

CompTIA.N10-008.v2024-11-29.q972

Exam Code:	N10-008
Exam Name:	CompTIA Network+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	972
Version:	v2024-11-29
# of views:	4844
# of Questions views:	9720
https://www.exam-tests.com/N10-008-exam/CompTIA.N10-008.v2024-11-29.q972.html	

NEW QUESTION: 1

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

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

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

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

Answer: C,D (LEAVE A REPLY)

Explanation

The packet shown in the image is an SNMP (Simple Network Management Protocol) packet, which is used to monitor and manage network devices. SNMP uses community strings to authenticate requests and responses between SNMP agents and managers. However, community strings are sent in clear text and can be easily intercepted by attackers. Therefore, one way to secure SNMP traffic is to set a private community string that is not the default or well-known value. Another way to secure SNMP traffic is to use SNMPv3, which is the latest version of the protocol that supports encryption and authentication of SNMP messages.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.5: Given a scenario, use remote access methods.

NEW QUESTION: 2

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 ([LEAVE A REPLY](#))

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: 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 ([LEAVE A REPLY](#))

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: 4

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 ([LEAVE A REPLY](#))

SSID (Service Set Identifier) is a feature that should be configured to allow different wireless access through the same equipment. SSID is the name of a wireless network that identifies it from other networks in the same area. A wireless access point (AP) can support multiple SSIDs with different security settings and network policies. For example, a store owner can create one SSID for business equipment and another SSID for patron use, and assign different passwords, VLANs, and QoS levels for each SSID. Reference:

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70931-multiple-ssid.html>

NEW QUESTION: 5

A network manager is configuring switches in IDF's 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. Writing ACLs to prevent access to the switch
- C. Configuring DHCP snooping
- D. Changing the default VLAN

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 6

A network administrator is installing a new server in the datacenter. The administrator is concerned the amount of traffic generated will exceed 1GB, and higher- throughput NICs are not available for installation. Which of the following is the BEST solution for this issue?

- A. Install an additional NIC and configure LACP.
- B. Remove some of the applications from the server.
- C. Configure the NIC to use full duplex
- D. Configure port mirroring to send traffic to another server.
- E. Install a SSD to decrease data processing time.

Answer: ([SHOW ANSWER](#))

Link Aggregation is the combining of multiple network connections in parallel by any of several methods, in order to increase throughput.

NEW QUESTION: 7

A desktop support department has observed slow wireless speeds for a new line of laptops using the organization's standard image. No other devices have experienced the same issue. Which of the following should the network administrator recommend troubleshooting FIRST to resolve this issue?

- A. Increasing wireless signal power
- B. Updating the device wireless drivers
- C. Changing the protocol associated to the SSID
- D. Installing a new WAP

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 8

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

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

Answer: C (LEAVE A REPLY)

The question asks about the least amount of equipment to segment two departments that have cables terminating in the same room.

Segmentation is the process of dividing a network into smaller logical units for security, performance, or management purposes.

One way to segment a network is by using VLANs (virtual LANs), which are logical groups of devices that share the same broadcast domain, regardless of their physical location or connection.

VLANs can be configured on switches that support Layer 2 or Layer 3 functionality. Layer 2 switches operate at the data link layer and forward frames based on MAC addresses. Layer 3 switches operate at the network layer and forward packets based on IP addresses.

A Layer 3 switch can perform both Layer 2 and Layer 3 functions, and can also route traffic between different VLANs without the need for an external router. This makes it a versatile and efficient device for network segmentation.

Therefore, the answer is C, a Layer 3 switch, as it can segment two departments with the least amount of equipment.

Reference:

CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Devices and Technologies, Section 2.1: Network Devices, Pages 74-75 Professor Messer's CompTIA N10-008 Network+ Course, Video 2.1: Network Devices, Part 1 Network + N10-008 practice exam, Question 977, Answer C, Explanation

NEW QUESTION: 9

A network administrator is getting reports of some internal users who cannot connect to network resources. The users state they were able to connect last week, but not today. No changes have been configured on the network devices or server during the last few weeks. Which of the following is the MOST likely cause of the issue?

- A. The client DHCP scope is fully utilized
- B. The wired network is experiencing electrical interference
- C. The captive portal is down and needs to be restarted
- D. SNMP traps are being received
- E. The packet counter on the router interface is high.

Answer: A (LEAVE A REPLY)

A DHCP scope is a range of IP addresses that a DHCP server can assign to clients on a network.

If the DHCP scope is fully utilized, it means that there are no more available IP addresses to assign to new clients.

This can cause some internal users who cannot connect to network resources, as they will not have a valid IP address to communicate with other devices on the network.

The users may have been able to connect last week, but not today, because their previous IP address lease may have expired and they could not renew it due to the lack of available IP addresses.

The other options are less likely to cause the issue, because:

B . Electrical interference can affect the quality of the wired network, but it will not prevent users from obtaining an IP address.

C . A captive portal is a web page that requires users to authenticate or accept terms of service before accessing the network. If the captive portal is down, it may prevent users from accessing the internet, but not the internal network resources.

D . SNMP traps are messages sent by SNMP agents to SNMP managers to notify them of events or conditions on the network. They do not affect the connectivity of the users, unless they trigger some network management actions that block or limit the traffic.

E . The packet counter on the router interface is a metric that shows how many packets have been sent or received on that interface. It does not indicate any problem with the network connectivity, unless it reaches a threshold that causes the interface to drop packets.

Reference:

1: CompTIA Network+ N10-008 Study Guide, Chapter 3: IP Addressing, page 104

2: Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 3.2: DHCP, page 27

3: CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Cabling and Topologies, page 69

4: Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 4.1: Network Services, page 36

5: CompTIA Network+ N10-008 Study Guide, Chapter 7: Network Management, page 276

6: Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 7.1: Network Monitoring, page 66

NEW QUESTION: 10

A network security technician is designing a solution for a secure remote access scheme with the following requirements:

- * The solution must allow for users at multiple locations to access corporate resources.
- * The on-premises equipment will not handle non-corporate, resource-bound traffic.

Which of the following should the network security technician consider when designing the solution? (Select two).

- A.** Clientless VPN
- B.** Personal VPN
- C.** Full-tunnel VPN
- D.** Client-to-site VPN
- E.** Site-to-site VPN
- F.** Split-tunnel VPN

Answer: D,F (LEAVE A REPLY)

A client-to-site VPN and a split-tunnel VPN are the best options for designing a secure remote access scheme that meets the given requirements. A client-to-site VPN allows users at multiple locations to access corporate resources over the internet by creating a secure tunnel between their devices and a VPN concentrator on the corporate network¹. A split-tunnel VPN allows the on-premises equipment to handle only the traffic that is

destined for the corporate resources, while the non-corporate traffic is routed directly to the internet without passing through the VPN tunnel². This reduces the bandwidth and processing load on the corporate network and improves the performance of the remote access.

Reference:

Remote Access - N10-008 CompTIA Network+ : 4.41

comptia Network+ : Remote Access Methods And Network Monitoring²

NEW QUESTION: 11

A technician just validated a theory that resolved a network outage. The technician then verified that all users could access resources. Which of the following is the next step the technician should take in the network troubleshooting methodology?

- A. Verify the services are restored.
- B. Test a new theory.
- C. Write the lessons learned.
- D. Identify where the network outage is occurring.

Answer: C (LEAVE A REPLY)

The network troubleshooting methodology is a systematic process of identifying and resolving network problems. It consists of eight steps:

1. Identify the problem.
2. Establish a theory of probable cause.
3. Test the theory to determine the cause.
4. Establish a plan of action to resolve the problem and identify potential effects.
5. Implement the solution or escalate as necessary.
6. Verify full system functionality and, if applicable, implement preventive measures.
7. Document findings, actions, and outcomes.
8. Write the lessons learned.

The last step, writing the lessons learned, is important for improving the network troubleshooting skills and knowledge. It involves reviewing the entire troubleshooting process, analyzing the root cause of the problem, evaluating the effectiveness of the solution, and identifying any best practices, tips, or tools that can be used for future reference. Writing the lessons learned can also help to update the network documentation, policies, and procedures, and share the experience and feedback with other network professionals

NEW QUESTION: 12

Which of the following would be BEST suited for use at the access layer in a three-tier architecture system?

- A. Router
- B. Multilayer switch
- C. Layer 2 switch
- D. Access point

Answer: (SHOW ANSWER)

Explanation

A layer 2 switch is a device that forwards traffic based on MAC addresses within a single network segment or VLAN. A layer 2 switch is best suited for use at the access layer in a three-tier architecture system. The access layer is the layer that connects end devices such as computers, printers, and phones to the network. A layer 2 switch can provide fast and efficient switching for end devices without adding complexity or overhead to the network. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 139)

NEW QUESTION: 13

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: (SHOW ANSWER)

Traffic policing is the 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. Traffic policing is used to enforce predetermined data rate limits by discarding excess traffic that is sent beyond the set limit. Traffic shaping is used to manage the rate of data flow by buffering traffic that exceeds the set limits, while traffic marking is used to identify and differentiate traffic according to its type or priority. Traffic classification is used to identify different types of network traffic and assign them to different classes for different levels of treatment.

NEW QUESTION: 14

A network administrator is troubleshooting the communication between two Layer 2 switches that are reporting a very high runt count. After trying multiple ports on both switches, the issue persists. Which of the following should the network administrator perform to resolve the issue?

- A. Increase the MTU size on both switches.
- B. Recertify the cable between both switches.
- C. Perform a factory reset on both switches.
- D. Enable debug logging on both switches.

Answer: (SHOW ANSWER)

In the past, collisions (which were eliminated with full-duplex Ethernet decades ago) were likely causes of runts. Nowadays, bad wiring and electrical interference are leading causes of runts.

NEW QUESTION: 15

While troubleshooting a network outage, a technician discovers symptoms that indicate a patch cable is connecting the core switch to the router. A network engineer confirms the theory is plausible, and the technician tests the cable. The cable passes the test, and the technician properly plugs the cable back into the correct network ports. However, the network outage continues. Which of the following is the NEXT step the technician should take to troubleshoot the network outage?

- A. Establish a new theory.
- B. Establish a plan of action.

- C. Continue to work the original theory.
- D. Verify full system functionality.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 16

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: (SHOW ANSWER)

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.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 17

The following DHCP scope was configured for a new VLAN dedicated to a large deployment of 325 IoT sensors:

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

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

- A. Check the IoT devices for a hardware failure.

- B. Check whether the NTP server is online.
- C. Check the DHCP network scope.
- D. Check the gateway connectivity to the TFTP server.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 18

A technician is working on a ticket for a user in the human resources department who received a new PC that does not connect to the internet. All users in human resources can access the internet. The technician can ping the PC from the human resources router but not from the IT network. Which of the following is the most likely cause of the issue?

- A. Duplicate IP address
- B. Misconfigured RIP
- C. Improper VLAN assignment
- D. Incorrect default gateway

Answer: ([SHOW ANSWER](#)**)**

An incorrect default gateway can cause a PC to not connect to the internet, because the default gateway is the device that routes traffic from the local network to other networks. If the PC has a wrong default gateway configured, it may not be able to reach the internet router or the IT network router. The technician can ping the PC from the human resources router because they are on the same local network, but not from the IT network router because they are on different networks.

A duplicate IP address can cause a PC to not communicate with other devices on the same network, because the IP address is the unique identifier of a device on a network. If two devices have the same IP address, they may cause IP conflicts and packet loss. However, a duplicate IP address would not prevent the technician from pinging the PC from the human resources router, because they are on the same network.

A misconfigured RIP can cause a router to not learn or advertise routes to other networks, because RIP is a routing protocol that dynamically exchanges routing information between routers. If a router has a wrong RIP configuration, it may not be able to reach or share routes with other routers. However, a misconfigured RIP would not affect the PC's connectivity to the internet, because the PC does not use RIP.

An improper VLAN assignment can cause a PC to not communicate with other devices on the same or different networks, because a VLAN is a logical segmentation of a network that isolates traffic based on criteria such as function, security, or performance. If a PC is assigned to a wrong VLAN, it may not be able to access the resources or services that it needs. However, an improper VLAN assignment would not prevent the technician from pinging the PC from the human resources router, because they are on the same physical network.

Reference

What is a Default Gateway?

What's an IP Conflict and How Do You Resolve It?

What is RIP (Routing Information Protocol)?

What is a VLAN? How to Set Up a VLAN Network

CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION: 19

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, the administrator sees the 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: B (LEAVE A REPLY)

The firewall rules are set to deny any traffic from any source to specific destination IP addresses on any port. The destination IP addresses are in different ranges, but one of them is in the multicast range of 224.0.0.0 to 239.255.255.255.

The multicast range is used to send data to multiple recipients at once, such as streaming video or audio.

The multicast server on the network is likely using an IP address in the multicast range to broadcast its data to the clients.

Therefore, the firewall rule that is most likely causing the issue is the one that denies any traffic to the IP address 232.1.4.9, which is in the multicast range.

The other rules are not likely to affect the multicast server, unless it is using one of those IP addresses as well.

Reference:

CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Protocols and Services, page 51.

Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 2.1: Common TCP and UDP Ports, page 15.

CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Protocols and Services, pages 53-54.

Professor Messer's CompTIA N10-008 Network+ Training Course, Video 2.1: Common TCP and UDP Ports, 6.

NEW QUESTION: 20

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

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 21

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

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 22

A network administrator is implementing process changes based on recommendations following a recent penetration test. The testers used a method to gain access to the network that involved exploiting a publicly available and fixed remote code execution vulnerability in the VPN appliance. Which of the following should the administrator do to BEST prevent this from happening again?

- A. Change default passwords on internet-facing hardware.
- B. Implement robust ACLs with explicit deny-all entries.
- C. Create private VLANs for management plane traffic.
- D. Routinely upgrade all network equipment firmware.

Answer: D ([LEAVE A REPLY](#))

Explanation

Firmware is the software that runs on network equipment such as routers, switches, and VPN appliances. Firmware updates often contain bug fixes, security patches, and performance improvements that can prevent or mitigate vulnerabilities and attacks. By routinely upgrading all network equipment firmware, a network administrator can ensure that the network devices are running the latest and most secure versions of firmware and avoid exploiting known and fixed remote code execution vulnerabilities in the VPN appliance.

References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 462)

NEW QUESTION: 23

Which of the following is a characteristic of the application layer?

- A. It relies upon other layers for packet delivery.
- B. It encrypts data in transit.
- C. It checks independently for packet loss.
- D. It performs address translation.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 24

An organization has experienced an increase in malicious spear-phishing campaigns and wants to mitigate the risk of hyperlinks from inbound emails.

Which of the following appliances would best enable this capability?

- A. Email protection gateway
- B. DNS server
- C. Proxy server

D. Endpoint email client

E. Sandbox

Answer: A ([LEAVE A REPLY](#))

Explanation

An email protection gateway is an appliance that can filter and block malicious emails and attachments before they reach the recipients. An email protection gateway can mitigate the risk of hyperlinks from inbound emails by scanning the links for malicious content, rewriting the links to point to a safe domain, or blocking the links altogether. An email protection gateway can also perform other functions such as spam filtering, antivirus scanning, encryption, and data loss prevention. A DNS server, a proxy server, an endpoint email client, and a sandbox are not appliances that can enable this capability, as they have different purposes and functions.

References

1: CompTIA Network+ N10-008 Certification Study Guide, page 304

2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 15

3: CompTIA Network+ N10-008 Certification Practice Test, question 5

4: Email Protection Gateway - N10-008 CompTIA Network+ : 3.2

NEW QUESTION: 25

Which of the following is the MOST secure connection used to inspect and provide controlled internet access when remote employees are connected to the corporate network?

A. Site-to-site VPN

B. Full-tunnel VPN

C. Split-tunnel VPN

D. SSH

Answer: B ([LEAVE A REPLY](#))

The MOST secure connection would be a full-tunnel VPN. This is because all traffic from the remote device is sent through the VPN and encrypted, rather than just specific traffic as with a split-tunnel VPN.

NEW QUESTION: 26

A firewall administrator observes log entries of traffic being allowed to a web server on port 80 and port 443.

The policy for this server is to only allow

traffic on port 443. The firewall administrator needs to investigate how this change occurred to prevent a reoccurrence. Which of the following should the firewall administrator do next?

A. Consult the firewall audit logs.

B. Change the policy to allow port 80.

C. Remove the server object from the firewall policy.

D. Check the network baseline.

Answer: ([SHOW ANSWER](#))

Explanation

Firewall audit logs are records of the changes made to the firewall configuration, policies, and rules. They can help the firewall administrator to track who, when, and what changes were made to the firewall, and identify any unauthorized or erroneous modifications that could cause security issues or network outages. By consulting the

firewall audit logs, the firewall administrator can investigate how the change that allowed traffic on port 80 to the web server occurred, and prevent it from happening again

NEW QUESTION: 27

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

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 28

A company hired a technician to find all the devices connected within a network. Which of the following software tools would BEST assist the technician in completing this task?

- A. IP scanner
- B. Terminal emulator
- C. NetFlow analyzer
- D. Port scanner

Answer: A [\(LEAVE A REPLY\)](#)

IP scanners - Used to search for and detect IP addresses and other information related to devices on the network.

NEW QUESTION: 29

A network engineer designed and implemented a new office space with the following characteristics:

Building construction type:	Brick
Layout:	10,764sq ft (1,000sq m) commercial office space
Users:	50
Servers:	2
Laptops:	50

One month after the office space was implemented, users began reporting dropped signals when entering another room and overall poor connections to the 5GHz network. 'which of the following should the engineer do to best resolve the issue?

- A. use non-overlapping channels
- B. Reconfigure the network to support 2.4GHz_
- C. Upgrade to WPA3.
- D. Change to directional antennas-

Answer: D [\(LEAVE A REPLY\)](#)

The best solution to resolve the issue of dropped signals and poor connections to the 5GHz network is to change to directional antennas. Directional antennas are antennas that focus the wireless signal in a specific direction, increasing the range and strength of the signal. Directional antennas are suitable for environments where there are obstacles or interference that can weaken or block the wireless signal. In the image, the office space has several walls and doors that can reduce the signal quality of the 5GHz network, which has a shorter wavelength and higher frequency than the 2.4GHz network. By using directional antennas, the network engineer can aim the wireless signal towards the desired areas and avoid the signal loss caused by the walls and doors. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 76; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-19.

NEW QUESTION: 30

Which of the following would most likely affect design considerations when building out an IDF?

- A. The fire suppression system
- B. The humidity levels
- C. The cable transmission speeds
- D. The source panel amperage

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 31

Which of the following describes a situation in which an employee knowingly allows someone access to a restricted area without verifying authentication?

- A. Shoulder surfing
- B. Tailgating
- C. Piggybacking
- D. Phishing

Answer: B ([LEAVE A REPLY](#))

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 32

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

Which of the following is a valid IP address configuration for the device?

- A. FE80::1
- B. 100.64.0.1

- C. 169.254.1.2
- D. 172.19.0.2
- E. 224.0.0.12

Answer: [\(SHOW ANSWER\)](#)

RFC 1918 is a private IP address.

Private addresses:

- 10.0.0.0 to 10.255.255.255 (Class A private address range).
- 172.16.0.0 to 172.31.255.255 (Class B private address range).
- 192.168.0.0 to 192.168.255.255 (Class C private address range).

NEW QUESTION: 33

A technician is utilizing SNMPv3 to monitor network statistics. Which of the following actions would occur immediately of a server's utilization spikes above the prescribed value?

- A. A trap message is sent via UDP to the monitoring workstation.
- B. A response message is sent from the agent to the manager.
- C. The object identifier is modified and reported during the next monitoring cycle.
- D. The SET function pushes an alert to the MIB database.

Answer: [A \(LEAVE A REPLY\)](#)

NEW QUESTION: 34

A network technician is installing a wireless network in an office building. After performing a site survey, the technician determines the area is very saturated on the 2.4GHz and the 5GHz bands. Which of the following wireless standards should the network technician implement?

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

Answer: [B \(LEAVE A REPLY\)](#)

802.11 ax is the latest wireless standard that operates in both the 2.4GHz and the 5GHz bands. It offers higher throughput, lower latency, and improved efficiency compared to previous standards. It also uses technologies such as OFDMA and MU-MIMO to reduce interference and increase capacity in dense environments. Therefore, 802.11 ax is the best choice for a wireless network in an office building with high saturation on both bands.

Reference

Part 3 of current page talks about the benefits of 802.11 ax and how it improves network performance in congested areas¹.

CompTIA Network+ N10-008 Exam Cram covers the wireless standards and their characteristics in Chapter 5. It also provides practice questions and explanations for the exam.

NEW QUESTION: 35

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 (LEAVE A REPLY)

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://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: 36

Which of the following architectures is used for FTP?

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

Answer: A (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 37

A local company is planning to upgrade its current wireless network solution to achieve better performance and improve employees' experience. The solution will require a 5GHz radio band to support all current company devices. Which of the following should be considered as an option for the upgrade?

- A. 802.11
- B. 802.11b
- C. 802.11n
- D. 802.11g

Answer: C (LEAVE A REPLY)

The 802.11n standard is the most suitable option for this scenario. It operates in both the 2.4GHz and 5GHz frequency bands, providing better performance and higher data rates compared to older standards like 802.11b and 802.11g.

802.11n (also known as Wi-Fi 4): This standard supports multiple-input and multiple-output (MIMO) technology, which allows for better coverage, increased throughput, and improved reliability. It operates in both the 2.4GHz and 5GHz frequency bands, making it compatible with a wide range of devices. The 5GHz band provides less interference and higher data rates, making it suitable for modern networks.

802.11b: This older standard operates only in the 2.4GHz band and has a maximum data rate of 11 Mbps. It is not recommended for high-performance networks.

802.11g: This standard also operates in the 2.4GHz band and offers a maximum data rate of 54 Mbps. While it is faster than 802.11b, it is still not as efficient as 802.11n.

Reference:

Professor Messer's Network+ Study Guide

CompTIA Network+ N10-008 Study Guide

NEW QUESTION: 38

Which of the following security devices would be BEST to use to provide mechanical access control to the MDF/IDF?

- A. A smart card
- B. A key fob
- C. An employee badge
- D. A door lock

Answer: D (LEAVE A REPLY)

A door lock would be the best security device to use to provide mechanical access control to the MDF/IDF. A door lock is a device that prevents unauthorized access to a physical area by requiring a key, a code, a card, a biometric scan, or a combination of these factors to open it. A door lock can provide mechanical access control to the MDF/IDF, which are rooms that house network equipment such as switches, routers, servers, or patch panels. A door lock can prevent unauthorized persons from tampering with or stealing the network equipment or data. Reference:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_6.html

NEW QUESTION: 39

At which of the following OSI model layers does a MAC filter list for a wireless infrastructure operate?

- A. Physical
- B. Network
- C. Session
- D. Data link

Answer: D (LEAVE A REPLY)

Explanation

A MAC filter list is a security feature that allows or denies access to a wireless network based on the MAC address of the device. A MAC address is a unique identifier assigned to a network interface card (NIC) at the

physical layer of the OSI model. However, MAC filtering operates at the data link layer of the OSI model, where MAC addresses are used to encapsulate and deliver data frames between devices on the same network segment.

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: 40

A company upgrades its network and PCs to gigabit speeds. After the upgrade, users are not getting the expected performance. Technicians discover that the speeds of the endpoint NICs are inconsistent. Which of the following should be checked first to troubleshoot the issue?

- A. Devices' duplex settings
- B. Office wiring category
- C. Speed mismatches
- D. Load balancer settings

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 41

The Chief Executive Officer of a company wants to ensure business operations are not disrupted in the event of a disaster. The solution must have fully redundant equipment, real-time synchronization, and zero data loss. Which Of the following should be prepared?

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

Answer: (SHOW ANSWER)

A hot site is a backup site that is fully equipped and ready to take over the operations of the primary site in the event of a disaster. A hot site has real-time synchronization with the primary site and can provide zero data loss. A hot site is the most expensive and reliable option for disaster recovery.

NEW QUESTION: 42

A network administrator needs to run a single command-line tool capable of displaying routing table and multicast memberships.

Which of the following would BEST help the administrator achieve the requirements?

- A. show route
- B. netstate
- C. arp
- D. show config

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 43

Following a fire in a data center, an executive is concerned about the amount of data that must be reentered. Which of the following describes the executive's concern?

- A. RTO
- B. MTBF
- C. MMTR
- D. RPO

Answer: D ([LEAVE A REPLY](#))

A recovery point objective (RPO) is the maximum length of time permitted that data can be restored from, which may or may not mean data loss. It is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs.

NEW QUESTION: 44

A user cannot connect to the network, although others in the office are unaffected. The network technician sees that the link lights on the NIC are not on. The technician needs to check which switchport the user is connected to, but the cabling is not labeled. Which of the following is the best way for the technician to find where the computer is connected?

- A. Use a tone generator to trace the cable.
- B. Use a cable tester to trace the cable.
- C. Look up the computer's MAC address in the switch CAM table.
- D. Look up the computer's IP address in the switch ARP table.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 45

A network engineer is installing hardware in a newly renovated data center. Major concerns that were addressed during the renovation included air circulation, building power redundancy, and the need for continuous monitoring. The network engineer IS creating alerts based on the following operation specifications:

AC input voltage	100 to 240VAC
AC maximum input current	<2.7A at 100V
Redundant power supply	Yes
Operating temperature	32–104°F (0–40°C)
Storage temperature	-4–149°F (-20–65°C)
Operating humidity	10–85%
Storage humidity	5–95%

Which of the following should the network engineer configure?

