicious user who is connected to an isolated guest network access to the corporate network is VLAN hopping. VLAN hopping is an attack technique which involves tricking a switch into sending traffic from one VLAN to another. This is done by sending specially crafted packets, which force the switch to send traffic from one VLAN to another, thus allowing the malicious user to gain access to the corporate network.
VLAN hopping is an attack technique which involves tricking a switch into sending traffic from one VLAN to another. This is done by sending specially crafted packets, which force the switch to send traffic from one VLAN to another, thus allowing the malicious user to gain access to the corporate network. According to the CompTIA Network+ N10-008 Exam Guide VLAN hopping is a type of attack that is used to gain access to network resources that are not meant to be accessible by a user on a guest network.

NEW QUESTION 366
- (Exam Topic 3)
A Fortune 500 firm is deciding On the kind or data center equipment to install given its five-year budget Outlook. The Chief Information comparing equipment based on the life expectancy Of different models.
Which Of the following concepts BEST represents this metric?

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

Answer: A

NEW QUESTION 370
- (Exam Topic 3)
Which of the following can be used to centrally manage credentials for various types of administrative privileges on configured network devices?

A. SSO
B. TACACS+
C. Zero Trust
D. Separation of duties
E. Multifactor authentication

Answer: B

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

NEW QUESTION 375
- (Exam Topic 3)
A store owner would like to have secure wireless access available for both business equipment and patron use. Which of the following features should be configured to allow different wireless access through the same equipment?

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

Answer: D

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

NEW QUESTION 378
- (Exam Topic 3)
Which of the following connectors and terminations are required to make a Cat 6 cable that connects from a PC to a non-capable MDIX switch? (Select TWO).

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

Answer: AD

NEW QUESTION 383

- (Exam Topic 3)
A technician is investigating why a PC cannot reach a file server with the IP address 192.168.8.129. Given the following TCP/IP network configuration:

Link-local IPv6 address	fe80::28e4:a7cc:a55e:4bea
IPv4 address	192.168.8.105
Subnet mask	255.255.255.128
Default gateway	192.168.8.1

Which of the following configurations on the PC is incorrect?

A. Subnet mask
B. IPv4 address
C. Default gateway
D. IPv6 address

Answer: C

Explanation:
The default gateway is the IP address of the router that connects the PC to other networks. The default gateway should be on the same subnet as the PC's IPv4 address. However, in this case, the default gateway is 192.168.9.1, which is on a different subnet than the PC's IPv4 address of 192.168.8.15. Therefore, the default gateway configuration on the PC is incorrect and prevents the PC from reaching the file server on another subnet.

NEW QUESTION 388
- (Exam Topic 3)
A network administrator is investigating a performance issue on a dual-link connection—VPN and MPLS—to a partner network. The MPLS is the primary path, and the VPN is used as a backup. While communicating, the delay is measured at 18ms, which is higher than the 6ms expected when the MPLS link is operational but lower than the 30ms expected tor the VPN connection. Which of the following will MOST likely point to the root cause of the Issue?

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

Answer: A

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

NEW QUESTION 392
- (Exam Topic 3)
A network attack caused a network outage by wiping the configuration and logs of the border firewall. Which of the following sources, in an investigation to determine how the firewall was compromised, can provide the MOST detailed data?

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

Answer: A

NEW QUESTION 395
- (Exam Topic 3)
A technician is trying to install a VoIP phone, but the phone is not turning on. The technician checks the cable gong from the phone to the switch, and the cable is good. Which of the following actions IS needed for this phone to work?

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

Answer: A

NEW QUESTION 399
- (Exam Topic 3)
A network administrator is preparing answers for an annual risk assessment that is required for compliance purposes. Which of the following would be an example of an internal threat?

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

Answer: A

Explanation:

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

NEW QUESTION 402
- (Exam Topic 3)
Which of the Mowing architectures reduces network latency by enforcing a limit on the number of switching devices on the frame's path between any internal hosts?

A. Spine and leaf
B. Software-defined network
C. Three-tiered
D. Collapsed core

Answer: A

Explanation:
It does this by using a two-level hierarchy of switches, where the spine switches connect to the leaf switches, which in turn connect to the end hosts. This reduces the number of hops a packet must take from one host to another, thus reducing latency. According to the CompTIA Network+ N10-008 Exam Guide, the Spine and Leaf topology is a modern architecture that is used to reduce latency in large networks.

NEW QUESTION 406
- (Exam Topic 3)
A network engineer is monitoring a fiber uplink to a remote office and notes the uplink has been operating at 100% capacity for a long duration. Which of the following performance metrics is MOST likely to be impacted with sustained link saturation?

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

Answer: A

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

NEW QUESTION 408
- (Exam Topic 3)
Users in a branch can access an In-house database server, but II is taking too long to fetch records. The analyst does not know whether the Issue is being caused by network latency. Which of the following will the analyst MOST likely use to retrieve the metrics that are needed to resolve this issue?

A. SNMP
B. Link state
C. Syslog
D. QoS
E. Traffic shaping

Answer: A

NEW QUESTION 410
.....

Relate Links

100% Pass Your N10-009 Exam with Exambible Prep Materials

https://www.exambible.com/N10-009-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/