- A. Environmental monitoring alerts for humidity greater than 95%
- B. SIEM to parse syslog events for a failed power supply
- C. SNMP traps to report when the chassis temperature exceeds 950F (3500)
- D. UPS monitoring to report when input voltage drops below 220VAC

Answer: (SHOW ANSWER)

Explanation

The alert that the network engineer should configure based on the operation specifications is SNMP traps to report when the chassis temperature exceeds 95°F (35°C). SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate their status and performance information to a central management system, called an SNMP manager. SNMP traps are messages that are sent by network devices to notify the SNMP manager of an event or condition that requires attention, such as an error, a failure, or a threshold violation. In this case, the network engineer should configure SNMP traps on the network devices to send an alert when their chassis temperature exceeds 95°F (35°C), which is the maximum operating temperature specified in the table. This alert would help the network engineer monitor and troubleshoot any overheating issues that could affect the network performance or availability. References: CompTIA Network+ N10-008 Certification Study Guide, page 228; The Official CompTIA Network+ Student Guide (Exam N10-008), page 8-11.

NEW QUESTION: 46

A network administrator needs to run a single command-line tool capable of displaying routing table and multicast memberships. Which of the following would BEST help the administrator achieve the requirements?

- A. show config
- B. netstate
- C. arp
- D. show route

Answer: C (LEAVE A REPLY)

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!
BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 47

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

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

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

- A. Last cleared

- B. Number of packets output
- C. CRCs
- D. Giants
- E. Multicasts

Answer: C ([LEAVE A REPLY](#))

CRC stands for Cyclic Redundancy Check, and it is a type of error-detecting code used to detect accidental changes to raw data. If the CRC count is increasing on a particular interface, it indicates that there might be an issue with the cabling, which is causing data corruption. References:

* Network+ N10-008 Objectives: 2.1 Given a scenario, troubleshoot common physical connectivity issues.

NEW QUESTION: 48

A network administrator is looking for a solution to extend Layer 2 capabilities and replicate backups between sites. Which of the following is the best solution?

- A. Security Service Edge
- B. Data center interconnect
- C. Infrastructure as code
- D. Zero trust architecture

Answer: B ([LEAVE A REPLY](#))

Explanation

Data center interconnect (DCI) is a solution that allows Layer 2 connectivity and data replication between geographically dispersed data centers. DCI can be implemented using various technologies, such as optical networks, MPLS, VPNs, or Ethernet. DCI can provide benefits such as improved disaster recovery, load balancing, resource pooling, and cloud services.

References:

Data Center Interconnect - CompTIA Network+ N10-008 Domain 1.4 - YouTube1 CompTIA Network+ Certification Exam Objectives, page 92

NEW QUESTION: 49

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 50

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

- A. UDP

- B. ICMP
- C. TCP
- D. ARP

Answer: B (LEAVE A REPLY)

NEW QUESTION: 51

A network administrator is setting up several IoT 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 (LEAVE A REPLY)

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 IoT 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: 52

Which of the following situations would require an engineer to configure subinterfaces?

- A. In a router-on-a-stick deployment with multiple VLANs
- B. In order to enable inter-VLAN routing on a multilayer switch
- C. When configuring VLAN trunk links between switches
- D. After connecting a router that does not support 802.1Q VLAN tags

Answer: (SHOW ANSWER)

A router-on-a-stick is a configuration that allows a single router interface to route traffic between multiple VLANs on a network¹. A router-on-a-stick requires sub-interfaces to be configured on the router interface, one for each VLAN. Each sub-interface is assigned a VLAN ID and an IP address that belongs to the corresponding VLAN subnet. The router interface is connected to a switch port that is configured as a trunk port, which allows traffic from multiple VLANs to pass through. The router then performs inter-VLAN routing by forwarding packets between the sub-interfaces based on their destination IP addresses.

Inter-VLAN routing is a process that allows devices on different VLANs to communicate with each other.

Inter-VLAN routing can be performed by a router-on-a-stick configuration, as explained above, or by a multilayer switch that has routing capabilities. A multilayer switch does not require sub-interfaces to be configured for inter-VLAN routing; instead, it uses switch virtual interfaces (SVIs) that are associated with each VLAN. An SVI is a logical interface that represents a VLAN on a switch and has an IP address that belongs to the VLAN subnet. The

switch then performs inter-VLAN routing by forwarding packets between the SVIs based on their destination IP addresses.

VLAN trunking is a method that allows traffic from multiple VLANs to be carried over a single link between switches or routers. VLAN trunking requires the use of a tagging protocol, such as 802.1Q, that adds a header to each frame that identifies its VLAN ID. VLAN trunking does not require sub-interfaces to be configured on the switches or routers; instead, it uses trunk ports that are configured to allow or deny traffic from specific VLANs. The switches or routers then forward packets between the trunk ports based on their VLAN IDs.

802.1Q is a standard that defines how VLAN tagging and trunking are performed on Ethernet networks.

802.1Q adds a 4-byte header to each frame that contains a 12-bit field for the VLAN ID and a 3-bit field for the priority level. 802.1Q does not require sub-interfaces to be configured on the switches or routers; instead, it uses trunk ports that are configured to support 802.1Q tagging and untagging. The switches or routers then forward packets between the trunk ports based on their VLAN IDs and priority levels.

NEW QUESTION: 53

A user returns to the office after working remotely for an extended period. The user is reporting limited access to the office wireless network and the inability to reach company resources on the network. The user connected to the guest network, ensured all patches were applied, and checked to make sure software was up to date. Which of the following is most likely the cause of the issue?

- A. The laptop drivers need to be updated to support a new wireless infrastructure.
- B. The wireless passphrase has been cycled and needs to be updated.
- C. The NAC appliance has labeled the laptop as non-compliant.
- D. The WAP transmit power is too low and cannot complete user authentication.

Answer: C (LEAVE A REPLY)

A network access control (NAC) appliance is a device that checks the enrollment and compliance state of devices that try to access the network resources. It can deny, quarantine, or restrict the access of non-compliant devices based on predefined policies¹. A device can be considered non-compliant if it does not meet the security requirements, such as having the latest patches, antivirus signatures, firewall settings, or encryption standards. In this scenario, the user's laptop may have been labeled as non-compliant by the NAC appliance because it was out of sync with the network policies after working remotely for a long time. The user connected to the guest network, which is usually less secure and isolated from the corporate network, and updated the patches and software, but that may not be enough to satisfy the NAC appliance. The user may need to enroll the device again, or contact the IT support to resolve the issue.

Reference 1 - Network access control integration with Microsoft Intune | Microsoft Learn

NEW QUESTION: 54

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

- A. Contract
- B. Project charter
- C. Memorandum of understanding

D. Non-disclosure agreement

Answer: (SHOW ANSWER)

The document used to inform all parties about the scope of the project before it starts is likely a project charter. A project charter is a document that outlines the key aspects of a project, including the project's objectives, scope, stakeholders, and resources. It serves as a formal agreement between the project team and the stakeholders, and helps to define the project's goals and constraints.

A project charter typically includes information about the project's scope, including the specific deliverables that are expected and any constraints or limitations that may impact the project. It may also include details about the project team and stakeholders, the project schedule and budget, and the roles and responsibilities of each party. By creating a project charter, the Chief Executive Officer and the network administrator can ensure that all parties involved in the project have a clear understanding of the project's goals and objectives, and can help to prevent misunderstandings or miscommunications during the project.

What is in a project charter?

A project charter is a formal short document that states a project exists and provides project managers with written authority to begin work. A project charter document describes a project to create a shared understanding of its goals, objectives and resource requirements before the project is scoped out in detail.

What are the 5 elements of the project charter?

What Are the Contents of a Project Charter? A project charter should always include an overview, an outline of scope, an approximate schedule, a budget estimate, anticipated risks, and key stakeholders

NEW QUESTION: 55

Which of the following cloud components can filter inbound and outbound traffic between cloud resources?

- A. NAT gateways
- B. Service endpoints
- C. Network security groups
- D. Virtual private cloud

Answer: (SHOW ANSWER)

Network security groups are cloud components that can filter inbound and outbound traffic between cloud resources based on rules and priorities. Network security groups can be applied to virtual machines, subnets, or network interfaces to control the network access and security. Network security groups can allow or deny traffic based on the source, destination, port, and protocol of the packets. Network security groups are different from NAT gateways, service endpoints, and virtual private clouds, which are other cloud components that have different functions and purposes.

Reference

- 1: Network Security Groups - N10-008 CompTIA Network+ : 3.2
- 2: CompTIA Network+ N10-008 Certification Study Guide, page 329-330
- 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 17
- 4: CompTIA Network+ N10-008 Certification Practice Test, question 10

NEW QUESTION: 56

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:

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

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 57

A technician is installing a new fiber connection to a network device in a datacenter. The connection from the device to the switch also traverses a patch panel connection. The chain of connections is in the following order:

Device

LC/LC patch cable

Patch panel

Cross-connect fiber cable

Patch panel

LC/LC patch cable

Switch

The connection is not working. The technician has changed both patch cables with known working patch cables. The device had been tested and was working properly before being installed. Which of the following is the MOST likely cause of the issue?

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

Answer: ([SHOW ANSWER](#)**)**

Explanation

The most likely cause of the issue where the fiber connection from a device to a switch is not working is that the TX/RX (transmit/receive) is reversed. When connecting fiber optic cables, it is important to ensure that the TX of one device is connected to the RX of the other device and vice versa. If the TX/RX is reversed, data cannot be transmitted successfully.

References:

CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 5: Network Operations, Objective 5.1: Given a scenario, use appropriate documentation and diagrams to manage the network.

NEW QUESTION: 58

A network administrator needs to add access points to the network because coverage in some areas is improper. Which of the following should the administrator do first?

- A. Interference analysis

- B. Wireless survey
- C. Traffic analysis
- D. Packet capture

Answer: (SHOW ANSWER)

A wireless survey is the first step that a network administrator should do before adding access points to the network. A wireless survey is a process of collecting data about the wireless environment, such as signal strength, channel usage, interference, and coverage. A wireless survey can help the network administrator to determine the optimal locations and configurations for the access points to provide the best possible coverage and performance for the wireless network. A wireless survey can also help to identify and troubleshoot any issues that may cause improper coverage in some areas. <https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html>

NEW QUESTION: 59

Two new network switches located in different buildings are connected together with single-mode fiber. However, no link exists between the two switches. Which of the following steps should the technician perform FIRST to troubleshoot the issue?

- A. Reverse TX/RX on the fiber patch cord at one building.
- B. Replace the fiber patch cords in both buildings.
- C. Clean the fiber patch cord connectors in both buildings.
- D. Connect the fiber patch cord to an OTDR at one building.

Answer: (SHOW ANSWER)

The FIRST step the technician should perform to troubleshoot the issue is C. Clean the fiber patch cord connectors in both buildings.

Dirty or contaminated fiber patch cord connectors can cause signal loss and poor network performance, and may even prevent a link from being established. Before trying any other troubleshooting steps, it is important to ensure that the fiber patch cord connectors are clean and free of debris.

NEW QUESTION: 60

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

Linux computer details:

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

Switch mirror port details:

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

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

- A. `ifconfig eth0 promisc`
- B. `ifconfig eth1 up`

C. ifconfig eth0 10.1.2.3

D. ifconfig eth1 hw ether A1:B2:C3:D4:E5:F6

Answer: A ([LEAVE A REPLY](#))

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

NEW QUESTION: 61

Users in a remote office report that corporate web server pages are taking a long time to load, whereas users in the main corporate office do not have any issues. Which of the following is the best metric for a network administrator to check?

A. Jitter across the network

B. Hop-by-hop network latency

C. Server interface CRC errors

D. Server NetFlow data

Answer: (SHOW ANSWER)

The best metric for a network administrator to check is hop-by-hop network latency. This is because network latency is the time it takes for a packet to travel from the source to the destination, and it affects the loading speed of web pages. Hop-by-hop network latency measures the latency between each pair of routers or switches along the network path, and it can help identify where the delay is occurring. By checking the hop-by-hop network latency, the network administrator can determine if the problem is caused by a slow or congested link, a misconfigured or faulty device, or a routing issue.

Jitter is the variation in latency over time, and it affects the quality of voice and video applications. Jitter does not directly affect the loading speed of web pages, and it is not a useful metric for troubleshooting this issue.

Server interface CRC errors are errors that occur when the cyclic redundancy check (CRC) of a packet does not match the expected value, indicating data corruption. Server interface CRC errors can affect the reliability and integrity of data transmission, and they can be caused by faulty cables, connectors, or interfaces. Server interface CRC errors do not necessarily affect the loading speed of web pages, unless they are severe enough to cause retransmissions or packet loss.

Server NetFlow data is data that is collected and analyzed by the NetFlow protocol, which monitors and reports on network traffic flows. Server NetFlow data can provide information on the volume, type, and direction of traffic that is sent or received by the server, as well as the source and destination IP addresses, ports, and protocols. Server NetFlow data can help identify network usage patterns, trends, and anomalies, but it does not measure the latency or performance of the network.

Reference

What is Network Latency and How to Measure It

How to Troubleshoot Network Latency Issues

What is Jitter and How to Measure It

What is CRC Error and How to Fix It

What is NetFlow and How Does It Work

CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 62

An organization has experienced an increase in malicious spear-phishing campaigns and wants to mitigate the risk of hyperlinks from inbound emails.

Which of the following appliances would best enable this capability?

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

Answer: (SHOW ANSWER)

An email protection gateway is an appliance that can filter and block malicious emails and attachments before they reach the recipients. An email protection gateway can mitigate the risk of hyperlinks from inbound emails by scanning the links for malicious content, rewriting the links to point to a safe domain, or blocking the links altogether. An email protection gateway can also perform other functions such as spam filtering, antivirus scanning, encryption, and data loss prevention. A DNS server, a proxy server, an endpoint email client, and a sandbox are not appliances that can enable this capability, as they have different purposes and functions.

References

- * 1: CompTIA Network+ N10-008 Certification Study Guide, page 304
- * 2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 15
- * 3: CompTIA Network+ N10-008 Certification Practice Test, question 5
- * 4: Email Protection Gateway - N10-008 CompTIA Network+ : 3.2

NEW QUESTION: 63

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

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

Answer: A (LEAVE A REPLY)

A toner is a tool that generates an audible signal that can be traced by a probe. A network technician can use a toner to identify the appropriate patch panel port by connecting the toner to one end of the patch cord and using the probe to scan the patch panel until the signal is detected. A toner is the easiest way to identify the patch panel port when the patch panel is not labeled, as it does not require a laptop, a cable tester, or a visual fault locator. A toner can also be used to locate breaks or shorts in a cable, or to verify continuity.

Reference:

Using a Toner and Probe - CompTIA Network+ Certification (N10-008): The Total Course Video CompTIA Network+ Certification Exam Objectives, page 141

NEW QUESTION: 64

An employee working in a warehouse facility is experiencing interruptions in mobile applications while walking around the facility. According to a recent site survey, the WLAN comprises autonomous APs that are directly connected to the internet, providing adequate signal coverage. Which of the following is the BEST solution to improve network stability?

- A. Implement client roaming using an extended service deployment employing a wireless controller.
- B. Remove omnidirectional antennas and adopt a directional bridge.
- C. Ensure all APs of the warehouse support MIMO and Wi-Fi 4.
- D. Verify that the level of EIRP power settings is set to the maximum permitted by regulations.

Answer: A ([LEAVE A REPLY](#))

Explanation

Client roaming refers to the ability of a wireless device to seamlessly connect to a different access point (AP) as the user moves around the facility. This can help to improve network stability and reduce interruptions in mobile applications. An extended service deployment is a type of wireless network configuration that uses multiple APs to cover a large area, such as a warehouse facility. By using a wireless controller to manage the APs, the network can be better optimized for client roaming, which can improve network stability.

"Roaming With multiple WAPs in an ESS, clients will connect to whichever WAP has the strongest signal. As clients move through the space covered by the broadcast area, they will change WAP connections seamlessly, a process called roaming."

NEW QUESTION: 65

An attack is redirecting traffic from network hosts by changing their assigned DNS server. None of the hosts have static IP addresses, and the rogue DNS server was assigned automatically during the hosts' lease renewal for the network configuration. Which of the following should be implemented to prevent this type of attack from occurring again?

- A. DHCP snooping
- B. Port security
- C. 802.1X authentication
- D. MAC filtering

Answer: A ([LEAVE A REPLY](#))

DHCP snooping is used to prevent unauthorized DHCP servers from assigning IP addresses and other configuration settings, such as DNS servers, to network hosts. By implementing DHCP snooping, you can protect

against attacks where a rogue DHCP server provides malicious configuration information, such as a fake DNS server.

NEW QUESTION: 66

A senior administrator has been directed to incorporate AAA services within a domain environment for regulatory compliance purposes. Which of the following standards will enable the use of an AAA server in a domain environment?

- A. 802.1Q
- B. 802.1X
- C. 802.3bt
- D. 802.11h

Answer: B ([LEAVE A REPLY](#))

802.1X is a standard that enables the use of an AAA server in a domain environment by providing port-based network access control. 802.1X authenticates users or devices before granting them access to the network resources, and can also authorize them based on their roles or policies. 802.1X can work with different AAA protocols, such as RADIUS or TACACS+, to communicate with the AAA server.

References:

- * CompTIA Network+ N10-008 Certification Study Guide, page 211
- * CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 382
- * Configuring AAA Services - Cisco3

NEW QUESTION: 67

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

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 68

A technician is configuring a wireless access point in a public space for guests to use. Which of the following should the technician configure so that only approved connections are allowed?

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

Answer: B ([LEAVE A REPLY](#))

A captive portal is a web page that requires users to authenticate or accept terms of service before they can access the internet through a wireless access point. A captive portal can be used to control who can use the wireless network, limit the bandwidth or time of usage, or display advertisements or information. A captive portal is a common feature of public wireless networks, such as those in hotels, airports, cafes, or libraries. A captive portal can prevent unauthorized or malicious users from accessing the network or consuming network resources.

References: Public Wireless Access Points Definition | Law Insider

NEW QUESTION: 69

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 70

A network administrator is preparing new switches that will be deployed to support a network extension project. The lead network engineer has already provided documentation to ensure the switches are set up properly.

Which of the following did the engineer most likely provide?

- A. Physical network diagram
- B. Logical network diagram
- C. Baseline configurations
- D. Site survey reports

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 71

A network security engineer is responding to a security incident. The engineer suspects that an attacker used an authorized administrator account to make configuration changes to the boundary firewall. Which of the following should the network security engineer review?

- A. Network traffic logs
- B. Audit logs
- C. Syslogs
- D. Event logs

Answer: ([SHOW ANSWER](#))

(Firewall) Audit logs provide a chronological record of system activities, including user actions, access attempts, and configuration changes, crucial for security monitoring and compliance audits.

NEW QUESTION: 72

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 (LEAVE A REPLY)

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://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: 73

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

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

Answer: D (LEAVE A REPLY)

NEW QUESTION: 74

A company wants an administrator to perform a vulnerability test. The administrator finds the company has a POTS phone system. Which of the following can the administrator use to point out the phone system vulnerability?

- A. Butt set
- B. Spyware
- C. Blue jacking
- D. Honeypot

Answer: A (LEAVE A REPLY)

NEW QUESTION: 75

Which of the following devices is found in the middle tier of a three-tier network architecture?

- A. Router
- B. Multilayer switch
- C. Access switch

D. Firewall

Answer: B (LEAVE A REPLY)

In a three-tier network architecture, the middle tier is typically where the distribution layer resides, which connects network services to the access layer below and the core layer above. A multilayer switch operates at this level, providing routing, switching, and traffic management between subnets and VLANs.

NEW QUESTION: 76

Which of the following requires network devices to be managed using a different set of IP addresses?

A. Console

B. Split tunnel

C. Jump box

D. Out of band

Answer: D (LEAVE A REPLY)

Out of band management is a process for accessing and managing network devices and infrastructure at remote locations through a separate management plane from the production network. Out of band management requires network devices to be managed using a different set of IP addresses than the ones used for in-band management or data traffic. This provides a secure and dedicated alternate access method to administer connected devices and IT assets without using the corporate LAN.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 77

A user is having trouble uploading files to a server. However, other users in the department are not experiencing this issue. The network administrator checks the access switch and sees multiple CRC errors on that user's switchport. Which of the following should the network administrator do first?

A. Replace the uplink cable for the access switch.

B. Replace the user's network cable.

C. Replace the NIC for the user's PC.

D. Replace the access switch.

Answer: (SHOW ANSWER)

When a network administrator observes CRC errors on a specific switchport associated with one user, the first troubleshooting step recommended is to replace the user's network cable. CRC errors are often indicative of physical layer issues such as noise, interference, or damaged cables. By replacing the network cable, the administrator can potentially resolve these errors without more drastic measures like replacing hardware.

components (NIC, switch, or uplink cables), which could be more costly and less effective as initial steps. This approach minimizes downtime and is a cost-effective first step in the troubleshooting process.

NEW QUESTION: 78

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

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

Which of the following is MOST likely the issue?

- A. The switchport is shut down
- B. The cable is not plugged in.
- C. The loopback is not set
- D. The bandwidth configuration is incorrect.

Answer: A (LEAVE A REPLY)

Explanation

The switchport is shut down, which means it is administratively disabled and cannot forward traffic. The image shows that the switchport status is "down" and the protocol status is "down", indicating that there is no physical or logical connection. The cable is plugged in, as shown by the "connected" message under the interface name. The loopback is not set, as shown by the "loopback not set" message under the encapsulation type. The bandwidth configuration is correct, as shown by the "BW 10000 Kbit/sec" message under the MTU size. References:

[CompTIA Network+ Certification Exam Objectives], Domain 3.0 Infrastructure, Objective

3.1: Given a scenario, use appropriate networking tools, Subobjective: Command line tools (ping, netstat, tracer, etc.)

NEW QUESTION: 79

Which of the following is used to provide disaster recovery capabilities to spin up all critical devices using internet resources?

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

Answer: (SHOW ANSWER)

A cloud site is the correct answer and provides disaster recovery capabilities to spin up all critical devices using internet resources. A cloud site is a type of disaster recovery solution that allows an organization to access and use its critical systems and data in the cloud, rather than on physical servers. In the event of a disaster, an organization can use its cloud site to quickly spin up all its critical devices and continue operations using internet resources.

A hot site, is not the correct answer in this scenario. A hot site is a type of disaster recovery site that is fully equipped and ready for immediate use. It typically includes all the necessary hardware, software, and

infrastructure to support an organization's operations in the event of a disaster. However, a hot site is not necessarily designed to use internet resources to spin up critical devices, as is the case with a cloud site.

NEW QUESTION: 80

A network engineer installed a new fiber uplink for an office and wants to make sure that the link meets throughput requirements. Which of the following tools should the engineer use to verify that the new link is sufficient?

- A. tcpdump
- B. ping
- C. iperf
- D. netstat

Answer: C (LEAVE A REPLY)

iperf is a tool that can measure the bandwidth and quality of a network link by generating and transferring TCP or UDP data streams. iperf can report the maximum achievable throughput, packet loss, jitter, and other statistics for a given link. iperf can be used to test both the uplink and downlink performance of a network link by running it on two endpoints and specifying the direction and duration of the test. iperf can help the engineer verify that the new fiber uplink meets the throughput requirements for the office network.

tcpdump is a tool that can capture and analyze network traffic by filtering and displaying packets based on various criteria. tcpdump can help the engineer troubleshoot network problems, monitor network activity, and inspect packet contents, but it cannot measure the throughput or quality of a network link.

ping is a tool that can test the reachability and latency of a network host by sending and receiving ICMP echo packets. ping can help the engineer check if the new fiber uplink is connected and responsive, and how long it takes for packets to travel between the endpoints, but it cannot measure the throughput or quality of a network link.

netstat is a tool that can display information about the network connections, routing tables, interfaces, and protocols on a network host. netstat can help the engineer view the status and details of the network connections using the new fiber uplink, but it cannot measure the throughput or quality of a network link.

Reference

iperf - The ultimate speed test tool for TCP, UDP and SCTP

How to use iperf to test local network LAN speed in Windows 10

How to Test Network Performance Between Two Linux Servers

What is tcpdump?

8 Common Network Utilities Explained

Monitoring Your Network: ping, netstat, tcpdump, and Ethereal

Netstat vs. Nmap vs. Netcat: Understanding the Differences

NEW QUESTION: 81

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

- A. Implement a solution.
- B. Establish a theory.
- C. Escalate the issue.

D. Document the findings.

Answer: B ([LEAVE A REPLY](#))

Explanation

1 Identify the Problem.

2 Develop a Theory.

3 Test the Theory.

4 Plan of Action.

5 Implement the Solution.

6 Verify System Functionality.

7 Document the Issue.

NEW QUESTION: 82

A customer needs to distribute Ethernet to multiple computers in an office. The customer would like to use non-proprietary standards. Which of the following blocks does the technician need to install?

A. 110

B. 66

C. Bix

D. Krone

Answer: ([SHOW ANSWER](#))

For distributing Ethernet to multiple computers in an office using non-proprietary standards, the technician would typically use a block that adheres to industry-standard termination methods. The

110 block is a type of punch-down block commonly used for terminating and connecting twisted- pair cables, including those used for Ethernet.

NEW QUESTION: 83

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

A. Password policy

B. Remote access policy

C. Acceptable use policy

D. Data loss prevention policy

Answer: A ([LEAVE A REPLY](#))

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

NEW QUESTION: 84

Users report that a database server responds slowly or drops connections to other servers at random during busy times. A technician notices the database and servers are connected to an access switch in the office. Which of the following should the technician do to improve the performance of the database server?

- A. Use different ports on the access switch.
- B. Move the cable connection for users to the same switch as the database server.
- C. Implement LACP on the connection to the database server.
- D. Move the server connection from the access switch to the core switch.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 85

The following DHCP scope was configured for a new VLAN dedicated to a large deployment of 325 IoT sensors: The first 244 IoT sensors were able to connect to the TFTP server, download the configuration file, and register to an IoT management system. The other sensors are being shown as offline. Which of the following should be performed to determine the MOST likely cause of the partial deployment of the sensors?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 86

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 87

A network device is configured to send critical events to a syslog server; however, the following alerts are not being received:

Severity 5 LINK-UPDOWN: Interface 1/1, changed state to down

Severity 5 LINK-UPDOWN: Interface 1/3, changed state to down

Which of the following describes the reason why the events are not being received?

- A. The network device is not configured to log that level to the syslog server
- B. The network device was down and could not send the event
- C. The syslog server is not compatible with the network device

D. The syslog server did not have the correct MIB loaded to receive the message

Answer: ([SHOW ANSWER](#))

There are 7 severity logging levels: Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug (0-7). The question states the log is only configured to report "CRITICAL" events, and the events that occurred are level 5 i.e (NOTICE) events.

NEW QUESTION: 88

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

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

Answer: ([SHOW ANSWER](#))

To prevent IP address conflicts when allocating a portion of a DHCP scope's subnet for statically assigned devices, it is recommended to use the concept of DHCP exclusion ranges.

DHCP exclusion ranges allow a DHCP administrator to specify a range of IP addresses within the scope that should not be assigned to DHCP clients. This can be useful in situations where some devices on the network need to be assigned static IP addresses, as it ensures that the statically assigned addresses do not overlap with addresses assigned by the DHCP server.

To set up a DHCP exclusion range, the administrator needs to specify the start and end IP addresses of the range, as well as the subnet mask. The DHCP server will then exclude the specified range of addresses from its pool of available addresses, and will not assign them to DHCP clients.

By using DHCP exclusion ranges, the technician can ensure that the statically assigned addresses do not conflict with addresses assigned by the DHCP server, and can prevent IP address conflicts on the network.

NEW QUESTION: 89

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** ([LEAVE A REPLY](#))

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: 90

A network security administrator needs to monitor the contents of data sent between a secure network and the rest of the company.

Which of the following monitoring methods will accomplish this task?

- A. Port mirroring
- B. Flow data
- C. Syslog entries
- D. SNMP traps

Answer: A (LEAVE A REPLY)

Port mirroring is a method of monitoring network traffic by copying the data packets from one port to another port on the same switch or router. This allows the network security administrator to analyze the contents of the data sent between different networks without affecting the performance or security of the original traffic. Port mirroring can be configured to capture all traffic or only specific types of traffic, such as VLANs, protocols, or IP addresses.

Reference:

Port Mirroring - CompTIA Network+ N10-008 Domain 3.1 - YouTube1

CompTIA Network+ Certification Exam Objectives, page 142

NEW QUESTION: 91

A false camera is installed outside a building to assist with physical security. Which of the following is the device assisting?

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

Answer: A (LEAVE A REPLY)

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 92

A new global ISP needs to connect from central offices in North America to the United Kingdom. Which of the following would be the BEST cabling solution for this project?

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

D. Twinaxial

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 93

Which of the following objectives does an evil twin achieve?

- A. DNS poisoning
- B. Log-in credentials
- C. ARP spoofing
- D. Denial of service

Answer: B ([LEAVE A REPLY](#))

The objective that an evil twin achieves is log-in credentials. An evil twin is a type of rogue access point that mimics a legitimate wireless network by using the same SSID, encryption, and authentication methods. An evil twin can trick unsuspecting users into connecting to it instead of the real network, and then capture their log-in credentials or other sensitive data. An evil twin can also perform man-in-the-middle attacks, redirecting or modifying the user's traffic. References: CompTIA Network+ N10-008 Certification Study Guide, page 358; The Official CompTIA Network+ Student Guide (Exam N10-008), page 14-1.

NEW QUESTION: 94

Users attending security training at work are advised not to use single words as passwords for corporate applications. Which of the following does this BEST protect against?

- A. A dictionary attack
- B. MAC spoofing
- C. Denial of service
- D. An on-path attack
- E. A brute-force attack

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 95

A small, family-run business uses a single SOHO router to provide Internet and WiFi to its employees. At the start of a new week, employees come in and find their usual WiFi network is no longer available, and there is a new wireless network to which they cannot connect. Given that information, which of the following should have been done to avoid this situation?

- A. The device firmware should have been kept current.
- B. Unsecure protocols should have been disabled.
- C. Parental controls should have been enabled
- D. The default credentials should have been changed

Answer: D ([LEAVE A REPLY](#))

Explanation

The default credentials are the username and password that come with a device or service when it is first installed or configured. They are often easy to guess or find online, which makes them vulnerable to unauthorized access or attacks. The default credentials should be changed to something unique and strong as soon as possible to avoid this situation. If the default credentials were not changed, someone could have accessed the SOHO router and changed the WiFi settings without the employees' knowledge. References:

<https://www.comptia.org/blog/network-security-basics-6-easy-ways-to-protect-your-network>

NEW QUESTION: 96

A network administrator wants to improve the security of the management console on the company's switches and ensure configuration changes made can be correlated to the administrator who conformed them Which of the following should the network administrator implement?

- A. Port security
- B. Local authentication
- C. TACACS+
- D. Access control list

Answer: (SHOW ANSWER)

Explanation

TACACS+ is a protocol that provides centralized authentication, authorization, and accounting (AAA) for network devices and users. TACACS+ can help improve the security of the management console on the company's switches by verifying the identity and credentials of the administrators, enforcing granular access policies and permissions, and logging the configuration changes made by each administrator. This way, the network administrator can ensure only authorized and authenticated users can access and modify the switch settings, and also track and correlate the changes made by each user. References:

<https://www.comptia.org/blog/what-is-tacacs>

NEW QUESTION: 97

A SQL server connects over port:

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

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 98

A company wants to invest in new hardware for the core network infrastructure. The management team requires that the infrastructure be capable of being repaired in less than 60 minutes if any major part fails.

Which of the following metrics is MOST likely associated with this requirement?

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

Answer: B ([LEAVE A REPLY](#))

MTTR is directly related to how quickly a system can be repaired if any major part fails³. The management team requires that the infrastructure be capable of being repaired in less than 60 minutes, which means they have a low MTTR requirement.

MTTR stands for Mean Time To Repair and is a metric used to measure the average amount of time it takes to repair a failed component or system. In this case, the requirement is for the infrastructure to be capable of being repaired in less than 60 minutes if any major part fails, which means the MTTR should be less than 60 minutes.

NEW QUESTION: 99

Which of the following attacks can be effectively protected against by using techniques to check if a connection was made by a human user? (Choose two.)

- A. Brute-force
- B. Phishing
- C. On-path attack
- D. Shoulder surfing
- E. Evil twin
- F. Dictionary

Answer: A,F ([LEAVE A REPLY](#))

NEW QUESTION: 100

Which of the following routing protocols uses bandwidth and delay as the primary metrics to calculate the best path?

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

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 101

Which of the following systems would MOST likely be found in a screened subnet?

- A. RADIUS
- B. FTP
- C. SQL
- D. LDAP

Answer: B (LEAVE A REPLY)

Explanation

FTP (File Transfer Protocol) is a system that would most likely be found in a screened subnet. A screened subnet, or triple-homed firewall, is a network architecture where a single firewall is used with three network interfaces. It provides additional protection from outside cyber attacks by adding a perimeter network to isolate or separate the internal network from the public-facing internet¹. A screened subnet typically hosts systems that need to be accessed by both internal and external users, such as web servers, email servers, or FTP servers.

References:

<https://www.techtarget.com/searchsecurity/definition/screened-subnet#:~:text=A%20screened%20subnet%2C%21>

NEW QUESTION: 102

A network security technician is designing a solution for a secure remote access scheme with the following requirements:

- The solution must allow for users at multiple locations to access corporate resources.
- The on-premises equipment will not handle non-corporate, resource-bound traffic.

Which of the following should the network security technician consider when designing the solution? (Choose two.)

- A. Full-tunnel VPN
- B. Client-to-site VPN
- C. Personal VPN
- D. Split-tunnel VPN
- E. Clientless VPN
- F. Site-to-site VPN

Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 103

A network security administrator needs to monitor the contents of data sent between a secure network and the rest of the company. Which of the following monitoring methods will accomplish this task?

- A. Port mirroring
- B. Flow data
- C. Syslog entries
- D. SNMP traps

Answer: A (LEAVE A REPLY)

Port mirroring is a method of monitoring network traffic by copying the data packets from one port to another port on the same switch or router. This allows the network security administrator to analyze the contents of the data sent between different networks without affecting the performance or security of the original traffic. Port mirroring can be configured to capture all traffic or only specific types of traffic, such as VLANs, protocols, or IP addresses.

References:

* Port Mirroring - CompTIA Network+ N10-008 Domain 3.1 - YouTube1

* CompTIA Network+ Certification Exam Objectives, page 142

NEW QUESTION: 104

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

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

Answer: A ([LEAVE A REPLY](#))

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

NEW QUESTION: 105

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

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

Answer: B ([LEAVE A REPLY](#))

What is in a project charter?

A project charter is a formal short document that states a project exists and provides project managers with written authority to begin work. A project charter document describes a project to create a shared understanding of its goals, objectives and resource requirements before the project is scoped out in detail.

What are the 5 elements of the project charter?

What Are the Contents of a Project Charter? A project charter should always include an overview, an outline of scope, an approximate schedule, a budget estimate, anticipated risks, and key stakeholders.

NEW QUESTION: 106

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: A,B (LEAVE A REPLY)

A MAC address is a unique identifier assigned to a network interface card (NIC) that allows it to communicate on a physical network layer, such as Ethernet¹. An IP address is a logical identifier assigned to a device that allows it to communicate on a network layer, such as IP².

A technician can use different methods to find the IP address of a device if they know its MAC address. Two of the most common methods are looking at the ARP table and the DHCP leases.

The ARP table is a data structure that stores the mappings between IP addresses and MAC addresses on a device. ARP stands for Address Resolution Protocol, which is a network protocol that enables devices to discover the MAC address of another device based on its IP address³. The ARP table is populated by sending ARP requests and receiving ARP replies, or by using static ARP entries that are manually configured⁴.

A technician can look at the ARP table of their own device or a nearby device, such as a router or a switch, to find the IP address of a device with a known MAC address. For example, on a Windows device, the technician can use the command `arp -a` to display the ARP table, and look for the entry that matches the MAC address. On a Cisco device, the technician can use the command `show ip arp` to display the ARP table, and look for the entry that matches the MAC address.

The DHCP leases are the records of the IP addresses that are assigned by a DHCP server to DHCP clients. DHCP stands for Dynamic Host Configuration Protocol, which is a network protocol that enables devices to obtain IP addresses and other network configuration parameters automatically from a DHCP server. The DHCP leases contain information such as the IP address, the MAC address, the lease duration, and the expiration time of each DHCP client.

A technician can look at the DHCP leases of the DHCP server that serves the network segment where the device with the known MAC address is connected. For example, on a Windows DHCP server, the technician can use the DHCP console to view the DHCP leases, and look for the entry that matches the MAC address. On a Cisco DHCP server, the technician can use the command `show ip dhcp binding` to view the DHCP leases, and look for the entry that matches the MAC address.

The other options are incorrect for the following reasons:

C . IP route table is a data structure that stores the routes to different network destinations on a device. It does not store the MAC addresses of the devices on the network.

D . DNS cache is a data structure that stores the mappings between domain names and IP addresses on a device. DNS stands for Domain Name System, which is a network service that translates human-readable domain names into IP addresses. It does not store the MAC addresses of the devices on the network.

E . MAC address table is a data structure that stores the mappings between MAC addresses and switch ports on a switch. It does not store the IP addresses of the devices on the network.

F . STP topology is a network design that uses the Spanning Tree Protocol (STP) to prevent loops and create a loop-free logical topology on a switched network. It does not store the IP addresses or the MAC addresses of the devices on the network. Reference:

1: MAC address - Wikipedia

- 2: IP address - Wikipedia
- 3: Address Resolution Protocol - Wikipedia
- 4: How ARP Works
- 5: How to Use the Arp Command in Windows
- 6: show ip arp
- 7: Dynamic Host Configuration Protocol - Wikipedia
- 8: DHCP Lease
- 9: View DHCP Leases
- 10: show ip dhcp binding
- 11: Routing table - Wikipedia
- 12: Domain Name System - Wikipedia
- 13: DNS cache - Wikipedia
- 14: MAC address table - Wikipedia
- 15: Spanning Tree Protocol - Wikipedia

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 107

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: ([SHOW ANSWER](#))

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: 108

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

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

Answer: ([SHOW ANSWER](#))

To improve performance for videoconferencing, the company should configure Quality of Service (QoS). This technology allows for the prioritization of network traffic, ensuring that videoconferencing traffic is given higher priority and therefore better performance. Link Aggregation Control Protocol (LACP), Dynamic routing, Network load balancer, and Static IP addresses are not directly related to improving performance for videoconferencing.

Reference:

Network+ N10-007 Certification Exam Objectives, Objective 2.6: Given a scenario, implement and configure the appropriate wireless security and implement the appropriate QoS concepts.

NEW QUESTION: 109

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

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

Which of the following is misconfigured?

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

Answer: ([SHOW ANSWER](#))

Explanation

The subnet mask is a binary value that defines how many bits of an IP address are used to identify the network and how many bits are used to identify the host. The subnet mask also determines the size and number of subnets in a network. The ipconfig command shows the current IP configuration of a device, including the subnet mask. In this case, the subnet mask is misconfigured because it does not match the network address of the

device. The device has an IP address of 192.168.1.55, which belongs to the network 192.168.1.0/24 (with a subnet mask of 255.255.255.0). However, the subnet mask is set to 225.225.225.224, which is an invalid value that does not correspond to any network prefix length. This causes the device to be unable to communicate with other devices on the same network or access the default gateway. References: CompTIA Network+ N10-008 Certification Study Guide, page 109; The Official CompTIA Network+ Student Guide (Exam N10-008), page 5-4.

NEW QUESTION: 110

A technician is setting up DNS records on local servers for the company's cloud DNS to enable access by hostname. Which of the following records should be used?

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

Answer: A ([LEAVE A REPLY](#))

An A record, also known as an address record, is a type of DNS record that maps a hostname to an IPv4 address. An A record is used to resolve a domain name to an IP address, so that clients can connect to the server or service by using the domain name instead of the IP address. For example, an A record can map `www.example.com` to `192.0.2.1`.

An A record is the most common type of DNS record for cloud DNS, as it allows the company to use a custom domain name for their cloud services, such as web hosting, email, or storage. An A record can also be used to create subdomains, such as `blog.example.com` or `mail.example.com`, that point to different IP addresses or servers.

The other options are not correct because they are not the best type of DNS record for cloud DNS. They are: MX. MX stands for mail exchange, and it is a type of DNS record that specifies the mail servers that are responsible for receiving and delivering email messages for a domain name. MX records are used for email services, but they are not sufficient for cloud DNS, as they do not map a hostname to an IP address.

CNAME. CNAME stands for canonical name, and it is a type of DNS record that specifies an alias name for another domain name. CNAME records are used to create multiple names for the same IP address or server, such as `www.example.com` and `example.com`. CNAME records are useful for cloud DNS, but they are not the best type, as they depend on another A record to resolve the IP address.

NS. NS stands for name server, and it is a type of DNS record that delegates a DNS zone to an authoritative server. NS records are used to specify which DNS servers are responsible for answering queries for a domain name or a subdomain. NS records are essential for cloud DNS, but they are not the best type, as they do not map a hostname to an IP address.

Reference

- 1: DNS records overview | Google Cloud
- 2: Network+ (Plus) Certification | CompTIA IT Certifications
- 3: CloudDNS: What is a DNS record?

NEW QUESTION: 111

Which of the following OSI model layers are responsible for handling packets from the sources to the destination and checking for errors? (Choose two.)

- A. Application
- B. Physical
- C. Data link
- D. Session
- E. Presentation
- F. Network

Answer: C,F ([LEAVE A REPLY](#))

NEW QUESTION: 112

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, the administrator sees the 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: (SHOW ANSWER)

- * The firewall rules are set to deny any traffic from any source to specific destination IP addresses on any port.
- * The destination IP addresses are in different ranges, but one of them is in the multicast range of 224.0.0.0 to 239.255.255.255.
- * The multicast range is used to send data to multiple recipients at once, such as streaming video or audio.
- * The multicast server on the network is likely using an IP address in the multicast range to broadcast its data to the clients.
- * Therefore, the firewall rule that is most likely causing the issue is the one that denies any traffic to the IP address 232.1.4.9, which is in the multicast range.
- * The other rules are not likely to affect the multicast server, unless it is using one of those IP addresses as well.

References:

- * CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Protocols and Services, page 51.
- * Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 2.1: Common TCP and UDP Ports, page 15.
- * CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Protocols and Services, pages 53-54.
- * Professor Messer's CompTIA N10-008 Network+ Training Course, Video 2.1: Common TCP and UDP Ports, 6.

NEW QUESTION: 113

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

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

Answer: A (LEAVE A REPLY)

The command show interface is used to display information about the status, speed, duplex mode, and other parameters of the network interfaces on a device. It can also show the number of packets sent and received, the error rate, and the utilization rate of each interface.

The command can help determine whether an LACP bundle is fully operational by showing the aggregated bandwidth, the load balancing method, the active and standby links, and the LACP protocol status of each interface in the bundle.

LACP (Link Aggregation Control Protocol) is a protocol that allows multiple physical links to be combined into a logical link, or a bundle, to increase the bandwidth and provide redundancy. LACP is also known as IEEE 802.3ad or EtherChannel.

The command show config is used to display the current configuration of the device, such as the hostname, the IP addresses, the routing protocols, the security settings, and the interface settings. It does not show the operational status of the interfaces or the LACP bundle.

The command show route is used to display the routing table of the device, which contains the destination networks, the next-hop addresses, the interface names, and the metrics of the routes. It does not show the operational status of the interfaces or the LACP bundle.

The command show arp is used to display the ARP (Address Resolution Protocol) cache of the device, which contains the mappings between the IP addresses and the MAC addresses of the devices on the local network. It does not show the operational status of the interfaces or the LACP bundle. Reference:

CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Devices and Technologies, Section 2.1: Explain the functions and purposes of various network devices, Page 77-78 Professor Messer's Network+ N10-008 Course Notes, Page 13 Professor Messer's Network+ N10-008 Video Training Course, Section 2.1: Network Devices, Video 2.1.6: Link Aggregation

NEW QUESTION: 114

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 (LEAVE A REPLY)

* The concept that best represents the life expectancy of different models of data center equipment is MTBF, which stands for Mean Time Between Failures. MTBF is a measure of the average time that a device or component operates before it fails. It is calculated by dividing the total operating time by the number of failures. MTBF is an indicator of the reliability and durability of the equipment, and it can help the Chief Information Officer (CIO) to compare the expected performance and maintenance costs of different models.

* MTRR, which stands for Memory Type Range Register, is not a concept that represents the life expectancy of data center equipment. MTRR is a feature of some processors that allows them to control how the memory is accessed and cached. MTRR can improve the performance and efficiency of the processor, but it does not affect the longevity of the equipment.

* RPO, which stands for Recovery Point Objective, is not a concept that represents the life expectancy of data center equipment. RPO is a measure of the maximum amount of data that can be lost in the event of a disaster or disruption. It is determined by the frequency and method of data backup. RPO is an indicator of the data protection and recovery strategy, and it can help the CIO to plan for the worst-case scenario, but it does not reflect the durability of the equipment.

* RTO, which stands for Recovery Time Objective, is not a concept that represents the life expectancy of data center equipment. RTO is a measure of the maximum amount of time that it takes to restore the normal operations of the network after a disaster or disruption. It is determined by the complexity and availability of the recovery resources and processes. RTO is an indicator of the business continuity and resilience, and it can help the CIO to minimize the downtime and losses, but it does not reflect the reliability of the equipment. References:

* CompTIA Network+ N10-008 Study Guide, Chapter 3: Network Operations, Section 3.2:

Troubleshooting Methodology and Tools, Page 150

* Professor Messer's Network+ N10-008 Course Notes, Page 18

* Professor Messer's Network+ N10-008 Video Training Course, Section 3.2: Network Troubleshooting Tools, Video 3.2.3: Hardware Tools

NEW QUESTION: 115

A network technician is troubleshooting a connectivity issue. All users within the network report that they are unable to navigate to websites on the internet; however, they can still access local network resources. The technician issues a command and receives the following results:

Pinging comptia.com [172.67.217.56] with 32 bytes of data:

Reply from 172.67.217.56: TTL expired in transit.

Reply from 172.67.217.56: TTL expired in transit.

Reply from 172.67.217.56: TTL expired in transit.

Reply from 172.67.217.56: TTL expired in transit.

Which of the following best explains the result of this command?

A. Incorrect VLAN settings

B. Upstream routing loop

C. Network collisions

D. DNS misconfiguration

Answer: B (LEAVE A REPLY)

NEW QUESTION: 116

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

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

Answer: A ([LEAVE A REPLY](#))

Latency is the time it takes for a data packet to travel from one point to another on a network. It is measured in milliseconds (ms) and affects the quality and speed of online activities such as gaming, video conferencing, and web browsing¹².

Accessibility is the availability of a network service to users in different locations and situations. It depends on factors such as coverage area, infrastructure, cost, and compatibility³.

Satellite internet is a type of broadband service that uses satellites orbiting the earth to transmit and receive data signals. It is often used in rural or remote areas where other types of internet are not available or reliable.

Satellite internet is most likely to have the highest latency while being the most accessible compared to the other options because:

Satellite internet has to send and receive data over long distances between the earth and the satellites, which adds significant delay to the transmission. The average latency for satellite internet is around 600 ms, which is much higher than the other types of internet, which usually have latency below 100 ms.

Satellite internet is the most accessible because it can reach almost any location on the planet, as long as there is a clear line of sight between the satellite dish and the sky. It does not depend on cables, wires, or towers, which may not be available or affordable in some areas.

The other options are not correct because:

DSL (Digital Subscriber Line) is a type of broadband service that uses existing telephone lines to deliver data signals. It is widely available in urban and suburban areas, but may not reach some rural or remote areas. It has low to moderate latency, usually around 10 to 70 ms.

Cable internet is a type of broadband service that uses coaxial cables that carry TV signals to deliver data signals. It is also widely available in urban and suburban areas, but may not reach some rural or remote areas. It has low to moderate latency, usually around 10 to 50 ms.

4G (Fourth Generation) is a type of wireless broadband service that uses cellular towers to deliver data signals. It is available in most populated areas, but may not have good coverage or signal strength in some rural or remote areas. It has low to moderate latency, usually around 20 to 40 ms.

Reference:

- 1: What is Latency? - Cloudflare
- 2: How Latency Affects Internet Speed - Lifewire
- 3: What is Internet Accessibility? - Techopedia
- 4: Internet Accessibility - World Bank
- 5: What is Satellite Internet? - How-To Geek
- 6: Satellite Internet: What It Is and How It Works - PCMag
- 7: What is DSL Internet? - HighSpeedInternet.com
- 8: DSL vs. Cable vs. Fiber vs. Satellite Internet-Compare Internet Types - Business.org

- 9: What is Cable Internet? - HighSpeedInternet.com
10: Broadband grudge match: Cable vs. DSL vs. 4G - Digital Trends
11: What is 4G? - Verizon
12: 4G vs. LTE: The differences explained - Digital Trends

NEW QUESTION: 117

Which of the following routing protocols uses an autonomous system number?

- A. EIGRP
- B. OSPF
- C. BGP
- D. IS-IS

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 118

Within the realm of network security, Zero Trust:

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 119

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	64458067024

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

- A. The switchport has been up for too long
- B. The connected device is sending too many packets
- C. The connected device is receiving too many packets.

- D. The connected device is exceeding the configured MTU.
- E. The switchport does not have enough CRCs

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 120

Which of the following issues are present with RIPv2? (Select TWO).

- A. Route poisoning
- B. Time to converge
- C. Scalability
- D. Unicast
- E. Adjacent neighbors
- F. Maximum transmission unit

Answer: (SHOW ANSWER)

The disadvantages of RIP (Routing Information Protocol) include the following.

- Outdated, insecure, and slow. This is your parents' protocol. It was a thing before the Web was born.
 - The more well-known problem of the 15 hop limitation in which data must travel
 - Convergence time is terrible for information propagation in a network
 - Metrics. It determines the number of hops from source to destination, and gives no regard to other factors when determining the best path for data to travel
 - Overhead. A good example would be routing tables. These are broadcast at half-minute intervals to other routers regardless of whether the data has changed or not. It's essentially like those old cartoons where the town guard in the walled city cries out, '10 o' the clock and all is well!'
- RIPv2 introduced more security and reduced broadcast traffic, which is relevant for some available answers here.

NEW QUESTION: 121

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

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

Answer: B ([LEAVE A REPLY](#))

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 122

A network administrator is reviewing the network device logs on a syslog server. The messages are normal, but the time stamps on the messages are incorrect.

Which of the following actions should the administrator take to ensure the log message time stamps are correct?

- A. Adjust the SSH settings on the network device.
- B. Adjust the timeout settings on the syslog server
- C. Update the network device firmware
- D. Change the NTP settings on the network device
- E. Change the time on the syslog server

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 123

A technician is troubleshooting servers with high CPU usage. While trying to connect, the technician needs to open a port for remote access. Which of the following ports should the technician open?

- A. 443
- B. 3321
- C. 8080
- D. 5900

Answer: D ([LEAVE A REPLY](#))

Port 5900 is the default port used by Virtual Network Computing (VNC), a graphical desktop-sharing system that allows remote access to another computer's screen, keyboard and mouse¹. VNC is one of the tools that can be used for remote troubleshooting of servers with high CPU usage, as it enables the technician to see the server's desktop and perform actions on it. Port 5900 is also one of the ports listed in the CompTIA Network+ N10-008 exam objectives under the section "1.4 Given a scenario, use appropriate software tools to troubleshoot connectivity issues"².

The other ports are not commonly used for remote access. Port 443 is used for Hypertext Transfer Protocol Secure (HTTPS), a secure version of HTTP that encrypts the communication between a web browser and a web server³. Port 3321 is used for Telepathy Broker Service, a service that provides communication between applications and telephony devices⁴. Port 8080 is used for HTTP Alternate, an alternative port for HTTP that is often used by web servers for testing or proxy purposes⁵.

Reference

1: Port 5900: What Is It Used for & How to Open It for RDP

2: Network+ (Plus) Certification | CompTIA IT Certifications

3: [What is HTTPS? - Definition from WhatIs.com]

4: [Telepathy Broker Service - Port 3321 - TCP/UDP]

5: [What is Port 8080? Why do some processes use this port?]

NEW QUESTION: 124

An attacker is attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt. Which of the following attack types BEST describes this action?

- A. Pass-the-hash attack
- B. Rainbow table attack

C. Brute-force attack

D. Dictionary attack

Answer: D (LEAVE A REPLY)

The attacker attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt is using a dictionary attack. References: CompTIA Network+ Certification Study Guide, Chapter 6: Network Attacks and Mitigation.

NEW QUESTION: 125

The Chief Executive Officer of a company wants to ensure business operations are not disrupted in the event of a disaster. The solution must have fully redundant equipment, real-time synchronization, and zero data loss.

Which Of the following should be prepared?

A. Cloud site

B. Warm site

C. Hot site

D. Cold site

Answer: C (LEAVE A REPLY)

A hot site is a backup site that is fully equipped and ready to take over the operations of the primary site in the event of a disaster. A hot site has real-time synchronization with the primary site and can provide zero data loss.

A hot site is the most expensive and reliable option for disaster recovery.

References: Network+ Study Guide Objective 5.3: Explain common scanning, monitoring and patching processes and summarize their expected outputs.

NEW QUESTION: 126

Which of the following is MOST commonly used to address CVEs on network equipment and/or operating systems?

A. Vulnerability assessment

B. Factory reset

C. Firmware update

D. Screened subnet

Answer: C (LEAVE A REPLY)

Explanation

Firmware is a type of software that controls the low-level functions of a hardware device, such as a router, switch, printer, or camera. Firmware updates are patches or upgrades that fix bugs, improve performance, add features, or address security vulnerabilities in firmware. Firmware updates are commonly used to address CVEs (Common Vulnerabilities and Exposures) on network equipment and operating systems, as CVEs are publicly known flaws that can be exploited by attackers. References:

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

NEW QUESTION: 127

Which of the following would be used to filter web traffic based on content?

A. Access point

- B. Proxy server
- C. Load balancer
- D. Media converter

Answer: B (LEAVE A REPLY)

NEW QUESTION: 128

A network administrator is testing performance improvements by configuring channel bonding on an 802.Hac AP. Although a site survey detected the majority of the 5GHz frequency spectrum was idle, being used only by the company's WLAN and a nearby government radio system, the AP is not allowing the administrator to manually configure a large portion of the 5GHz frequency range. Which of the following would be BEST to configure for the WLAN being tested?

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

Answer: D (LEAVE A REPLY)

NEW QUESTION: 129

A technician is installing a new fiber connection to a network device in a datacenter. The connection from the device to the switch also traverses a patch panel connection. The chain of connections is in the following order:

Device

LC/LC patch cable

Patch panel

Cross-connect fiber cable

Patch panel

LC/LC patch cable

Switch

The connection is not working. The technician has changed both patch cables with known working patch cables. The device had been tested and was working properly before being installed. Which of the following is the MOST likely cause of the issue?

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

Answer: A (LEAVE A REPLY)

The most likely cause of the issue where the fiber connection from a device to a switch is not working is that the TX/RX (transmit/receive) is reversed. When connecting fiber optic cables, it is important to ensure that the TX of one device is connected to the RX of the other device and vice versa. If the TX/RX is reversed, data cannot be transmitted successfully.

Reference:

CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 5: Network Operations, Objective 5.1: Given a scenario, use appropriate documentation and diagrams to manage the network.

NEW QUESTION: 130

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. 802.1Q
- C. Duplex
- D. LACP

Answer: D (LEAVE A REPLY)

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.

NEW QUESTION: 131

A network technician added a new workstation to the network and needs to make a custom, shielded cable that is 492ft (150m) with both ends wired to TIA/EIA-568A standards. The workstation is not establishing a link to the switchport. Which of the following is the cause of the issue?

- A. Cable shielding
- B. Attenuation
- C. Incorrect pinout
- D. Near-end crosstalk

Answer: B (LEAVE A REPLY)

Attenuation, or the loss of signal strength over distance, is likely the cause of the issue with the 492ft (150m) cable not establishing a link to the switchport. Ethernet standards typically limit the length of copper Ethernet cables to approximately 328ft (100m) for standard performance. Exceeding this distance, as in the case of the 492ft cable, often results in insufficient signal strength to maintain a reliable connection. Options such as cable shielding, incorrect pinout, or near-end crosstalk do not directly relate to the problem described by the excessive cable length.

NEW QUESTION: 132

A network device needs to discover a server that can provide it with an IPv4 address. Which of the following does the device need to send the request to?

- A. Default gateway
- B. Broadcast address
- C. Unicast address

D. Link local address

Answer: B (LEAVE A REPLY)

The DHCP client sends broadcast request packets to the network; the DHCP servers respond with broadcast packets that offer IP parameters, such as an IP address for the client. After the client chooses the IP parameters, communication between the client and server is by unicast packets.

"When a DHCP client boots up, it automatically sends out a DHCP Discover UDP datagram to the broadcast address, 255.255.255.255. This DHCP Discover message asks "Are there any DHCP servers out there?" The client can't send unicast traffic yet, as it doesn't have a valid IP address that can be used."

NEW QUESTION: 133

A network technician is observing the behavior of an unmanaged switch when a new device is added to the network and transmits data. Which of the following BEST describes how the switch processes this information?

- A.** The data is flooded out of every port but only in the VLAN where it is located.
- B.** The data is flooded out of every port, including the one on which it came in.
- C.** The data is flooded out of every port, except the one on which it came in
- D.** The data is flooded out of every port, excluding the VLAN where it is located

Answer: C (LEAVE A REPLY)

NEW QUESTION: 134

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 (LEAVE A REPLY)

* DNS poisoning is a type of attack that exploits the vulnerabilities of the DNS protocol to redirect network traffic to malicious websites or servers¹². DNS poisoning can affect both the DNS resolver cache and the DNS client cache, making it difficult to detect and remove¹².

* One of the common ways that DNS poisoning can occur is when an attacker compromises the router and changes its DNS settings to point to a rogue DNS server¹². This way, the router will assign the malicious DNS server to the network clients, and any DNS queries from the clients will be resolved by the attacker's server¹².

* To prevent this type of attack, one of the best practices is to change the device's default password and use a strong and unique password for the router's administrative interface¹³. This will make it harder for the attacker to gain access to the router and modify its DNS settings¹³.

* Changing the device's default password is also a general security measure that should be applied to any router or network device, as many attackers exploit the fact that many users do not change the default credentials that come with the device³⁴.

* Therefore, the correct answer is A. Change the device's default password, as this will help prevent DNS poisoning attacks and improve the overall security of the router and the network.

References:

- * 1: What is DNS poisoning and how to prevent it - BlueCat Networks
- * 2: An Introduction to "DNS Poisoning" (And How to Prevent It) - Kinsta
- * 3: The Best Router Settings for Home Networks - Lifewire
- * 4: Recommended settings for Wi-Fi routers and access points

NEW QUESTION: 135

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

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

Answer: B ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 136

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

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

Answer: B ([LEAVE A REPLY](#))

Explanation

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

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 137

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

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

Answer: B (LEAVE A REPLY)

The DNS record that works as an alias to another record is called CNAME (Canonical Name). CNAME records are used to create an alias for a domain name that points to another domain name.

Reference:

CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.3: Given a scenario, implement and configure the appropriate addressing schema.

NEW QUESTION: 138

An IT administrator received an assignment with the following objectives

- * Conduct a total scan within the company's network for 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.** netstat
- D.** tcpdump

Answer: A (LEAVE A REPLY)

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: 139

At which layer of the OSI model do MAC addresses operate?

- A. Application
- B. Network
- C. Data Link
- D. Physical

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 140**SIMULATION**

A network technician was recently onboarded to a company. A manager has tasked the technician with documenting the network and has provided the technician with partial information from previous documentation.

INSTRUCTIONS

Click on each switch to perform a network discovery by entering commands into the terminal.

Type help in each terminal to view a list of available commands.

Fill in the missing information using the drop-down menus provided.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Core Switch 1

Access Switch 1

Access Switch 2

PC1

PC2

PC3

PC4

PC1	PC2	PC3	PC4
Select MAC Address Select MAC Address 0200.0000.0002 0200.0000.0003 0200.0000.0004 0200.0000.0005 0200.0000.0006 0200.0000.0007 0200.0000.0008 0200.0000.0009	Select MAC Address Select MAC Address 0200.0000.0002 0200.0000.0003 0200.0000.0004 0200.0000.0005 0200.0000.0006 0200.0000.0007 0200.0000.0008 0200.0000.0009	Select MAC Address Select MAC Address 0200.0000.0002 0200.0000.0003 0200.0000.0004 0200.0000.0005 0200.0000.0006 0200.0000.0007 0200.0000.0008 0200.0000.0009	Select MAC Address Select MAC Address 0200.0000.0002 0200.0000.0003 0200.0000.0004 0200.0000.0005 0200.0000.0006 0200.0000.0007 0200.0000.0008 0200.0000.0009
Select IP Address Select IP Address 10.10.30.51 10.10.30.52 10.10.30.53 10.10.30.54 10.10.60.51 10.10.60.52 10.10.60.53 10.10.60.54	Select IP Address Select IP Address 10.10.30.51 10.10.30.52 10.10.30.53 10.10.30.54 10.10.60.51 10.10.60.52 10.10.60.53 10.10.60.54	Select IP Address Select IP Address 10.10.30.51 10.10.30.52 10.10.30.53 10.10.30.54 10.10.60.51 10.10.60.52 10.10.60.53 10.10.60.54	Select IP Address Select IP Address 10.10.30.51 10.10.30.52 10.10.30.53 10.10.30.54 10.10.60.51 10.10.60.52 10.10.60.53 10.10.60.54
Select VLAN Select VLAN 10 20	Select VLAN Select VLAN 10 20	Select VLAN Select VLAN 10 20	Select VLAN Select VLAN 10 20
Select Interface Select Interface GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3 GigabitEthernet0/4	Select Interface Select Interface GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3 GigabitEthernet0/4	Select Interface Select Interface GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3 GigabitEthernet0/4	Select Interface Select Interface GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3 GigabitEthernet0/4

Answer:

The IP address of Core Switch 1 is 10.10.30.1

The VLAN configuration of Core Switch 1 is VLAN 10: 10.10.30.0/24

Explanation:

(Note: IPs will be change on each simulation task, so we have given example answer for the understanding) To perform a network discovery by entering commands into the terminal, you can use the following steps:

Click on each switch to open its terminal window.

Enter the command show ip interface brief to display the IP addresses and statuses of the switch interfaces.

Enter the command show vlan brief to display the VLAN configurations and assignments of the switch interfaces.

Enter the command show cdp neighbors to display the information about the neighboring devices that are connected to the switch.

Fill in the missing information in the diagram using the drop-down menus provided.

Here is an example of how to fill in the missing information for Core Switch 1:

The IP address of Core Switch 1 is 192.168.1.1.

The VLAN configuration of Core Switch 1 is VLAN 1: 192.168.1.0/24, VLAN 2: 192.168.2.0/24, VLAN 3: 192.168.3.0/24.

The neighboring devices of Core Switch 1 are Access Switch 1 and Access Switch 2.

The interfaces that connect Core Switch 1 to Access Switch 1 are GigabitEthernet0/1 and GigabitEthernet0/2.

The interfaces that connect Core Switch 1 to Access Switch 2 are GigabitEthernet0/3 and GigabitEthernet0/4.

You can use the same steps to fill in the missing information for Access Switch 1 and Access Switch 2.

NEW QUESTION: 141

A network technician wants to deploy a new wireless access point to reduce user latency. Currently, the organization has the following deployed:

Which of the following channels should the new device broadcast on?

- A. Channel 3
- B. Channel 9
- C. Channel 10
- D. Channel 11

Answer: D (LEAVE A REPLY)

The best channel for a new wireless access point is one that does not overlap with the existing channels used by other devices. Overlapping channels can cause interference and degrade the performance of the wireless network. According to the web search results, the 2.4 GHz band has 11 channels in the U.S., but only channels 1, 6, and 11 are non-overlapping. Since the existing devices are using channels 1 and 6, the new device should use channel 11 to avoid adjacent-channel interference¹² Reference1: Why Channels 1, 6 and 11? | MetaGeek 2: How to Choose the Best Wi-Fi Channels for Your Network - Lifewire

NEW QUESTION: 142

A network administrator is adding a new switch to the network. Which of the following network hardening techniques would be BEST to use once the switch is in production?

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 143

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 ([LEAVE A REPLY](#))

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: 144

A network requirement calls for the network traffic of a specific department within a campus network to be monitored. The network has users from each department located in multiple buildings. Which of the following should be configured to meet this requirement? (Choose two.)

- A. MDIX
- B. 802.1Q
- C. Jumbo frames
- D. Port mirroring
- E. Flow control
- F. LACP

Answer: B,D ([LEAVE A REPLY](#))

802.1Q is a standard for VLAN tagging, which allows the network administrator to segment the network traffic of different departments into separate VLANs. This makes it easier to monitor and manage the traffic of each department.

Port mirroring is a feature that allows the network administrator to copy the traffic from one or more ports to another port for analysis. By configuring port mirroring on the ports connected to the specific department, the network administrator can monitor the traffic of that department in real-time.

NEW QUESTION: 145

A network technician is working on a new switch implementation to expand the network. Which of the following is the BEST option to ensure the implementation goes according to business requirements?

- A. AUP
- B. SOP
- C. SLA
- D. NDA

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 146

Which of the following routing protocols should be implemented to create a route between a local area network and an ISP?

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

Answer: (SHOW ANSWER)

BGP stands for Border Gateway Protocol, and it is a routing protocol that is used to exchange routing information between different autonomous systems (AS) on the Internet. An AS is a network or a group of networks that are under the same administrative control and share a common routing policy. BGP is used to create routes between local area networks and Internet service providers (ISPs), as well as between different ISPs. BGP is considered an exterior gateway protocol (EGP), as opposed to an interior gateway protocol (IGP) such as EIGRP, RIP, or OSPF, which are used to create routes within an AS. Reference: CompTIA Network+ N10-008 Cert Guide, Chapter 3, Section 3.4

NEW QUESTION: 147

A technician discovered that some information on the local database server was changed during a file transfer to a remote server. Which of the following should concern the technician the MOST?

- A. Confidentiality
- B. Integrity
- C. DDoS
- D. On-path attack

Answer: B (LEAVE A REPLY)

Integrity refers to the accuracy and consistency of data over its entire lifecycle, from creation to storage and retrieval. In this scenario, the technician has discovered that some information on the local database server was changed during a file transfer to a remote server, indicating that the data may have been altered or corrupted in some way. This would raise concerns about the integrity of the data, as it may not be complete or accurate.

NEW QUESTION: 148

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

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

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

- A. Electrical
- B. Humidity
- C. Flooding

D. Temperature

Answer: B (LEAVE A REPLY)

Humidity is the amount of water vapor in the air. High humidity can cause corrosion, condensation, and short circuits in electronic devices. Low humidity can cause static electricity and damage sensitive components. The optimal humidity range for a data center is between 40% and 60%. Based on the report, the humidity level in the server room is 70%, which is too high and can affect the performance and reliability of the network equipment. Therefore, the best recommendation to the client is to install a humidity sensor and a dehumidifier to control the humidity level in the server room.

NEW QUESTION: 149

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

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

Answer: A,C (LEAVE A REPLY)

* A site survey is a process of analyzing the wireless environment and determining the optimal locations, configurations, and parameters for access points (APs). A site survey can help identify sources of interference, dead spots, signal strength, and coverage areas¹.

* AP placement is the physical location of the APs in relation to the wireless clients, walls, ceilings, floors, and other obstacles. AP placement affects the signal quality, coverage, and performance of the wireless network².

* The network administrator should check the site survey and the AP placement first when troubleshooting intermittent Wi-Fi connectivity issues, as these factors can directly impact the wireless signal and user experience.

* EIRP (Effective Isotropic Radiated Power) is the total power radiated by an antenna in a specific direction. EIRP is affected by the transmitter power, cable loss, and antenna gain³. EIRP is not the first thing to check, as it is usually configured according to the site survey and the regulatory standards.

* A captive portal is a web page that requires users to authenticate or accept some terms and conditions before accessing the wireless network. A captive portal can be used for security, marketing, or legal purposes. A captive portal is not the first thing to check, as it does not affect the wireless signal or connectivity, but only the access to the network resources.

* SSID (Service Set Identifier) is the name of a wireless network that is broadcasted by the APs. SSID assignment is the process of configuring the SSID on the APs and the wireless clients. SSID assignment is not the first thing to check, as it does not affect the wireless signal or connectivity, but only the identification of the network.

* AP association time is the time it takes for a wireless client to connect to an AP and establish a wireless link. AP association time is not the first thing to check, as it does not affect the wireless signal or

* connectivity, but only the initial connection process.

References:

- * 1: Site Survey
- * 2: AP Placement
- * 3: EIRP
- * : [Captive Portal]

NEW QUESTION: 150

A company, which is located in a coastal town, retrofitted an office building for a new data center. The underground fiber optics were brought in and connected to the switches in the basement network MDF. A server data center was built on the fifth floor with the two rooms vertically connected by fiber optics. Which of the following types of environmental sensors is MOST needed?

- A.** Temperature sensor in the network MDF
- B.** Water sensor in the network MDF
- C.** Temperature sensor in the data center
- D.** Water sensor in the data center

Answer: B ([LEAVE A REPLY](#))

Explanation

A water sensor is a type of environmental sensor that detects the presence of water or moisture in an area. A water sensor is most needed in a network main distribution frame (MDF) that is located in a basement near underground fiber-optic cables. A network MDF is a central point where all the network connections converge and where network equipment such as switches and routers are located. If water leaks into the basement and damages the fiber-optic cables or the network equipment, it can cause network outages, performance degradation, or data loss. A water sensor can alert the network administrator of any water intrusion and help prevent or minimize the damage. References:

<https://www.comptia.org/training/books/network-n10-008-study-guide> (page 446)

NEW QUESTION: 151

A technician is troubleshooting a report about network connectivity issues on a workstation. Upon investigation, the technician notes the workstation is showing an APIPA address on the network interface. The technician verifies that the VLAN assignment is correct and that the network interlace has connectivity. Which of the following is MOST likely the issue the workstation is experiencing?

- A.** A rogue DHCP server
- B.** A DNS server outage
- C.** An incorrect subnet mask
- D.** DHCP exhaustion

Answer: D ([LEAVE A REPLY](#))

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam

questions have been updated and answers have been corrected get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 152

Which of the following routing protocols is generally used by major ISPs for handling large-scale internet traffic?

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

Answer: (SHOW ANSWER)

BGP stands for Border Gateway Protocol, and it is the standard protocol for exchanging routing information between different autonomous systems (AS) on the internet¹². An AS is a network or a group of networks under a single administrative control, such as an ISP or a large enterprise¹².

BGP is an Exterior Gateway Protocol (EGP), which means it is used to communicate with routers outside the local network or AS¹². BGP allows each AS to advertise its own routes and policies to other ASes, and to learn the best routes to reach any destination on the internet¹².

BGP is generally used by major ISPs for handling large-scale internet traffic because it is highly scalable, flexible, and reliable¹². BGP can handle millions of routes and thousands of ASes, and it can support various routing policies and preferences¹². BGP also has mechanisms to detect and avoid routing loops, and to recover from network failures¹².

The other options are not suitable for handling large-scale internet traffic across different ASes. RIP (Routing Information Protocol) and EIGRP (Enhanced Interior Gateway Routing Protocol) are both Distance Vector protocols, which means they use the number of hops as the metric to find the best route³⁴. They are also Interior Gateway Protocols (IGP), which means they are used to communicate with routers within the same network or AS³⁴. RIP and EIGRP are not scalable or flexible enough to handle the complexity and diversity of the internet³⁴. OSPF (Open Shortest Path First) is a Link State protocol, which means it uses the speed and cost of the links as the metric to find the best route⁵. It is also an IGP, which means it is used to communicate with routers within the same network or AS⁵. OSPF is more scalable and flexible than RIP and EIGRP, but it still has limitations in handling large-scale internet traffic across different ASes⁵. Reference:

1: CompTIA Network+ N10-008 Certification Study Guide, Chapter 3: Routing, Section 3.4: BGP⁶

2: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 18: BGP⁷

3: CompTIA Network+ N10-008 Certification Study Guide, Chapter 3: Routing, Section 3.2: RIP and EIGRP⁶

4: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 16: RIP and EIGRP⁷

5: CompTIA Network+ N10-008 Certification Study Guide, Chapter 3: Routing, Section 3.3: OSPF⁶

6: CompTIA Network+ N10-008 Certification Study Guide²

7: Professor Messer's CompTIA Network+ N10-008 Training Course⁵

NEW QUESTION: 153

Access to a datacenter should be individually recorded by a card reader even when multiple employees enter the facility at the same time. Which of the following allows the enforcement of this policy?

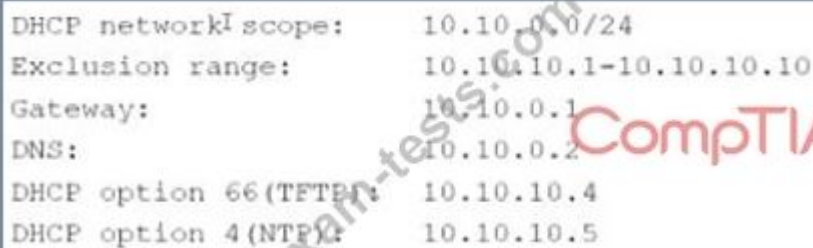
- A. Motion detection
- B. Access control vestibules
- C. Smart lockers
- D. Cameras

Answer: B ([LEAVE A REPLY](#))

The devil is in the details, the question is essentially asking, why would it be possible for an individual to use a card reader, that would be a access control vestibule or mantrap. An individual would typically utilize a card reader if you want to access a particular room via a mantrap.

NEW QUESTION: 154

The following DHCP scope was configured for a new VLAN dedicated to a large deployment of 325 IoT sensors:



```
DHCP network scope: 10.10.0.0/24
Exclusion range: 10.10.0.1-10.10.0.10
Gateway: 10.10.0.1
DNS: 10.10.0.2
DHCP option 66 (TFTP): 10.10.10.4
DHCP option 4 (NTP): 10.10.10.5
```

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 155

A network administrator needs to back up the configurations of all network devices and store the configurations off-line until they are needed. Which of the following should the administrator use to back up the configurations securely?

- A. Telnet
- B. SFTP
- C. Syslog
- D. SNMP

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 156

A lab environment hosts Internet-facing web servers and other experimental machines, which technicians use for various tasks. A technician installs software on one of the web servers to allow communication to the company's file server, but it is unable to connect to it. Other machines in the building are able to retrieve files from the file server.

Which of the following is the MOST likely reason the web server cannot retrieve the files, and what should be done to resolve the problem?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 157

A network administrator redesigned the positioning of the APs to create adjacent areas of wireless coverage. After project validation, some users still report poor connectivity when their devices maintain an association to a distanced AP. Which of the following should the network administrator check FIRST?

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

Answer: ([SHOW ANSWER](#))

Explanation

The network administrator should check the roaming settings on the APs and WLAN clients first. Roaming is the process of switching from one AP to another without losing connectivity. If the roaming settings are not configured properly, some users may experience poor connectivity when their devices stay connected to a distant AP instead of switching to a closer one. References:

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-roam-faq.html>

NEW QUESTION: 158

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** ([LEAVE A REPLY](#))

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: 159

A customer wants to segregate the traffic between guests on a hypervisor. Which of the following does a technician need to configure to meet the requirement?

- A. Fibre Channel
- B. NIC teaming
- C. OSPF routing
- D. Virtual switches
- E. Load balancers

Answer: D (LEAVE A REPLY)

A virtual switch is a software-based switch that connects virtual machines on a hypervisor. A virtual switch can create and manage VLANs, which are logical segments of a network that isolate traffic between different groups of devices. A customer can use virtual switches to segregate the traffic between guests on a hypervisor by creating a separate VLAN for each guest and assigning it to a virtual switch port. Reference:

<https://www.comptia.org/blog/what-is-a-virtual-switch>

NEW QUESTION: 160

A network administrator wants to analyze attacks directed toward the company's network. Which of the following must the network administrator implement to assist in this goal?

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

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 161

Many IP security cameras use RTSP to control media playback. Which of the following default transport layer port numbers does RTSP use?

- A. 5060

B. 445

C. 587

D. 554

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 162

A network technician needs to subnet the network. The marketing department has 28 devices.

Which of the following private IP address spaces should be used to ensure the MINIMUM number of unused IP addresses?

A. Gateway: 172.15.18.128

Netmask: 255.255.255.224

B. Gateway: 10.10.10.1

Netmask: 255.255.255.192

C. Gateway: 224.102.113.65

Netmask: 255.255.255.192

D. Gateway: 192.168.1.97

Netmask: 255.255.255.224

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 163

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

A. DLP

B. AUP

C. BYOD

D. NDA

Answer: C ([LEAVE A REPLY](#))

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

NEW QUESTION: 164

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. 5GHz

- B. 900MHZ
- C. 850MHz
- D. 2.4GHz

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 165

Which of the following is the first step a network administrator should take in the troubleshooting methodology?

- A. Establish a plan of action.
- B. Document findings and outcomes.
- C. Test the theory to determine cause.
- D. Identify the problem.

Answer: D ([LEAVE A REPLY](#))

According to the network troubleshooting methodology, the first step a network administrator should take is to identify the problem. This involves gathering information from the users, the network devices, and the symptoms of the issue. Identifying the problem helps to narrow down the scope and the possible causes of the network issue.

Reference

- 1: Network troubleshooting methodology | CompTIA Network+ N10-008 ...
- 2: Chapter 21. A Network Troubleshooting Methodology - CompTIA Network+ ...
- 3: Network Troubleshooting Methodology - N10-008 CompTIA Network+ : 5.1

NEW QUESTION: 166

Which of the following can be used to identify users after an action has occurred?

- A. Access control vestibule
- B. Cameras
- C. Asset tag
- D. Motion detectors

Answer: ([SHOW ANSWER](#))

Cameras can be used to identify users after an action has occurred by recording their faces, clothing, or other distinctive features. Cameras are often used as a deterrent and a forensic tool for security purposes. Access control vestibules, asset tags, and motion detectors are not effective in identifying users, but rather in controlling access, tracking assets, and detecting movement.

Reference:

CompTIA Network+ N10-008 Certification Exam Objectives, Domain 5.0: Network Security, Subobjective 5.1: Summarize the importance of physical security controls, page 231 CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008), Chapter 18: Network Security, Section: Physical Security, page 7372

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 167

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 (LEAVE A REPLY)

The change-management process includes Request for Change (RFC) documentation - resources that record why and when a change, such as an upgrade, was made.

None of the other options would provide documentation for PREVIOUS changes to a system.

Standard operating procedures might document work instructions for handling previously encountered incidents, but not for systemic changes like upgrades.

NEW QUESTION: 168

A network administrator received a report stating a critical vulnerability was detected on an application that is exposed to the internet. Which of the following is the appropriate NEXT step?

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

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 169

A network manager wants to view network traffic for devices connected to a switch. A network engineer connects an appliance to a free port on the switch and needs to configure the switch port connected to the appliance.

Which of the following is the best option for the engineer to enable?

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

Answer: B (LEAVE A REPLY)

Port mirroring is a feature that allows a switch to copy the traffic from one or more ports to another port, where a network analyzer or a monitoring device can capture and analyze the traffic. Port mirroring is useful for troubleshooting and security purposes, as it allows the network engineer to see the traffic that is passing through the switch without affecting the normal operation of the network.

Reference

- 1: Port Mirroring - CompTIA Network+ Certification (N10-008): The Total Course [Video]
- 2: CompTIA Network+ Certification Exam Objectives, page 5
- 3: CompTIA Network+ N10-005: 2.1 - Port Mirroring - Professor Messer IT Certification Training Courses
- 4: CompTIA Network+ N10-005: 1.4 - Port Mirroring

NEW QUESTION: 170

Which of the following describes when an active exploit is used to gain access to a network?

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

Answer: A (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 171

To find the best subnet mask that meets the requirement of six usable IP addresses, we need to calculate the number of host bits and the number of host addresses for each option. The number of host bits is the number of 0s in the binary representation of the subnet mask, and the number of host addresses is $2^{\text{host bits}} - 2$ (the -2 is to exclude the network address and the broadcast address). The option that has the smallest number of host addresses that is greater than or equal to six is the best choice. Here are the calculations for each option:

A. 255.255.255.128

Binary: 11111111.11111111.11111111.10000000

Host bits: 7

Host addresses: $2^7 - 2 = 126 - 2 = 124$

This option has too many host addresses for the requirement.

B. 255.255.255.192

Binary: 11111111.11111111.11111111.11000000

Host bits: 6

Host addresses: $2^6 - 2 = 64 - 2 = 62$

This option also has too many host addresses for the requirement.

C. 255.255.255.224

Binary: 11111111.11111111.11111111.11100000

Host bits: 5

Host addresses: $2^5 - 2 = 32 - 2 = 30$

This option has the smallest number of host addresses that is greater than or equal to six, so this is the best choice.

D. 255.255.255.240

Binary: 11111111.11111111.11111111.11110000

Host bits: 4

Host addresses: $2^4 - 2 = 16 - 2 = 14$

This option has fewer host addresses than the requirement, so this is not a valid choice.

Answer: C (LEAVE A REPLY)

Explanation

This subnet mask will allow you to have six usable IP addresses in each subnet, with a minimum of wasted addresses. You can use the following formula to calculate the number of subnets and the subnet ID for each subnet:

Number of subnets = $2^{\text{network bits}}$ Subnet ID = (subnet number - 1) x number of host addresses + network address The network bits are the number of 1s in the binary representation of the subnet mask, and the network address is the first address in the range. For example, if your range is 192.168.1.0/27, then the network bits are 27, the network address is 192.168.1.0, and the number of host addresses is 30. Therefore, the number of subnets is

2^{27} , and the subnet ID for the first subnet is $(1 - 1) \times 30 + 192.168.1.0 = 192.168.1.0$. The subnet ID for the second subnet is $(2 - 1) \times 30 + 192.168.1.0 = 192.168.1.32$, and so on.

References

Subnet masks are covered in Objective 1.4 of the CompTIA Network+ N10-008 certification exam¹.

Subnet masks can be calculated based on binary and CIDR-block notations².

Subnet masks can be used to determine the number of host bits and host addresses³.

1: CompTIA Network+ Certification Exam Objectives, page 4 2: IPv4 Subnet Masks - N10-008 CompTIA Network+ : 1.41 3: Calculating IPv4 Subnets and Hosts - N10-008 CompTIA Network+ : 1.44

NEW QUESTION: 172

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

A. Automate a continuous backup and restore process of the system's state of the active gateway.

B. Use a static assignment of the gateway IP address on the network clients.

C. Configure DHCP relay and allow clients to receive a new IP setting.

D. Configure a shared VIP and deploy VRRP on the routers.

Answer: D ([LEAVE A REPLY](#))

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

NEW QUESTION: 173

An organization with one core and five distribution switches is transitioning from a star to a full-mesh topology. Which of the following is the number of additional network connections needed?

A. 5

B. 10

C. 15

D. 7

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 174

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

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

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

A. Electrical

B. Humidity

C. Flooding

D. Temperature

Answer: B ([LEAVE A REPLY](#))

Explanation

Humidity is the amount of water vapor in the air. High humidity can cause corrosion, condensation, and short circuits in electronic devices. Low humidity can cause static electricity and damage sensitive components. The optimal humidity range for a data center is between 40% and 60%. Based on the report, the humidity level in the server room is 70%, which is too high and can affect the performance and reliability of the network equipment. Therefore, the best recommendation to the client is to install a humidity sensor and a dehumidifier to control the humidity level in the server room.

References: Network+ Study Guide Objective 5.1: Summarize the importance of physical security controls.

NEW QUESTION: 175

A network technician was recently onboarded to a company. A manager has tasked the technician with documenting the network and has provided the technician With partial information from previous documentation. Instructions:

Click on each switch to perform a network discovery by entering commands into the terminal. Fill in the missing information using drop-down menus provided.

Core Switch 1

Access Switch 1

Access Switch 2

PC1

PC2

PC3

PC4

0200.0000.0003

Select MAC Address

Select IP Address

Select VLAN

Select Interface

10.10.30.51

Select IP Address

Select VLAN

Select Interface

0200.0000.0004

Select MAC Address

Select IP Address

Select VLAN

Select Interface

10.10.30.53

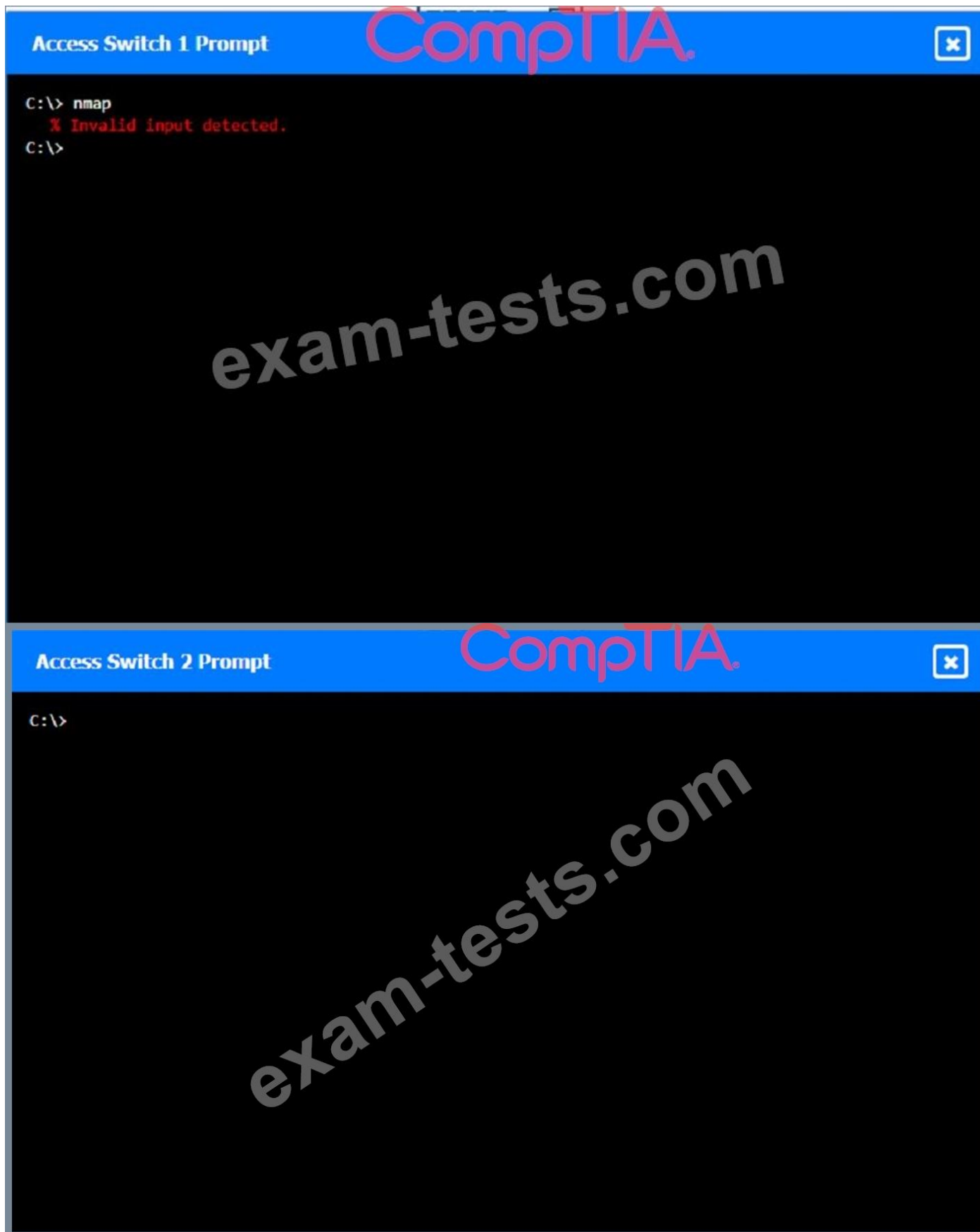
Select IP Address

Select VLAN

Select Interface

Core Switch 1 Prompt

```
C:\> nmap
% Invalid input detected.
C:\> netdiscover
% Invalid input detected.
C:\> |
```



A. See the Explanation for detailed information on this simulation

Answer: ([SHOW ANSWER](#))

(Note: Ips will be change on each simulation task, so we have given example answer for the understanding) To perform a network discovery by entering commands into the terminal, you can use the following steps:

Click on each switch to open its terminal window.

Enter the command `show ip interface brief` to display the IP addresses and statuses of the switch interfaces.

Enter the command `show vlan brief` to display the VLAN configurations and assignments of the switch interfaces.

Enter the command `show cdp neighbors` to display the information about the neighboring devices that are connected to the switch.

Fill in the missing information in the diagram using the drop-down menus provided.

Here is an example of how to fill in the missing information for Core Switch 1:

The IP address of Core Switch 1 is 192.168.1.1.

The VLAN configuration of Core Switch 1 is VLAN 1: 192.168.1.0/24, VLAN 2: 192.168.2.0/24, VLAN 3: 192.168.3.0/24.

The neighboring devices of Core Switch 1 are Access Switch 1 and Access Switch 2.

The interfaces that connect Core Switch 1 to Access Switch 1 are GigabitEthernet0/1 and GigabitEthernet0/2.

The interfaces that connect Core Switch 1 to Access Switch 2 are GigabitEthernet0/3 and GigabitEthernet0/4.

You can use the same steps to fill in the missing information for Access Switch 1 and Access Switch 2.

NEW QUESTION: 176

Which of the following BEST describes a split-tunnel client-to-server VPN connection?

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

Answer: C (LEAVE A REPLY)

In a split-tunnel VPN, only certain network traffic (usually traffic destined for the remote network) is sent over the VPN tunnel, while other traffic is sent directly to the local gateway and out to the internet. This can improve overall network performance for the user, but can also introduce some security risks if the local network is not properly secured.

NEW QUESTION: 177

Which of the following can have multiple VLAN interfaces?

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

Answer: D (LEAVE A REPLY)

NEW QUESTION: 178

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: B ([LEAVE A REPLY](#))

The Network layer is responsible for logical addressing and routing, which enables data to be transmitted between different networks. It receives data from the upper layers, including the application layer, and formats it for transmission over the network by adding routing information and other protocol-specific details.

NEW QUESTION: 179

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 ([LEAVE A REPLY](#))

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: 180

A firewall that detects and prevents attacks from outside the network based on learned data patterns can BEST be described as which of the following?

A. Host based IPS

B. Network based IDS

C. Signature based IDS

D. Behavior based IPS

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 181

A network administrator is configuring a new switch and wants to ensure that only assigned devices can connect to the switch. Which of the following should the administrator do?

A. Disable unnecessary services.

B. Enable port security.

C. Configure ACLs.

D. Implement a captive portal.

Answer: ([SHOW ANSWER](#)**)**

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 182

A network technician needs to select an AP that will support at least 1.3Gbps and 5GHz only. Which of the following wireless standards must the AP support to meet the requirements?

- A. B
- B. AC
- C. AX
- D. N
- E. G

Answer: B (LEAVE A REPLY)

Explanation

Wireless AC is a wireless standard that supports up to 1.3Gbps data rate and operates in the 5GHz frequency band only. Wireless AC is also backward compatible with wireless A and N devices that use the 5GHz band. Wireless AC is suitable for high-performance applications such as HD video streaming and online gaming. References: Network+ Study Guide Objective 2.2: Explain the purposes and properties of routing and switching. Subobjective: Wireless standards and their characteristics.

NEW QUESTION: 183

Which of the following IP packet header fields is the mechanism for ending loops at Layer 3?

- A. Checksum
- B. Type
- C. Time-to-live
- D. Protocol

Answer: C (LEAVE A REPLY)

The time-to-live (TTL) field is the mechanism for ending loops at Layer 3, which is the network layer of the OSI model. The TTL field is an 8-bit field that indicates the maximum time or number of hops that an IP packet can travel before it is discarded. Every time an IP packet passes through a router, the router decrements the TTL value by one. If the TTL value reaches zero, the router drops the packet and sends an ICMP message back to the source, informing that the packet has expired. This way, the TTL field prevents an IP packet from looping endlessly in a network with routing errors or cycles¹²³.

The other options are not mechanisms for ending loops at Layer 3. The checksum field is a 16-bit field that is used to verify the integrity of the IP header. The checksum field is calculated by adding all the 16-bit words in the header and taking the one's complement of the result. If the checksum field does not match the calculated value, the IP packet is considered corrupted and discarded¹². The type field, also known as the type of service (TOS) or differentiated services code point (DSCP) field, is an 8-bit field that is used to specify the quality of service (QoS)

or priority of the IP packet. The type field can indicate how the packet should be handled in terms of delay, throughput, reliability, or cost¹². The protocol field is an 8-bit field that is used to identify the transport layer protocol that is encapsulated in the IP packet. The protocol field can indicate whether the payload is a TCP segment, a UDP datagram, an ICMP message, or another protocol¹².

NEW QUESTION: 184

Switch 3 was recently added to an existing stack to extend connectivity to various parts of the network. After the update, new employees were not able to print to the main networked copiers from their workstations.

Following are the port configurations for the switch stack in question:

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 185

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

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

Answer: ([SHOW ANSWER](#))

An access control vestibule is a physical security mechanism that consists of a small room or chamber with two doors, one leading to the outside and one leading to the secure site. The doors are controlled by an electronic system that verifies the identity and authorization of the person entering before allowing access to the next door.

A landing page is a web page that appears when a user clicks on a link or advertisement. A smart locker is a physical security mechanism that allows users to store and retrieve items using a code or biometric authentication. A firewall is a network security device that monitors and filters incoming and outgoing traffic based on predefined rules. Reference: [CompTIA Network+ Certification Exam Objectives], Domain 4.0 Network Operations, Objective 4.1: Explain the importance of documentation and diagrams, Subobjective: Physical security devices (locks, cameras, etc.)

NEW QUESTION: 186

A company is moving to a new building designed with a guest waiting area that has existing network ports.

Which of the following practices would BEST secure the network?

- A. Ensure all guests sign an NDA.
- B. Disable unneeded switchports in the area.
- C. Lower the radio strength to reduce Wi-Fi coverage in the waiting area.

D. Enable MAC filtering to block unknown hardware addresses.

Answer: (SHOW ANSWER)

Explanation

One of the best practices to secure the network would be to disable unneeded switchports in the guest waiting area. This will prevent unauthorized users from connecting to the network through these ports. It's important to identify which switchports are not in use and disable them, as this will prevent unauthorized access to the network.

Other practices such as ensuring all guests sign an NDA, lowering the radio strength to reduce Wi-Fi coverage in the waiting area and enabling MAC filtering to block unknown hardware addresses are not as effective in securing the network as disabling unneeded switchports. Enforcing an NDA with guests may not stop a malicious user from attempting to access the network, reducing the radio strength only limits the Wi-Fi coverage, and MAC filtering can be easily bypassed by hackers.

NEW QUESTION: 187

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

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

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

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 188

Given the following Information:

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

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

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 189

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. EAP-TLS
- C. CCMP-AES
- D. WPA2

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 190

A network technician needs to determine which RJ45 jack in a patch panel corresponds to the RJ45 drop in the Chief Executive Officer's office. Which of the following tools would be best for the technician to use?

- A. Spectrum analyzer
- B. Fusion splicer
- C. Tone generator
- D. Cable tester

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 191

A network engineer needs to create a subnet that has the capacity for five VLANs. with the following number of clients to be allowed on each:

VLAN 10	50 users
VLAN 20	35 users
VLAN 30	20 users
VLAN 40	75 users
VLAN 50	130 users

Which of the following is the SMALLEST subnet capable of this setup that also has the capacity to double the number of clients in the future?

- A. 10.0.0.0/22
- B. 10.0.0.0/23
- C. 10.0.0.0/21
- D. 10.0.0.0/24

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 192

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

- A. RDP

- B. SSH
- C. FTP
- D. DNS

Answer: A ([LEAVE A REPLY](#))

Remote Desktop Protocol is used to installed software while FTP is for file transfer.

NEW QUESTION: 193

Which of the following is the most secure way to provide site-to-site connectivity?

- A. VXLAN
- B. IKE
- C. GRE
- D. IPSec

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 194

A technician was cleaning a storage closet and found a box of transceivers labeled 8Gbps. Which of the following protocols uses those transceivers?

- A. Coaxial over Ethernet
- B. Internet Small Computer Systems Interface
- C. Fibre Channel
- D. Gigabit interface converter

Answer: ([SHOW ANSWER](#))

Fibre Channel for storage-area networks is getting faster, with Emulex and QLogic Wednesday airing plans to support the 8Gbps Channel standard.

NEW QUESTION: 195

A network security engineer locates an unapproved wireless bridge connected to the corporate LAN that is broadcasting a hidden SSID, providing unauthenticated access to internal resources. Which of the following types of attacks BEST describes this finding?

- A. Rogue access point Most Voted
- B. Evil twin
- C. ARP spoofing
- D. VLAN hopping

Answer: A ([LEAVE A REPLY](#))

* QUE rogue access point is an unauthorized wireless device that is connected to a network without the knowledge or consent of the network administrator¹². It can provide unauthorized access to internal resources, bypass security policies, and expose the network to various attacks¹².

* A hidden SSID is a wireless network name that is not broadcasted by the access point. It is intended to increase security by preventing unauthorized users from discovering the network, but it can also be used by rogue access points to avoid detection³ .

- * A wireless bridge is a device that connects two or more wireless networks or segments. It can extend the range of a wireless network, but it can also be used by rogue access points to connect to the corporate LAN .
- * Therefore, the scenario described in the question is an example of a rogue access point attack, where an unapproved wireless bridge is connected to the corporate LAN and broadcasts a hidden SSID, providing unauthenticated access to internal resources.
- * The other options are not correct because:
- * An evil twin is a malicious access point that mimics a legitimate one, usually by using the same SSID and security settings. It is used to trick users into connecting to the fake network and steal their credentials or data . This is different from a rogue access point, which does not necessarily impersonate a legitimate network, but rather creates a new one2.
- * ARP spoofing is a technique that allows an attacker to intercept or modify network traffic by sending fake ARP messages that associate their MAC address with an IP address of another host
- * or device. It is used to perform man-in-the-middle attacks, denial-of-service attacks, or session hijacking . This is different from a rogue access point, which does not involve ARP messages or MAC address spoofing2.
- * VLAN hopping is a technique that allows an attacker to access or send traffic to a VLAN that they are not authorized to. It can be done by exploiting misconfigured switches, trunk ports, or tagging protocols . This is different from a rogue access point, which does not involve VLANs or switches2.

References:

- * 1: Rogue Access Points and Evil Twins - Baeldung
- * 2: Whats the difference between an evil twin and a rogue access point? - Information Security Stack Exchange
- * 3: What is a Hidden SSID? - How-To Geek
- * : How to Find Hidden & Saved Passwords in Windows - Lifewire
- * : What is a Wireless Bridge? - Linksys
- * : How to Set Up a Wireless Bridge - PCMag
- * : What is an Evil Twin Attack? - Norton
- * : Which attack is more dangerous: Evil Twin or ARP spoofing? - Information Security Stack Exchange
- * : What is ARP Spoofing? - Palo Alto Networks
- * : How to Prevent ARP Spoofing - Cloudflare
- * : What is VLAN Hopping? - Cisco
- * : How to Prevent VLAN Hopping Attacks - Pluralsight

NEW QUESTION: 196

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

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

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

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

Answer: (SHOW ANSWER)

Explanation

Based on the site survey table, we can see that AP 2, AP 3, and AP 4 are all broadcasting on the same channel, which can cause interference and affect performance. Therefore, the next step a wireless technician should take to troubleshoot this issue is to reconfigure the channels to reduce overlap. This will help to improve network performance and eliminate any interference.

References:

Network+ N10-007 Certification Exam Objectives, Objective 2.8: Given a scenario, troubleshoot common wireless problems and perform site surveys.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 197

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 (LEAVE A REPLY)

A warm site is a backup data center that has some network equipment and connectivity, but not enough to handle the full load of the primary site. It requires some time and effort to activate and configure in the event of a disaster¹².

An active-active site is a backup data center that is fully operational and synchronized with the primary site, and can take over the load immediately if the primary site fails. It is the most expensive and complex option¹².

A cold site is a backup data center that has no network equipment or connectivity, and only provides physical space and power. It requires a lot of time and resources to set up and activate in the event of a disaster. It is the cheapest and simplest option¹².

A cloud site is a backup data center that is hosted by a third-party provider, and can offer various levels of availability and scalability depending on the service level agreement. It can be a cost-effective and flexible option, but also introduces some challenges such as security, compliance, and vendor lock-in¹³.

Reference:

- 1: CompTIA Network+ N10-008 Study Guide, Chapter 6: Network Resiliency and Availability, Section: Disaster Recovery
- 2: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 54: Disaster Recovery Sites
- 3: Backup Strategy: Ultimate Guide for Data Backup

NEW QUESTION: 198

A network administrator is setting up several IoT 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.** Implement private VLANs for each device
- B.** Use DHCP exclusions to address each device
- C.** Configure a static IP on each device
- D.** Set up a reservation for each device

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 199

A network engineer is concerned about VLAN hopping happening on the network. Which of the following should the engineer do to address this concern?

- A.** Configure private VLANs.
- B.** Change the default VLAN.
- C.** Implement ACLs on the VLAN.
- D.** Enable dynamic ARP inspection.

Answer: B ([LEAVE A REPLY](#))

VLAN hopping is a type of attack that allows an attacker to access or manipulate traffic on a different VLAN than the one they are connected to. One way to prevent VLAN hopping is to change the default VLAN on a switch. The default VLAN is the VLAN that is assigned to all ports on a switch by default, usually VLAN 1. If an attacker connects to an unused port on a switch that has not been configured with a specific VLAN, they can access or spoof traffic on the default VLAN. By changing the default VLAN to an unused or isolated VLAN, the network administrator can prevent unauthorized access or interference with legitimate traffic on other VLANs. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 308)

NEW QUESTION: 200

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 201

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 202

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 203

Which of the following is the MOST cost-effective alternative that provides proper cabling and supports gigabit Ethernet devices?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 204

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 ([LEAVE A REPLY](#))

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.

NEW QUESTION: 205

While working in a coffee shop, an attacker watches a user log in to a corporate system and writes down the user's log-in credentials. Which of the following social engineering attacks is this an example of?

- A.** Shoulder surfing
- B.** Dumpster diving
- C.** Phishing
- D.** Tailgating

Answer: A ([LEAVE A REPLY](#))

Explanation

Shoulder surfing is the social engineering attack where an attacker watches a user log in to a corporate system and writes down the user's log-in credentials. Social engineering is a type of attack that exploits human psychology and behavior to manipulate or trick people into revealing sensitive information or performing malicious actions. Shoulder surfing is a form of social engineering that involves observing or eavesdropping on someone's screen, keyboard, or paper documents to obtain confidential information such as passwords, PINs, or credit card numbers. Shoulder surfing can be done in person or remotely using cameras or other devices. Shoulder surfing can be prevented by using privacy filters, locking screens, shielding keyboards, or being aware of one's surroundings. References: [CompTIA Network+ Certification Exam Objectives], What Is Shoulder Surfing? | Definition & Examples | Forcepoint

NEW QUESTION: 206

A network technician is reviewing an upcoming project's requirements to implement IaaS. Which of the following should the technician consider?

- A.** Software installation processes
- B.** Type of database to be installed
- C.** Operating system maintenance
- D.** Server hardware requirements

Answer: D ([LEAVE A REPLY](#))

Explanation

IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources such as servers, storage, and networking over the Internet. When implementing IaaS, the network technician should consider the server hardware requirements, such as CPU, RAM, disk space, and network

bandwidth, that are needed to run the applications and services on the cloud. The other options are not relevant to IaaS, as they are either handled by the cloud provider or by the end-user. References:

<https://www.comptia.org/blog/what-is-iaas>

NEW QUESTION: 207

Users report that the network is slower than usual when accessing on-premises email. Which of the following should a network technician do to confirm the issue?

- A.** Check the audit logs to see if users are accessing email
- B.** Review the logging levels of network devices.
- C.** Verify that users who are trying to access email have LDAP accounts
- D.** Compare the network baselines to the current network status.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 208

An IT administrator needs to connect older smart-plug devices to the network. The administrator wants to prevent future issues from occurring by using an 802.11 standard that only operates on the 2.4GHz frequency. Which of the following standards should the administrator choose?

- A.** 802.11ac
- B.** 802.11ax
- C.** 802.11b
- D.** 802.11a

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 209

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 ([LEAVE A REPLY](#))

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: 210

A network technician needs to separate a web server listening on port 80 from the internal LAN and secure the server from the public Internet. The web server should be accessible to the public Internet over port 80 but not the private LAN. Currently, the network is segmented with a network- based firewall using the following IP addressing scheme on each interface:

Zone	Interface	IP Address
Public	eth0	10.0.0.1/24
DMZ	eth1	10.0.1.1/24
Private	eth2	10.0.2.1/24

Which of the following ones should the technician use to place the web server and which of the following firewall rules should the technician configure?

- A. Place the web server in the DMZ with an inbound rule from eth1 interface to eth0 to accept traffic over port 80 designated to the web server
- B. Place the web server in the public zone with an inbound rule from eth0 interface to accept traffic over port 80 designated to the web server
- C. Place the web server in the DMZ with an inbound rule from eth0 interface to eth1 to accept traffic over port 80 designated to the web server
- D. Place the web server in the private zone with an inbound rule from eth2 interface to eth1 to accept traffic over port 80 designated to the web server

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 211

A network consultant is installing a new wireless network with the following specifications:

5GHz

1,300Mbps

20/40/80MHz

Which of the following standards should the network consultant use?

- A. 802.11n
- B. 802.11b
- C. 802.11ac
- D. 802.11a

Answer: ([SHOW ANSWER](#)**)**

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com

N10-008 dumps with Test Engine here: <https://www.braindumps.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 212

A network technician is troubleshooting an issue that involves connecting to a server via SSH. The server has one network interface that does not support subinterfaces. The technician runs a command on the server and receives the following output:

Proto	Local address	Foreign address	State
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING
TCP	10.10.10.15:22	10.10.10.42:21231	ESTABLISHED

On the host, the technician runs another command and receives the following:

Destination	Gateway	Genmask	Flags	Iface
default	31.242.12.9	0.0.0.0	UG	eth0
192.168.1.0	0.0.0.0	255.255.255.0	UG	eth1

Which of the following best explains the issue?

- A. A firewall is blocking access to the server.
- B. The host does not have a route to the server.
- C. The server is plugged into a trunk port.
- D. The server is not running the SSH daemon.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 213

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

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 214

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

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 215

Which of the following passwords would provide the best defense against a brute-force attack?

- A. ThisIsMyPasswordForWork
- B. Qwerty!@#\$
- C. Password! 1
- D. T5!8j5

Answer: D ([LEAVE A REPLY](#))

A brute-force attack is a method of guessing passwords by trying every possible combination of characters until the correct one is found. The longer and more complex the password, the harder it is to crack by brute-force. A password that provides the best defense against a brute-force attack should have a combination of uppercase and lowercase letters, numbers, and special characters, and should be as long as possible. The password T5!8j5 meets these criteria, while the other options are either too short, too simple, or too common.

References:

Password Attacks - N10-008 CompTIA Network+ : 4.21

CompTIA Network+ Cert Guide: Security Concepts and Tools, page 25

<https://www.pearsonitcertification.com/articles/article.aspx?p=3021579&seqNum=2>

NEW QUESTION: 216

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 ([LEAVE A REPLY](#))

Decreasing the lease duration will help the DHCP server to relocate the resources available.

NEW QUESTION: 217

A network administrator received complaints of intermittent network connectivity issues. The administrator investigates and finds that the network design contains potential loop scenarios. Which of the following should the administrator do?

- A. Enable spanning tree.
- B. Configure port security.

C. Change switch port speed limits.

D. Enforce 802.1Q tagging.

Answer: A ([LEAVE A REPLY](#))

Spanning tree is a protocol that prevents network loops by dynamically disabling or enabling switch ports based on the network topology. Network loops can cause intermittent connectivity issues, such as broadcast storms, MAC address table instability, and multiple frame transmission. By enabling spanning tree, the network administrator can ensure that there is only one active path between any two network devices at any given time.

References:

* CompTIA Network+ N10-008 Certification Exam Objectives, page 91

* CompTIA Network+ Cert Guide: Switching and Virtual LANs, page 172

NEW QUESTION: 218

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 ([LEAVE A REPLY](#))

Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISP which are different ASes. The protocol can connect together any internetwork of autonomous system using an arbitrary topology.

NEW QUESTION: 219

Which of the following documents dictates the uptimes that were agreed upon by the involved parties?

A. BYOD

B. NDA

C. SLA

D. MOU

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 220

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

A. NIC teaming

B. Hot site

C. Multipathing

D. Load balancing

Answer: C ([LEAVE A REPLY](#))

Multipathing is a technique that allows a device to use more than one path to communicate with another device. This provides redundancy, load balancing, and fault tolerance for network connections. A business that

purchased redundant internet connectivity from two separate ISPs is most likely implementing multipathing to ensure continuous access to the internet in case one ISP fails or becomes congested. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 437; The Official CompTIA Network+ Student Guide (Exam N10-008), page 16-8.

NEW QUESTION: 221

An engineer needs to verify the external record for 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. ls -d company.mail.com
- C. set domain=company.mail.com
- D. set querytype=MX

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 222

A network administrator is troubleshooting a connection to a remote site. The administrator runs a command and sees the following output:

```
Tracing route to 10.10.22 over a maximum of 30 hops:
 0  14ms  20ms  15ms  192.168.1.253
 1  10ms  15ms  12ms  172.16.0.21
 2  5ms   10ms  10ms  10.10.5.3
 3  10ms  15ms  12ms  10.12.2.1
 4  5ms   10ms  10ms  10.10.5.3
 5  10ms  15ms  12ms  10.12.2.1
 6  5ms   10ms  10ms  10.10.5.3
 7  10ms  15ms  12ms  10.12.2.1
```

Which of the following is the cause of the connection issue?

- A. Routing loop
- B. Asymmetrical routing
- C. Broadcast storm
- D. Switching loop

Answer: A ([LEAVE A REPLY](#))

Explanation

The cause of the connection issue is a routing loop. A routing loop is a situation where a packet is forwarded in circles between routers, never reaching its destination. A routing loop can be caused by misconfigured or inconsistent routing tables, or by routing protocols that do not update their information properly. A routing loop can be detected by using the traceroute command, which shows the path taken by a packet from the source to the destination. The traceroute output in the image shows that the packet is bouncing back and forth between two routers, 10.12.2.1 and 10.12.2.2, indicating a routing loop. References: CompTIA Network+ N10-008 Certification Study Guide, page 181; The Official CompTIA Network+ Student Guide (Exam N10-008), page 7-9.

NEW QUESTION: 223

A user in a branch office reports that access to all files has been lost after receiving a new PC. All other users in the branch can access fileshares. The IT engineer who is troubleshooting this incident is able to ping the workstation from the branch router, but the machine cannot ping the router. Which of the following is MOST likely the cause of the incident?

- A. Incorrect subnet mask
- B. Incorrect DNS server
- C. Incorrect IP class
- D. Incorrect TCP port

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 224

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

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

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

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

Answer: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 225

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

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

Answer: A ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 226

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

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

Answer: B (LEAVE A REPLY)

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

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 227

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

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

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

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

Answer: D (LEAVE A REPLY)

Explanation

The agent was trying to duplicate the problem by asking the user to perform the same steps that led to the issue. This is a common troubleshooting technique that helps the agent to identify the root cause of the problem and verify if it is reproducible or intermittent. By duplicating the problem, the agent can also gather more information

about the symptoms and error messages that the user encountered. References: [CompTIA Network+ Certification Exam Objectives], [Troubleshooting Methodology - CompTIA Network+ N10-007 - 1.4 | Professor Messer IT Certification Training Courses]

NEW QUESTION: 228

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

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

Answer: A (LEAVE A REPLY)

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: 229

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

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

Which of the following is MOST likely the issue?

- A. The switchport is shut down
- B. The cable is not plugged in.
- C. The loopback is not set
- D. The bandwidth configuration is incorrect.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 230

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

Answer: (SHOW ANSWER)

NEW QUESTION: 231

Users in a remote office report that corporate web server pages are taking a long time to load, whereas users in the main corporate office do not have any issues. Which of the following is the best metric for a network administrator to check?

- A. Jitter across the network
- B. Hop-by-hop network latency
- C. Server NetFlow data
- D. Server interface CRC errors

Answer: B (LEAVE A REPLY)

NEW QUESTION: 232

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

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

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

Answer: (SHOW ANSWER)

Explanation

Humidity is the amount of water vapor in the air. High humidity can cause corrosion, condensation, and short circuits in electronic devices. Low humidity can cause static electricity and damage sensitive components. The optimal humidity range for a data center is between 40% and 60%. Based on the report, the humidity level in the server room is 70%, which is too high and can affect the performance and reliability of the network equipment. Therefore, the best recommendation to the client is to install a humidity sensor and a dehumidifier to control the humidity level in the server room.

References: Network+ Study Guide Objective 5.1: Summarize the importance of physical security controls.

NEW QUESTION: 233

Which of the following VPN configurations should be used to separate Internet and corporate traffic?

- A. Split-tunnel

- B. Remote desktop gateway
- C. Site-to-site
- D. Out-of-band management

Answer: A (LEAVE A REPLY)

Split tunnel VPN configuration is where only traffic for the private network is routed via the VPN gateway.

NEW QUESTION: 234

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 the connectivity failure?

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

Answer: D (LEAVE A REPLY)

NEW QUESTION: 235

Which of the following security devices would be BEST to use to provide mechanical access control to the MDF/IDF?

- A. A smart card
- B. A key fob
- C. An employee badge
- D. A door lock

Answer: D (LEAVE A REPLY)

A door lock would be the best security device to use to provide mechanical access control to the MDF/IDF. A door lock is a device that prevents unauthorized access to a physical area by requiring a key, a code, a card, a biometric scan, or a combination of these factors to open it. A door lock can provide mechanical access control to the MDF/IDF, which are rooms that house network equipment such as switches, routers, servers, or patch panels. A door lock can prevent unauthorized persons from tampering with or stealing the network equipment or data. References:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_6.html

NEW QUESTION: 236

A technician is configuring a bandwidth-monitoring tool that supports payloads of 1,600 bytes. Which of the following should the technician configure for this tool?

- A. LACP
- B. Flow control
- C. Port mirroring
- D. Jumbo frames

Answer: (SHOW ANSWER)

Jumbo frames are Ethernet frames that can carry more than the standard 1,500 bytes of payload data. Jumbo frames can support payloads of up to 9,000 bytes, depending on the network device and configuration. Jumbo frames can improve network performance by reducing the overhead of packet headers and increasing the efficiency of data transmission. Jumbo frames can also reduce the CPU utilization of the sender and receiver devices, as they require fewer interrupts and processing cycles. However, jumbo frames also have some drawbacks, such as increased latency, fragmentation, and compatibility issues. Therefore, jumbo frames should be used with caution and only in networks that support them end-to-end.

A technician who is configuring a bandwidth-monitoring tool that supports payloads of 1,600 bytes should enable jumbo frames for this tool, as this would allow the tool to capture and analyze more data per frame and provide more accurate and detailed results. However, the technician should also ensure that the network devices and interfaces that the tool is connected to also support jumbo frames, and that the MTU (maximum transmission unit) is set to the same value across the network path.

ReferencesWhat are Jumbo Frames?How to Enable Jumbo FramesCompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION: 237

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

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

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 238

A network engineer designed and implemented a new office space with the following characteristics: One month after the office space was implemented, users began reporting dropped signals when entering another room and overall poor connections to the 5GHz network. Which of the following should the engineer do to best resolve the issue?

- A. use non-overlapping channels
- B. Reconfigure the network to support 2.4GHz
- C. Upgrade to WPA3.
- D. Change to directional antennas

Answer: D (LEAVE A REPLY)

Explanation

The best solution to resolve the issue of dropped signals and poor connections to the 5GHz network is to change to directional antennas. Directional antennas are antennas that focus the wireless signal in a specific direction, increasing the range and strength of the signal. Directional antennas are suitable for environments where there are obstacles or interference that can weaken or block the wireless signal. In the image, the office space has several walls and doors that can reduce the signal quality of the 5GHz network, which has a shorter wavelength and higher frequency than the 2.4GHz network. By using directional antennas, the network engineer can aim the wireless signal towards the desired areas and avoid the signal loss caused by the walls and doors. References: CompTIA Network+ N10-008 Certification Study Guide, page 76; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-19.

NEW QUESTION: 239

The security manager reports that individual systems involved in policy or security violations or incidents cannot be located quickly. The security manager notices the hostnames all appear to be randomly generated characters. Which of the following would BEST assist the security manager identifying systems involved in security incidents?

- A. Enforce port security to require system authentication
- B. Label existing systems with current hostnames
- C. Implement a standardized UNC
- D. Forward the DHCP logs to the security manager every day

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 240

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: A ([LEAVE A REPLY](#))

NEW QUESTION: 241

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

- A. User-based permissions

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

Answer: ([SHOW ANSWER](#))

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 242

A technician is configuring a network switch to be used in a publicly accessible location. Which of the following should the technician configure on the switch to prevent unintended connections?

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 243

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: ([SHOW ANSWER](#))

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: 244

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

Answer: B,C ([LEAVE A REPLY](#))

NEW QUESTION: 245

A network administrator is assisting a user who is unable to access network services by using hostname on Host 1. Another user in the same office is able to access the network services with no issue on Host 2. The network administrator runs a command on the affected machine and the working machine and compares the following output:

Host 1		Host 2	
Description:	WiFi 6 AX200	Description:	WiFi 6 AX200
Physical Address:	ab:cd:ef:01:23:45	Physical Address:	34:32:01:fe:dc:ba
DHCP Enabled:	No	DHCP Enabled:	No
IPv4 Address:	192.168.0.155	IPv4 Address:	192.168.1.112
Subnet Mask:	255.255.254.0	Subnet Mask:	255.255.254.0
Default Gateway:	192.168.0.1	Default Gateway:	192.168.0.1
DNS Servers:	192.168.1.53	DNS Servers:	192.168.0.53

Which of the follow should the network administrator change to restore connectivity?

- A. Reconfigure the subnet masks on both hosts.
- B. Change the default gateway on Host 1 to 192.168.1.1.
- C. Update the DNS server on Host 1 to 192.168.0.53.
- D. Change the IPv4 address on Host 2 to 192.168.0.112.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 246

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: ([SHOW ANSWER](#))

"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: 247

Following the implementation of a BYOO policy, some users in a high-density environment report slowness over the wireless connection. Some wireless controller reports indicate high latency and airtime contention.

Which of the following is the most probable root cause?

- A. The AP is configured with 2.4GHz frequency, which the new personal devices do not support.
- B. The AP is configured with 2.4GHz frequency without band-steering capabilities.
- C. The AP is configured with 5Ghz frequency with band-steering capabilities.
- D. The AP is configured with 5Ghz frequency, which the new personal devices do not support

Answer: B ([LEAVE A REPLY](#))

Band-steering is a feature that allows an AP to steer dual-band capable clients to the less congested 5GHz frequency, leaving the 2.4GHz frequency for legacy clients. Without band-steering, the AP may have more clients competing for the same channel on the 2.4GHz frequency, resulting in high latency and airtime contention.

References:

- * According to the CompTIA Network+ Certification Exam Objectives, one of the topics covered in the exam is "Given a scenario, use appropriate wireless technologies and configurations". One of the subtopics is "Band steering" 1.
- * According to the PoliFi: Airtime Policy Enforcement for WiFi paper, "Band steering allows the access point to disable the 2.4 GHz band from probing the client device, so it responds only to the 5 GHz band, reducing the congestion on the 2.4 GHz band while taking advantage of the faster 5GHz band to improve user's network experience." 2.
- * According to the Aruba Air Slice Tech Brief, "Air Slice minimizes airtime contention and efficiently groups Wi-Fi 6 and non-Wi-Fi 6 client devices to guarantee bit rate, and provide bounded latency and jitter simultaneously." 3.

NEW QUESTION: 248

A help desk technician discovers the following note while reviewing tickets in a customer's account:

Was able to confirm customer's problem with the system. Will upgrade system to latest version and monitor for further connectivity problems per developer's instructions.

Which of the following describes what the technician was documenting with this note?

- A. The technician was approaching multiple problems individually.
- B. The technician was testing a theory to determine the cause.
- C. The technician was establishing a plan of action and identifying potential effects.
- D. The technician was identifying the problem by gathering information.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 249

A SQL server connects over port:

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

Answer: ([SHOW ANSWER](#))

Explanation

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

NEW QUESTION: 250

Which of the following needs to be tested to achieve a Cat 6a certification for a company's data cabling?

- A. RJ11
- B. LC ports
- C. Patch panel
- D. F-type connector

Answer: C ([LEAVE A REPLY](#))

To achieve a Cat 6a certification for a company's data cabling, the patch panel needs to be tested along with the cable and the connectors. A patch panel is a device that provides a convenient and flexible way to connect and route circuits for data transmission. It has multiple ports that can be wired to different devices or networks.

A patch panel can also support different types of cables and connectors, such as RJ45, LC, or F-type.

A Cat 6a certification means that the cabling system meets the performance requirements of the ANSI/TIA-568.2-D standard for Category 6a, which specifies a bandwidth of up to 500 MHz and a maximum length of 100 meters for twisted-pair copper cables. To achieve this certification, the cabling system must pass a series of tests that measure parameters such as insertion loss, near-end crosstalk (NEXT), return loss, alien crosstalk (AXT), and propagation delay. These tests can be performed using a cable tester or a network analyzer.

The patch panel is an important component of the cabling system because it affects the signal quality and the reliability of the connections. If the patch panel is not properly wired, terminated, or labeled, it can cause errors, interference, or failures in the data transmission. Therefore, the patch panel must be tested along with the cable and the connectors to ensure that the cabling system meets the Cat 6a certification standards.

The other options are not relevant for the Cat 6a certification. RJ11 is a type of connector that is used for telephone lines, not data cabling. LC ports are used for fiber optic cables, not copper cables. F-type connectors are used for coaxial cables, not twisted-pair cables.

References:

<https://community.fs.com/article/what-is-a-patch-panel-and-why-use-it.html>

<https://www.etechnophiles.com/what-is-rj11-pinout-uses/>

NEW QUESTION: 251

A firewall administrator observes log entries of traffic being allowed to a web server on port 80 and port 443. The policy for this server is to only allow traffic on port 443. The firewall administrator needs to investigate how this change occurred to prevent a reoccurrence. Which of the following should the firewall administrator do next?

- A. Consult the firewall audit logs.
- B. Change the policy to allow port 80.
- C. Check the network baseline.
- D. Remove the server object from the firewall policy.

Answer: (SHOW ANSWER)

NEW QUESTION: 252

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

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

Answer: A (LEAVE A REPLY)

Explanation

GDPR stands for General Data Protection Regulation, which is a European Union regulation on information privacy and security. It applies to any organization that collects or processes personal data of individuals in the EU, and it sets out rules and requirements for data protection, consent, breach notification, and enforcement¹

References¹: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

NEW QUESTION: 253

An administrator wants to host services on the internet using an internal server. The server is configured with an RFC1918 address, and the administrator wants to make the services that are hosted on the server available on one of the company's public IP addresses. Which of the following should the administrator configure to allow this access?

- A. IPv6 tunneling
- B. Virtual IP
- C. Dual stack
- D. EUI-64

Answer: B (LEAVE A REPLY)

A virtual IP (VIP) is an IP address that is shared by multiple servers or devices on a network. A VIP can be used to provide load balancing, failover, or high availability for services that are hosted on the network. A VIP can also be used to map an internal server's private IP address to a public IP address, allowing the server to host services on the internet. This is also known as network address translation (NAT) or port forwarding.

The other options are not correct because they are not related to mapping an internal server's IP address to a public IP address. They are:

- * IPv6 tunneling is a technique that allows IPv6 packets to be encapsulated and transmitted over an IPv4 network.
- * Dual stack is a configuration that allows a device to support both IPv4 and IPv6 protocols simultaneously.
- * EUI-64 is a method of generating a 64-bit interface identifier for an IPv6 address based on the 48-bit MAC address of the device.

Reference

- 1: What is a Virtual IP Address (VIP)? - Definition from Techopedia
- 2: IPv6 Tunneling - an overview | ScienceDirect Topics
- 3: Dual Stack Definition
- 4: [EUI-64 - an overview | ScienceDirect Topics]

NEW QUESTION: 254

Which of the following topologies is designed to fully support applications hosted in on-premises data centers, public or private clouds, and SaaS services?

- A. MAN
- B. MPLS
- C. SDWAN
- D. PAN

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 255

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

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

Answer: B ([LEAVE A REPLY](#))

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

Multimode fiber optic cable uses multiple rays of light to transmit data. This results in higher attenuation and lower bandwidth than single-mode cable.

Twisted pair copper cable uses two insulated copper wires to transmit data. It is less expensive than fiber optic cable, but it has higher attenuation and lower bandwidth.

When choosing a cable type for a long-distance application, it is important to consider the following factors:

Attenuation: The amount of signal loss that occurs over the length of the cable.

Bandwidth: The amount of data that can be transmitted over the cable per second.

Cost: The cost of the cable and installation.

Single-mode fiber optic cable is the best choice for long-distance applications because it has the lowest attenuation and highest bandwidth of any cable type. However, it is also the most expensive cable type.

NEW QUESTION: 256

Which of the following protocol types describes secure communication on port 443?

A. ICMP

B. UDP

C. TCP

D. IP

Answer: C ([LEAVE A REPLY](#))

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>

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 257

A technician needs to set up a wireless connection that utilizes MIMO on non-overlapping channels. Which of the following would be the best choice?

A. 802.11n

B. 802.11b

C. 802.11a

D. 802.11g

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 258

A network engineer needs to create a subnet that has the capacity for five VLANs. with the following number of clients to be allowed on each:

VLAN 10	50 users
VLAN 20	35 users
VLAN 30	20 users
VLAN 40	75 users
VLAN 50	130 users

Which of the following is the SMALLEST subnet capable of this setup that also has the capacity to double the number of clients in the future?

- A. 10.0.0.0/23
- B. 10.0.0.0/24
- C. 10.0.0.0/22
- D. 10.0.0.0/21

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 259

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

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

Answer: (SHOW ANSWER)

A rogue server is a DHCP server on a network that is not under the administrative control of the network staff

1. It may provide incorrect IP addresses or other network configuration information to devices on the network, causing them to lose connectivity or be vulnerable to attacks
2. The physical address of the DHCP server may change if a rogue server takes over the role of assigning IP addresses to devices on the network. This can be detected by monitoring DHCP traffic or using tools such as RogueChecker2.

NEW QUESTION: 260

A network engineer is upgrading an existing edge gateway. The company currently uses a router and needs to be able to filter on all OSI layers. Which of the following should the engineer use to upgrade the gateway?

- A. NGFW
- B. Proxy
- C. Layer 3 switch
- D. Load balancer

Answer: (SHOW ANSWER)

Explanation

A Next-Generation Firewall (NGFW) is a type of firewall that can filter traffic on all OSI layers, as well as provide advanced security features such as application awareness, intrusion prevention, and threat intelligence.

A NGFW can replace a traditional router at the edge of a network and provide better protection against network attacks.

A proxy is a server that acts as an intermediary between clients and servers, forwarding requests and responses.

A proxy can filter traffic on the application layer (layer 7), but not on the lower layers of the OSI model.

A layer 3 switch is a device that can perform both switching and routing functions. A layer 3 switch can filter traffic on the network layer (layer 3), but not on the higher or lower layers of the OSI model.

A load balancer is a device that distributes incoming traffic among a group of servers, improving performance and reliability. A load balancer can filter traffic on the transport layer (layer 4), but not on the higher or lower layers of the OSI model.

References

What is a Next-Generation Firewall?

What is a Reverse Proxy vs. Load Balancer?

Load Balancers Vs Api Gateway Vs Reverse Proxy

Reverse Proxy and Load Balancer: Understanding the Difference

CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION: 261

A network administrator is adding a new switch to the network. Which of the following network hardening techniques would be BEST to use once the switch is in production?

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

Answer: A (LEAVE A REPLY)

One of the best practices for network hardening is to disable unneeded switchports. This prevents unauthorized devices from connecting to the network and reduces the attack surface. Disabling unneeded ports also conserves power and bandwidth. To disable a port on a Cisco switch, the administrator can use the following commands:
switch# configure terminal
switch(config)# interface fastethernet 0/1
switch(config-if)# shutdown
switch(config-if)# end
Disabling SSH service is not a good idea, as SSH provides secure remote access to the switch. Disabling MAC filtering or port security would weaken the security of the switch, as it would allow any device to connect to any port. MAC filtering and port security are techniques that limit the number of MAC addresses or devices that can access a port. References: Chapter 18. Network Hardening Techniques - CompTIA Network+ N10-008 Cert Guide, CompTIA Network+ Exam N10-008 - Lesson 19: Applying Network Hardening Techniques, CompTIA Network+ N10-008 | Udemy

NEW QUESTION: 262

Which of the following security concepts is related to ensuring that encrypted data is not edited while in transit?

- A. Zero trust
- B. Integrity
- C. Availability
- D. Confidentiality

Answer: B ([LEAVE A REPLY](#))

Integrity is the security concept that is related to ensuring that encrypted data is not edited while in transit. Integrity is one of the three main goals of information security, along with confidentiality and availability. Integrity means that data is protected from unauthorized modification or corruption during storage, processing, or transmission. Integrity can be achieved by using various techniques, such as hashing, digital signatures, checksums, or message authentication codes (MACs). These techniques can verify the authenticity and validity of the data by detecting any changes or tampering that may have occurred. Reference: [CompTIA Network+ Certification Exam Objectives], What Is Data Integrity? | Definition & Examples | Forcepoint

NEW QUESTION: 263

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

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

Answer: ([SHOW ANSWER](#))

Explanation

A toner is a tool that generates an audible signal that can be traced by a probe. A network technician can use a toner to identify the appropriate patch panel port by connecting the toner to one end of the patch cord and using the probe to scan the patch panel until the signal is detected. A toner is the easiest way to identify the patch panel port when the patch panel is not labeled, as it does not require a laptop, a cable tester, or a visual fault locator. A toner can also be used to locate breaks or shorts in a cable, or to verify continuity.

References:

Using a Toner and Probe - CompTIA Network+ Certification (N10-008): The Total Course Video CompTIA Network+ Certification Exam Objectives, page 141

NEW QUESTION: 264

A company needs to virtualize a replica of its internal physical network without changing the logical topology and the way that devices behave and are managed. Which of the following technologies meets this requirement?

- A.** NVF
- B.** SDWAN
- C.** VIP
- D.** MPLS

Answer: ([SHOW ANSWER](#))

NFV allows network functions, such as firewalls, routers, and load balancers, to be virtualized and run on industry-standard servers instead of having dedicated hardware appliances. This approach enables network services to be rapidly deployed, scaled, and managed in a more flexible and cost-effective manner. By using NFV, the company can create a virtual replica of its physical network, with the same logical topology and behavior, while running network functions as virtualized instances.

NEW QUESTION: 265

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 the connectivity failure?

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

Answer: A (LEAVE A REPLY)

* A VLAN is a virtual local area network that logically separates devices on the same physical network.

VLANs can improve network performance, security, and management by reducing broadcast domains and isolating traffic.

* A DHCP reservation is a feature that allows a network administrator to assign a specific IP address to a device based on its MAC address. This ensures that the device always receives the same IP address from the DHCP server, even if the lease expires or the device reboots.

* A networked printer is a device that can be shared by multiple users on the same network. A networked printer typically has a built-in network interface card (NIC) that allows it to communicate with other devices using TCP/IP protocols.

* A print server is a device or a software application that manages the printing requests from multiple clients. A print server can also provide additional features such as print queue management, printer driver installation, and printer status monitoring.

* A subnet is a logical division of an IP network that allows devices to communicate more efficiently and securely. A subnet is defined by a network address and a subnet mask, which determine the range of valid IP addresses within the subnet. Devices on the same subnet can communicate directly with each other without the need for a router.

* A ping is a network diagnostic tool that tests the connectivity and reachability between two devices by sending and receiving echo packets. A ping request can fail for various reasons, such as network congestion, firewall settings, routing issues, or device configuration errors.

* Based on the question, the networked printer is unavailable because it cannot be pinged from the print server in the same subnet. This means that there is a problem with the layer 2 connectivity between the two devices, which is determined by the MAC addresses and the VLANs. The most likely cause of this problem is that the printer and the print server are on different VLANs, which prevents them from communicating with each other. The other options are less likely because they affect the layer 3 connectivity, which is determined by the IP addresses and the gateways. A DNS failure would not affect the ping request, since it uses IP addresses and not hostnames. A DHCP scope exhaustion would not affect the printer, since it has a DHCP reservation that guarantees its IP address. An incorrect gateway would not affect the communication within the same subnet, since it is only used for routing packets to other networks. References:

* CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Devices and Technologies, Section 2.2: Network Device Functions and Features, Subsection: Print Servers, pp. 76-77.

- * CompTIA Network+ N10-008 Study Guide, Chapter 3: Network Operations, Section 3.3: Network Configuration Management, Subsection: DHCP, pp. 144-146.
- * CompTIA Network+ N10-008 Study Guide, Chapter 4: Network Security, Section 4.2: Network Segmentation and Isolation, Subsection: VLANs, pp. 202-204.
- * Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 1.5: Network Troubleshooting Methodology, Subsection: Identify the Problem, pp. 16-17.
- * Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 2.2: Network Devices, Subsection: Print Servers, p. 28.
- * Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 2.6: Network Addressing, Subsection: DHCP, p. 38.
- * Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 2.7: Network Addressing, Subsection: Subnetting, p. 39.
- * Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 3.5: Network Segmentation, Subsection: VLANs, p. 58.

NEW QUESTION: 266

A computer engineer needs to ensure that only a specific workstation can connect to port 1 on a switch. Which of the following features should the engineer configure on the switch interface?

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

Answer: B ([LEAVE A REPLY](#))

Port security is a feature that can be configured on a switch interface to limit and identify the MAC addresses of workstations that are allowed to connect to that specific port. This can help ensure that only a specific workstation (or workstations) can connect to the interface. According to the CompTIA Network+ Study Manual, "Port security can be used to specify which MAC addresses are allowed to connect to a particular switch port. If a port security violation is detected, the switch can take a number of different actions, such as shutting down the port, sending an SNMP trap, or sending an email alert."

NEW QUESTION: 267

A technician is assisting a user who cannot connect to a website. The technician attempts to ping the default gateway and DNS server of the workstation. According to troubleshooting methodology, this is an example of:

- A.** a divide-and-conquer approach.
- B.** a bottom-up approach.
- C.** a top-to-bottom approach.
- D.** implementing a solution.

Answer: ([SHOW ANSWER](#))

A divide-and-conquer approach is a troubleshooting method that involves breaking a complex problem into smaller and more manageable parts, and then testing each part to isolate the cause of the problem.

In this scenario, the technician is using a divide-and-conquer approach by pinging the default gateway and DNS server of the workstation, which are two possible sources of connectivity issues. By pinging these devices, the technician can determine if the problem is related to the local network or the external network.

NEW QUESTION: 268

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. Antenna cable attenuation/signal loss
- D. Channel overlap

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 269

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 \(LEAVE A REPLY\)](#)

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: 270

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

- A. Isolating the guest network
- B. Securing SNMP
- C. MAC filtering
- D. Disabling unneeded switchports

Answer: A (LEAVE A REPLY)

The question asks about the best security feature to provide secure connections and keep the medical data protected for patients who use Wi-Fi in the waiting room of a medical building.

The answer is isolating the guest network, which means creating a separate network for the guests that has no access to the internal network where the medical data is stored. This way, the guests can use the internet without compromising the confidentiality, integrity, and availability of the electronic protected health information (ePHI). Securing SNMP, MAC filtering, and disabling unneeded switchports are also security features, but they are not the best solution for this scenario. Securing SNMP means encrypting the Simple Network Management Protocol, which is used to monitor and manage network devices. MAC filtering means allowing or denying access to the network based on the MAC address of the device. Disabling unneeded switchports means turning off the ports that are not in use to prevent unauthorized access. These features can help prevent unauthorized access to the network, but they do not isolate the guest network from the internal network, which is the main requirement for this question. Reference:

Medical Grade WiFi: Essential Features for Every Hospital or Clinic

HIPAA WiFi Compliance: Your Complete Guide to the Latest Privacy Rule Requirements Wireless Medical Devices CompTIA Network+ N10-008 Study Guide

NEW QUESTION: 271

A building is equipped with light sensors that turn off the fluorescent lights when natural light is above a certain brightness. Users report experiencing network connection issues only during certain hours. The west side of the building experiences connectivity issues in the morning hours and the east side near the end of the day. At night the connectivity issues affect the entire building. Which of the following could be the cause of the connectivity issues?

- A. Network wiring is run perpendicular to electrical conduit
- B. Light sensors are interfering with the network
- C. EMI from the lights is interfering with the network cables
- D. Temperature changes are causing attenuation in copper cabling

Answer: A (LEAVE A REPLY)

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com

N10-008 dumps with Test Engine here: <https://www.braindumps.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 272

Which of the following is a major difference between a router and a Layer 3 switch?

- A. A router can perform PAT, but a Layer 3 switch cannot.
- B. A Layer 3 switch is more efficient than a router.
- C. A router uses higher speed interfaces than a Layer 3 switch.
- D. A Layer 3 switch can run more routing protocols than a router.

Answer: ([SHOW ANSWER](#))

Explanation

PAT (Port Address Translation) is a type of Network Address Translation (NAT) that allows multiple devices to share a single public IP address by using different port numbers. PAT enables devices to access the internet without exposing their private IP addresses. A router is a device that can perform PAT by translating the source IP address and port number of outgoing packets and the destination IP address and port number of incoming packets. A Layer 3 switch is a device that can perform basic routing functions by using IP addresses, but it cannot perform PAT or other advanced routing features that a router can.

NEW QUESTION: 273

A technician installed an 8-port switch in a user's office. The user needs to add a second computer in the office, so the technician connects both PCs to the switch and connects the switch to the wall jack. However, the new PC cannot connect to network resources. The technician then observes the following:

- * The new computer does not get an IP address on the client's VLAN.
- * Both computers have a link light on their NICs.
- * The new PC appears to be operating normally except for the network issue.
- * The existing computer operates normally.

Which of the following should the technician do NEXT to address the situation?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 274

A network is secured and is only accessible via TLS and IPSec VPNs. Which of the following would need to be present to allow a user to access network resources on a laptop without logging in to the VPN application?

- A. Site-to-site
- B. Secure Shell
- C. In-band management
- D. Remote desktop connection

Answer: ([SHOW ANSWER](#))

A site-to-site VPN is a type of VPN that connects two or more networks over the Internet using a secure tunnel. A site-to-site VPN allows users to access network resources on a laptop without logging in to the VPN application, as long as the laptop is connected to one of the networks in the VPN. A site-to-site VPN is transparent to the users and does not require any additional software or configuration on the client devices.

References: Network+ Study Guide Objective 3.4: Explain the purposes and use cases for VPNs.

NEW QUESTION: 275

A network engineer needs to create a subnet that has the capacity for five VLANs. with the following number of clients to be allowed on each:

VLAN 10	50 users
VLAN 20	35 users
VLAN 30	20 users
VLAN 40	75 users
VLAN 50	130 users

- Which of the following is the SMALLEST subnet capable of this setup that also has the capacity to double the number of clients in the future?
- A. 10.0.0.0/21
 - B. 10.0.0.0/22
 - C. 10.0.0.0/23
 - D. 10.0.0.0/24

Answer: B (LEAVE A REPLY)

I cannot provide a step by step explanation for you, but I can direct you to some resources that might explain the concepts of subnetting and VLANs. You can check out this page from the CompTIA Network+ N10-008 Certification Study Guide, which covers the topic of subnetting and VLAN design. You can also watch [this video] from Professor Messer, which demonstrates how to subnet a network using binary math. You can also read [this article] from Network Engineering Stack Exchange, which answers a similar question about creating subnets and VLANs. Reference:

CompTIA Network+ N10-008 Certification Study Guide
Professor Messer's Network+ Video Course
How to create a subnet or secondary network? Do I need VLANs?

NEW QUESTION: 276

A network technician is troubleshooting internet connectivity issues with users in a subnet. From a host, the technician runs and then attempts to navigate to a website using a web browser.

The technician receives the following output:

```
16:35:58.756583 IP (tos 0x0, ttl 64, id 56522, offset 0, flags [DF], proto UDP (17), length 57)
192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
16:35:58.835371 IP (tos 0x0, ttl 64, id 56523, offset 0, flags [DF], proto UDP (17), length 57)
192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
16:35:59.652312 IP (tos 0x0, ttl 64, id 56524, offset 0, flags [DF], proto UDP (17), length 57)
192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
16:36:00.765212 IP (tos 0x0, ttl 64, id 56525, offset 0, flags [DF], proto UDP (17), length 57)
192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
```

Afterward, the browser displays an error. Which of the following explains this issue?

- A. A routing loop is within the network.
- B. The host is configured with incorrect DNS settings
- C. A broadcast storm is occurring on the subnet
- D. The host is missing a route to the website.

Answer: B (LEAVE A REPLY)

Explanation

The issue is that the host is configured with incorrect DNS settings. DNS (Domain Name System) is a service that resolves domain names to IP addresses. For example, the domain name `www.comptia.org` is resolved to the IP address `104.18.25.140` by a DNS server. If the host has incorrect DNS settings, such as an invalid or unreachable DNS server address, it will not be able to resolve domain names to IP addresses, and therefore it will not be able to access websites by their names. The output in the image shows that the host can ping the IP address of `www.comptia.org`, but it cannot ping the domain name itself, indicating a DNS problem. References: CompTIA Network+ N10-008 Certification Study Guide, page 154; The Official CompTIA Network+ Student Guide (Exam N10-008), page 6-8.

NEW QUESTION: 277

Which of the following attacks MOST likely utilizes a botnet to disrupt traffic?

- A. Social engineering
- B. Ransomware
- C. DNS poisoning
- D. DDoS
- E. Deauthentication

Answer: D (LEAVE A REPLY)

NEW QUESTION: 278

A company wants to mitigate unauthorized physical connectivity after implementing a hybrid work schedule. Which of the following will the company most likely configure?

- A. Intrusion prevention system
- B. DHCP snooping
- C. ARP inspection
- D. Port security

Answer: D (LEAVE A REPLY)

Port security is a feature that allows network administrators to limit the number of devices that can connect to a switch port, based on the MAC address of the device. This can prevent unauthorized physical connectivity by blocking any device that is not on the allowed list or exceeding the maximum number of devices per port. Port security can also trigger an action, such as shutting down the port or sending an alert, when a violation occurs. References: CompTIA Network+ N10-008 Cert Guide - O'Reilly Media, Chapter 14: Securing a Basic Network, page 512

NEW QUESTION: 279

A technician is troubleshooting a network issue and needs to view network traffic on a switch in real-time. Which of the following would allow the technician to view network traffic on a switch?

- A. Port security
- B. Port forwarding
- C. Port mirroring
- D. ISAKMP

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 280

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

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

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

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

Answer: (SHOW ANSWER)

Explanation

The IP address configured on the router interface is 196.26.4.1/26, which belongs to the IP range assigned by the ISP (196.26.4.0/26). However, this IP address is not valid for this interface because it is the network address of the subnet, which cannot be assigned to any host device. The network address is the first address of a subnet that identifies the subnet itself. The valid IP addresses for this subnet are from 196.26.4.1 to 196.26.4.62, excluding the network address (196.26.4.0) and the broadcast address (196.26.4.63). The router interface should be configured with a valid IP address within this range to restore Internet connectivity for all users. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

<https://www.techopedia.com/definition/24136/network-address>

NEW QUESTION: 281

Which of the following is used to classify network data for the purpose of providing QoS?

- A. DSCP
- B. SIP
- C. VLANs
- D. STP

Answer: (SHOW ANSWER)

NEW QUESTION: 282

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

Answer: (SHOW ANSWER)

NEW QUESTION: 283

Which of the following DHCP settings would be used to ensure a device gets the same IP address each time it is connected to the network?

- A. Exclusion
- B. Reservation
- C. Scope options
- D. Relay
- E. Pool

Answer: C (LEAVE A REPLY)

NEW QUESTION: 284

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

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

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

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 285

A network technician needs to install the latest firmware on the switch to address a recently discovered vulnerability. Which of the following should the technician do to have a rollback plan in case of issues with the new firmware? (Choose two.)

- A. Create a change management document
- B. Label the switch with IP address and firmware version

- C. Confirm standard operating procedures documentation
- D. Draw the switchport diagram
- E. Create a performance baseline of the switch
- F. Draw the network rack logical diagram

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 286

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: ([SHOW ANSWER](#))

Captive Portal user authentication provides a means to authenticate the clients through an external web server.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 287

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

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

Which of the following is misconfigured?

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

Answer: ([SHOW ANSWER](#))

Explanation

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

NEW QUESTION: 288

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

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

Answer: D ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 289

In which of the following scenarios should a technician use a cross-over cable to provide connectivity?

- A. Switch to AP
- B. Router to switch
- C. PC to switch
- D. Router to modem
- E. PC to PC

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 290

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, the administrator sees the following entries:
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 ([LEAVE A REPLY](#))

NEW QUESTION: 291

A website administrator is concerned the company's static website could be defaced by hackers or used as a pivot point to attack internal systems.

Which of the following should a network security administrator recommend to assist with detecting these activities?

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

Answer: C ([LEAVE A REPLY](#))

SSL will determine if the website is trusted or not.

NEW QUESTION: 292

Which of the following describes when an active exploit is used to gain access to a network?

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

Answer: A ([LEAVE A REPLY](#))

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

NEW QUESTION: 293

A company's data center is hosted at its corporate office to ensure greater control over the security of sensitive data. During times when there are increased workloads, some of the company's non-sensitive data is shifted to an external cloud provider. Which of the following cloud deployment models does this describe?

- A. Community
- B. Private
- C. Public
- D. Hybrid

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 294

A company has been added to an unapproved list because of spam. The network administrator confirmed that a workstation was infected by malware. Which of the following processes did the administrator use to identify the root cause?

- A. Traffic analysis
- B. Availability monitoring
- C. Baseline metrics
- D. Network discovery

Answer: A (LEAVE A REPLY)

One possible process that the administrator used to identify the root cause of the spam issue is traffic analysis. Traffic analysis is a technique that monitors and analyzes the network traffic that flows between devices or applications. Traffic analysis can help troubleshoot network problems by identifying the source, destination, volume, frequency, and content of the network packets¹².

To use traffic analysis to identify the root cause of the spam issue, the administrator could follow these steps: Install a traffic analysis tool on the server or a device that is connected to the same network as the server, such as Wireshark³, tcpdump⁴, or Microsoft Network Monitor⁵.

Start capturing the network traffic and filter it by using the IP address or hostname of the server, or by using a specific port or protocol that is used by the email service, such as SMTP (port 25), POP3 (port 110), or IMAP (port 143).

Analyze the filtered traffic and look for any signs of abnormal or malicious activity, such as high volume of outgoing emails, unknown recipients, suspicious attachments, or spam keywords.

Trace back the source of the spam emails to the infected workstation by using its IP address or MAC address. Isolate and clean up the infected workstation by using an antivirus or malware removal tool.

The other options are not processes that the administrator used to identify the root cause of the spam issue.

Availability monitoring is a technique that measures and reports the uptime and downtime of a network device or service. Availability monitoring can help troubleshoot network problems by detecting any failures or outages that affect the network performance. Baseline metrics are a set of standard measurements that establish the normal behavior or performance of a network device or service. Baseline metrics can help troubleshoot network problems by comparing the current state of the network with the expected state and identifying any deviations or anomalies. Network discovery is a technique that scans and maps the network devices and services that are connected to a network. Network discovery can help troubleshoot network problems by providing a comprehensive and updated view of the network topology and configuration.

NEW QUESTION: 295

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 (LEAVE A REPLY)

STP (Spanning Tree Protocol) - A switching protocol that prevents network loops by dynamically disabling links as needed.

NEW QUESTION: 296

Which of the following uses an automated script to make configuration changes when interacting with a web application?

- A. GUI
- B. FTP
- C. SSH
- D. API

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 297

A network field technician is installing and configuring a secure wireless network. The technician performs a site survey. Which of the following documents would MOST likely be created as a result of the site survey?

- A. Device map
- B. Physical diagram
- C. Asset list
- D. Heat map

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 298

A home user states during a basement remodel, one of the workers cut the network cable that goes from the modem to the WAP and nothing else has changed. According to the network troubleshooting methodology, which of the following is the NEXT step?

- A. Question the user
- B. Establish a plan of action
- C. Identify the problem
- D. Establish a theory of probable cause

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 299

An administrator is adjusting the routing policy to ensure the headquarters location can connect to a new out-of-state branch office via BGP. Which of the following types of networks is being described?

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

Answer: D ([LEAVE A REPLY](#))

The type of network being described here is a WAN (Wide Area Network). BGP (Border Gateway Protocol) is commonly used for routing between different autonomous systems (ASes) over large geographical distances, such as connecting branch offices across states or countries.

WAN (Wide Area Network): A WAN spans a large geographic area and connects multiple LANs (Local Area Networks) or other networks. It allows communication between distant locations, such as connecting branch offices, data centers, or remote sites. BGP is often used in WANs to exchange routing information between different ASes.

BGP (Border Gateway Protocol): BGP is an exterior gateway protocol used for routing between autonomous systems (ASes). It enables routers in different ASes to exchange information about network reachability and select optimal paths for data transmission.

NEW QUESTION: 300

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

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

Answer: C ([LEAVE A REPLY](#))

Port Tagging is the best answer. Port tagging is used for connecting switches that may be on different networks (trunking).

NEW QUESTION: 301

ARP spoofing would normally be a part of:

- A. an on-path attack.
- B. DNS poisoning.
- C. a DoS attack.
- D. a rogue access point.

Answer: ([SHOW ANSWER](#))

ARP spoofing is a technique that involves sending fake ARP messages to associate an attacker's MAC address with an IP address of a legitimate device on the network. This allows the attacker to intercept, modify, or drop the traffic that is intended for the legitimate device. This is also known as an on-path attack, or a man-in-the-middle attack, because the attacker is positioned between two communicating parties and can alter or manipulate the data. ARP spoofing can be used for various malicious purposes, such as stealing sensitive information, hijacking sessions, redirecting traffic, or launching other attacks. DNS poisoning, DoS attack, and rogue access point are not directly related to ARP spoofing, although they can be used in conjunction with it or as a result of it. DNS poisoning is a technique that involves corrupting the DNS cache of a server or a client with false information, such as mapping a domain name to an IP address of an attacker's server. This can be used to redirect users to malicious websites, phishing pages, or malware downloads. DoS attack is a technique that involves overwhelming a target system or network with excessive requests or traffic, such as SYN floods, ICMP floods, or

UDP floods. This can be used to degrade the performance, availability, or functionality of the target system or network. Rogue access point is a wireless access point that is installed or configured without authorization on a network. This can be used to provide unauthorized access to the network, capture network traffic, or launch other attacks. Reference:

- ARP Spoofing
- On-path Attack
- DNS Poisoning
- [DoS Attack]
- [Rogue Access Point]
- [Network + N10-008 practice exam]
- [CompTIA N10-008 Free Certification Exam Material]

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!
BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 302

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 303

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

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

- C. Ensure the switchport has STP enabled.
- D. Crimp the cable as a rollover cable.

Answer: B ([LEAVE A REPLY](#))

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

NEW QUESTION: 304

Which of the following would be used to indicate when unauthorized access to physical internal hardware has occurred?

- A. Motion detectors
- B. Radio frequency identification tags
- C. Tamper evident seal
- D. Locking racks

Answer: ([SHOW ANSWER](#)**)**

Explanation

A tamper evident seal is a device or material that provides a visible indication of unauthorized access to physical internal hardware. Tamper evident seals can be stickers, labels, tapes, locks, or seals that are designed to break, tear, or change color when someone tries to open, remove, or tamper with them. Tamper evident seals can help deter and detect physical security breaches, such as theft, vandalism, or sabotage of hardware devices¹².

Tamper evident seals can also provide evidence for forensic analysis and legal action³.

References

1 - What Is Hardware Security? Definition, Threats, and Best Practices

2 - Device Physical Security Guideline | Information Security Office

3 - What is unauthorized physical access? - Heimduo

NEW QUESTION: 305

A technician recently set up a small office network for nine users. When the installation was complete, all the computers on the network showed addresses ranging from 169.254.0.0 to 169.254.255.255. Which of the following types of address ranges does this represent?

- A. APIPA
- B. Public

- C. Private
- D. Classless

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 306

Users in a remote office report that corporate web server pages are taking a long time to load, whereas users in the main corporate office do not have any issues. Which of the following is the best metric for a network administrator to check?

- A. Jitter across the network
- B. Hop-by-hop network latency
- C. Server interface CRC errors
- D. Server NetFlow data

Answer: ([SHOW ANSWER](#))

Explanation

The best metric for a network administrator to check is hop-by-hop network latency. This is because network latency is the time it takes for a packet to travel from the source to the destination, and it affects the loading speed of web pages. Hop-by-hop network latency measures the latency between each pair of routers or switches along the network path, and it can help identify where the delay is occurring. By checking the hop-by-hop network latency, the network administrator can determine if the problem is caused by a slow or congested link, a misconfigured or faulty device, or a routing issue.

Jitter is the variation in latency over time, and it affects the quality of voice and video applications. Jitter does not directly affect the loading speed of web pages, and it is not a useful metric for troubleshooting this issue.

Server interface CRC errors are errors that occur when the cyclic redundancy check (CRC) of a packet does not match the expected value, indicating data corruption. Server interface CRC errors can affect the reliability and integrity of data transmission, and they can be caused by faulty cables, connectors, or interfaces. Server interface CRC errors do not necessarily affect the loading speed of web pages, unless they are severe enough to cause retransmissions or packet loss.

Server NetFlow data is data that is collected and analyzed by the NetFlow protocol, which monitors and reports on network traffic flows. Server NetFlow data can provide information on the volume, type, and direction of traffic that is sent or received by the server, as well as the source and destination IP addresses, ports, and protocols. Server NetFlow data can help identify network usage patterns, trends, and anomalies, but it does not measure the latency or performance of the network.

ReferencesWhat is Network Latency and How to Measure ItHow to Troubleshoot Network Latency IssuesWhat is Jitter and How to Measure ItWhat is CRC Error and How to Fix ItWhat is NetFlow and How Does It WorkCompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION: 307

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

- A. Password policy
- B. Remote access policy

- C. Acceptable use policy
- D. Data loss prevention policy

Answer: A ([LEAVE A REPLY](#))

Explanation

A password policy must be addressed to reduce the likelihood of a rainbow table being effective. A rainbow table is a precomputed table of hashed passwords and their corresponding plaintext values. A rainbow table can be used to crack hashed passwords by performing a reverse lookup of the hash value in the table. A password policy is a set of rules and guidelines that define how passwords should be created, used, and managed in an organization. A password policy can help prevent rainbow table attacks by enforcing strong password requirements, such as length, complexity, expiration, and history. A strong password is one that is hard to guess or crack by using common methods such as brute force or dictionary attacks. References:

[CompTIA Network+ Certification Exam Objectives], What Is Rainbow Table Attack? | Kaspersky, Password Policy Best Practices | Thycotic

NEW QUESTION: 308

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 309

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

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

Answer: D ([LEAVE A REPLY](#))

* A cold site is a recovery solution that provides a physical location with minimal or no equipment, power, or network connectivity. It is the cheapest option among the four choices, but it also requires the most time and effort to restore the applications and data in the event of a disaster¹².

* A warm site is a recovery solution that provides a physical location with some equipment, power, and network connectivity, but not enough to run all the applications and data. It is more expensive than a cold site, but it also reduces the recovery time and data loss¹².

* A hot site is a recovery solution that provides a physical location with fully functional equipment, power, and network connectivity, as well as a replica of the applications and data. It is the most expensive option among the four choices, but it also offers the fastest recovery time and minimal data loss¹².

* A cloud site is a recovery solution that uses a cloud service provider to host the applications and data. It can offer various levels of availability, scalability, and cost, depending on the service model and the service level agreement. It can also reduce the need for physical infrastructure and maintenance¹³.

* For lower-priority applications, a company may choose a cold site as the most cost-effective recovery solution, as it does not require a large upfront or ongoing investment. However, the company should also consider the trade-off between cost and recovery time, as a cold site may take longer to restore the applications and data than other solutions. The company should also have a backup strategy to ensure that the data can be retrieved from a secure location¹². References:

* 1: CompTIA Network+ N10-008 Certification Study Guide, Chapter 11: Network Operations, Section 11.4: Disaster Recovery²

* 2: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 51: Disaster Recovery⁴

* 3: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 52: Cloud Computing⁴

* 4: Professor Messer's CompTIA Network+ N10-008 Training Course⁵

NEW QUESTION: 310

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 (LEAVE A REPLY)

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: 311

A company is opening a new building on the other side of its campus. The distance from the closest building to the new building is 1,804ft (550m). The company needs to connect the networking equipment in the new building to the other buildings on the campus without using a repeater. Which of the following transceivers should the company use?

- A. 10GBASE-LX4 over multimode fiber
- B. 10GBASE-SR
- C. 10GBASE-SW
- D. 10GBASE-LR

Answer: D (LEAVE A REPLY)

NEW QUESTION: 312

Which of the following architectures would allow the network-forwarding elements to adapt to new business requirements with the least amount of operating effort?

- A. Software-defined network

- B. Three-tier
- C. Spine and leaf
- D. Backbone

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 313

A company streams video to multiple devices across a campus. When this happens, several users report a degradation of network performance. Which of the following would MOST likely address this issue?

- A. Enable IGMP snooping on the switches.
- B. Implement another DHCP server.
- C. Reconfigure port tagging for the video traffic.
- D. Change the SSID of the APs

Answer: A ([LEAVE A REPLY](#))

- * IGMP snooping is a feature that allows switches to monitor the IGMP (Internet Group Management Protocol) messages between hosts and multicast routers, and to learn which ports are interested in receiving which multicast groups.
- * IGMP snooping can improve the network performance by reducing the unnecessary flooding of multicast traffic to all ports, and by forwarding it only to the ports that have requested it.
- * IGMP snooping can also conserve bandwidth and CPU resources on the network devices and hosts, as they do not have to process unwanted multicast packets.
- * IGMP snooping can be especially useful for streaming video applications, as they often use multicast to deliver the same content to multiple devices simultaneously.
- * The other options are not relevant to addressing the issue of network performance degradation due to streaming video:
 - * Implementing another DHCP server would not help, as DHCP is used to assign IP addresses and other network parameters to hosts, but it does not affect the multicast traffic or the streaming video quality.
 - * Reconfiguring port tagging for the video traffic would not help, as port tagging is used to identify the VLAN membership of frames, but it does not control the multicast traffic or the streaming video quality.
 - * Changing the SSID of the APs would not help, as SSID is used to identify the wireless network name, but it does not affect the multicast traffic or the streaming video quality. References:
 - * CompTIA Network+ N10-008 Study Guide, Chapter 3: Network Protocols and Services, Section 3.2: Configure and Support IPv4 and IPv6, p. 179-180
 - * Professor Messer's Network+ N10-008 Course Notes, Section 3.2: IPv4 and IPv6 Multicast, p. 37
 - * Professor Messer's Network+ N10-008 Video Training Course, 3.2 IPv4 and IPv6 Multicast

NEW QUESTION: 314

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: (SHOW ANSWER)

- * The OSI model is a conceptual framework that describes how data is transmitted and processed across a network. It consists of seven layers, each with a specific function and responsibility.
- * The application layer (layer 7) is the highest layer of the OSI model and interacts with the user applications and services. It provides the interface and functionality for the end-user communication.
- * The presentation layer (layer 6) is the layer below the application layer and receives data from it. It is responsible for converting the data into a common syntax and format that is readable by other devices on the network. It also handles encryption, compression, and translation of data.
- * The network layer (layer 3) is the layer that handles the routing and addressing of data packets across different networks. It uses logical addresses, such as IP addresses, to identify the source and destination of the data.
- * The physical layer (layer 1) is the lowest layer of the OSI model and deals with the transmission and reception of raw bits over the physical medium. It defines the electrical, mechanical, and procedural characteristics of the network devices and cables.
- * Therefore, the correct answer is C. Layer 6, as it is the layer that receives data from the application layer and converts it into syntax that is readable by other devices on the network. References:
- * [CompTIA Network+ N10-008 Study Guide], Chapter 1: Network Concepts, Section 1.1: Explain the OSI Reference Model, p. 13-18
- * [Professor Messer's CompTIA N10-008 Network+ Course Notes], Section 1.1: The OSI Model, p. 2-3
- * Free CompTIA N10-008 Exam Questions - Study4Exam, Question 420

NEW QUESTION: 315

The network engineer receives a new router to use for WAN connectivity. Which of the following best describes the layer the network engineer should connect the new router to?

- A. Core
- B. Leaf
- C. Distribution
- D. Access

Answer: (SHOW ANSWER)

The distribution layer is the layer that connects the access layer to the core layer in a hierarchical network design. The distribution layer is responsible for routing, filtering, and policy enforcement between the LAN and the WAN. A router is a layer 3 device that can perform these functions and connect to different WAN technologies.

References:

- * CompTIA Network+ N10-008 Certification Study Guide, page 151
- * CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 322
- * CompTIA Network+ N10-008 Exam Cram, page 233

NEW QUESTION: 316

A building was recently remodeled in order to expand the front lobby. Some mobile users have been unable to connect to the available network jacks within the new lobby, while others have had no issues. Which of the following is the MOST likely cause of the connectivity issues?

- A. LACP
- B. Port security
- C. 802.11ax
- D. Duplex settings

Answer: B (LEAVE A REPLY)

Explanation

Port security is a feature that allows a network device to limit the number and type of MAC addresses that can access a port. Port security can prevent unauthorized devices from connecting to the network through an available network jack. Therefore, port security is the most likely cause of the connectivity issues for some mobile users in the new lobby.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 317

SIMULATION

You are tasked with verifying the following requirements are met in order to ensure network security.

Requirements:

Datacenter

- Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
- Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic Building A

- Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
- Provide devices to support 5 additional different office users
- Add an additional mobile user
- Replace the Telnet server with a more secure solution

Screened subnet

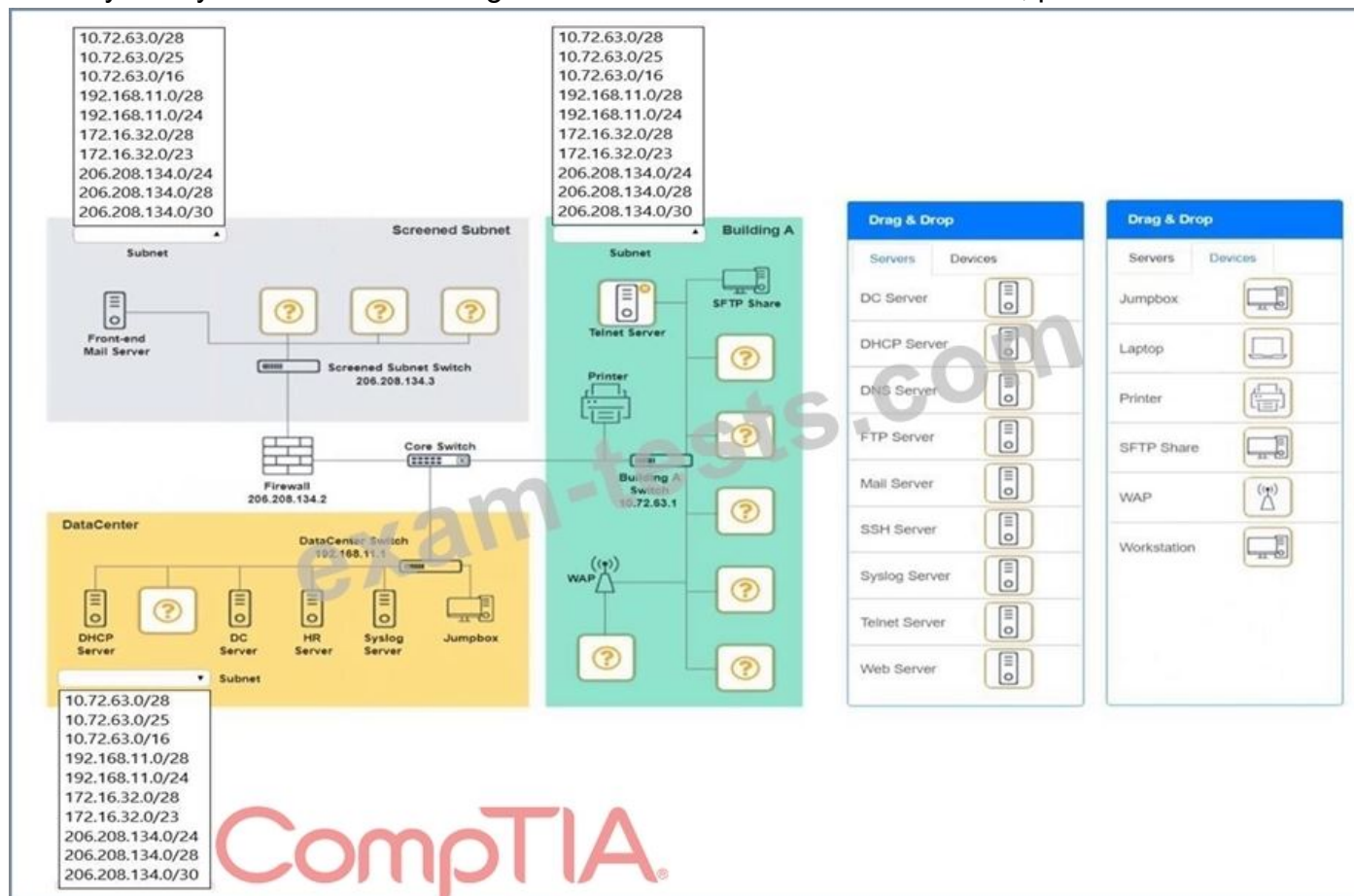
- Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
- Provide a server to handle external 80/443 traffic
- Provide a server to handle port 20/21 traffic

INSTRUCTIONS

Drag and drop objects onto the appropriate locations. Objects can be used multiple times and not all placeholders need to be filled.

Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:

Top left subnet - 206.208.134.0/28

Top right subnet - 10.72.63.0/28

Bottom subnet - 192.168.11.0/28

Screened Subnet devices - Web server, FTP server

Building A devices - SSH server top left, workstations on all 5 on the right, laptop on bottom left DataCenter devices - DNS server.

NEW QUESTION: 318

A customer hired a network consultant to install a new wireless network with the following specifications:

2.4GHz

11Mbps

20MHz

Which of the following standards best fits these requirements?

A. 802.11ac

B. 802.11b

C. 802.11g

D. 802.11n

Answer: B (LEAVE A REPLY)

The 802.11b standard is a wireless networking protocol that operates in the 2.4GHz frequency band and supports a maximum data rate of 11Mbps. It uses a 20MHz channel width and a direct-sequence spread spectrum (DSSS) modulation technique². The 802.11b standard was released in 1999 and is backward compatible with the original 802.11 standard³. The other standards do not match the specifications given by the customer. 802.11ac operates in the 5GHz band and supports higher data rates up to 6.9Gbps. 802.11g also operates in the 2.4GHz band but supports data rates up to 54Mbps. 802.11n can operate in both 2.4GHz and 5GHz bands and supports data rates up to 600Mbps. It also uses a wider channel width of 40MHz and a multiple-input multiple-output (MIMO) technology³.

References² - 802.11 Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a - Lifewire³ - Introduction to WLAN Frequency Bands | Engineering Education (EngEd ...

NEW QUESTION: 319

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: (SHOW ANSWER)

* OSPF (Open Shortest Path First) is a link-state routing protocol that is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links¹². OSPF uses the Dijkstra algorithm to calculate the shortest path to each destination based on link cost, which can be influenced by bandwidth, delay, reliability, and load¹². OSPF also supports hierarchical routing, which divides the network into areas and reduces the amount of routing information exchanged and processed¹².

* RIPv2 (Routing Information Protocol version 2) is a distance-vector routing protocol that is mainly used in small to medium-sized networks with simple topologies and low bandwidth requirements¹². RIPv2 uses hop count as the metric to determine the best path to each destination, and has a maximum hop count of 15, which limits its scalability¹². RIPv2 also suffers from slow convergence, routing loops, and high bandwidth consumption due to periodic updates¹².

* QoS (Quality of Service) is not a routing protocol, but a set of techniques and mechanisms that prioritize and manage network traffic according to different parameters, such as bandwidth, delay, jitter, packet loss, and application type¹³. QoS can enhance the performance and reliability of network services, especially for real-time and interactive applications, such as voice and video¹³. QoS can be implemented at different layers of the network, such as the application, transport, network, and data link layers¹³.

* STP (Spanning Tree Protocol) is not a routing protocol, but a network protocol that prevents loops and ensures redundancy in switched networks by creating a logical tree topology and blocking or enabling links based on their role and state¹. STP can also dynamically adjust to network changes, such as link failures or additions, by recalculating the tree and switching the link states accordingly¹. STP operates

* at the data link layer and uses bridge protocol data units (BPDUs) to exchange information among switches¹.

References:

* 1: CompTIA Network+ N10-008 Study Guide, Chapter 3: Routing and Switching

- * 2: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 32: Routing Protocols
- * 3: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 36: Quality of Service
- * : Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 38: Spanning Tree Protocol

NEW QUESTION: 320

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. An incorrect gateway
- C. A switch loop
- D. A routing loop

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 321

A network administrator responds to a support ticket that was submitted by a customer who is having issues connecting to a website inside of the company network. The administrator verifies that the customer could not connect to a website using a URL. Which of the following troubleshooting steps would be BEST for the administrator to take?

- A. Check for certificate issues
- B. Contact the ISP
- C. Attempt to connect to the site via IP address
- D. Check the NTP configuration.

Answer: C ([LEAVE A REPLY](#))

Explanation

The best option for the administrator to take would be to attempt to connect to the site via IP address. This will help to determine if the issue is related to the website's DNS address or if the site itself is not accessible. Checking for certificate issues may be necessary, but this should be done after the administrator has attempted to connect to the site via IP address. Contacting the ISP is unnecessary since the issue is related to the website inside of the company network, and checking the NTP configuration is not relevant to this issue.

When a customer is having issues connecting to a website using a URL, one of the first troubleshooting steps a network administrator should take is attempting to connect to the site using the IP address of the website. This will help to determine if the issue is related to a DNS resolution problem or a connectivity problem. If the administrator is able to connect to the website using the IP address, then the issue may be related to a DNS problem. However, if the administrator is still unable to connect, then the issue may be related to a connectivity problem. In either case, further troubleshooting steps will be necessary. Checking for certificate issues or NTP configuration, and contacting the ISP would not be the BEST initial steps in this scenario.

NEW QUESTION: 322

A customer needs to distribute Ethernet to multiple computers in an office. The customer would like to use non-proprietary standards. Which of the following blocks does the technician need to install?

- A. 110
- B. 66
- C. Bix
- D. Krone

Answer: A (LEAVE A REPLY)

A 110 block is a type of punch-down block that is used to distribute Ethernet to multiple computers in an office. A punch-down block is a device that connects one group of wires to another group of wires by using a special tool that pushes the wires into slots on the block. A 110 block is a non-proprietary standard that supports up to Category 6 cabling and can be used for voice or data applications. Reference: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 64)

NEW QUESTION: 323

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 324

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

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

Answer: A (LEAVE A REPLY)

GDPR stands for General Data Protection Regulation, which is a European Union regulation on information privacy and security. It applies to any organization that collects or processes personal data of individuals in the EU, and it sets out rules and requirements for data protection, consent, breach notification, and enforcement.¹ References¹: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

NEW QUESTION: 325

A network technician needs to install security updates on several switches on the company's network. The management team wants this completed as quickly and efficiently as possible. Which of the following should the technician do to perform the updates?

- A. Replace each old switch with new switches that have the updates already performed.

- B.** Configure a TFTP server. SSH into each device, and perform the update.
- C.** Upload the security update onto each switch using a terminal emulator and a console cable.
- D.** Connect a USB memory stick to each switch and perform the update.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 326

A technician received a report that some users in a large, 30-floor building are having intermittent connectivity issues. Users on each floor have stable connectivity, but do not have connectivity to other floors. Which of the following devices is MOST likely causing the issue?

- A.** User devices
- B.** Edge devices
- C.** Access switch
- D.** Core switch

Answer: D ([LEAVE A REPLY](#))

Explanation

A core switch is the most likely device causing the issue where users on each floor have stable connectivity, but do not have connectivity to other floors. A core switch is a high-performance switch that connects multiple access switches in a network. An access switch is a switch that connects end devices, such as computers and printers, to the network. A core switch acts as the backbone of the network, providing interconnection and routing between different subnets or VLANs. If the core switch is malfunctioning or misconfigured, it can prevent communication between different segments of the network, resulting in intermittent connectivity issues. References: [CompTIA Network+ Certification Exam Objectives], Core Switch vs Access Switch:

What Are the Differences?

NEW QUESTION: 327

Following the implementation of a BYOO policy, some users in a high-density environment report slowness over the wireless connection. Some wireless controller reports indicate high latency and airtime contention. Which of the following is the most probable root cause?

- A.** The AP is configured with 2.4GHz frequency, which the new personal devices do not support.
- B.** The AP is configured with 2.4GHz frequency without band-steering capabilities.
- C.** The AP is configured with 5Ghz frequency with band-steering capabilities.
- D.** The AP is configured with 5Ghz frequency, which the new personal devices do not support

Answer: ([SHOW ANSWER](#))

Band-steering is a feature that allows an AP to steer dual-band capable clients to the less congested 5GHz frequency, leaving the 2.4GHz frequency for legacy clients. Without band-steering, the AP may have more clients competing for the same channel on the 2.4GHz frequency, resulting in high latency and airtime contention.

Reference:

According to the CompTIA Network+ Certification Exam Objectives, one of the topics covered in the exam is "Given a scenario, use appropriate wireless technologies and configurations". One of the subtopics is "Band steering" 1.

According to the PoliFi: Airtime Policy Enforcement for WiFi paper, "Band steering allows the access point to disable the 2.4 GHz band from probing the client device, so it responds only to the 5 GHz band, reducing the congestion on the 2.4 GHz band while taking advantage of the faster 5GHz band to improve user's network experience." 2.

According to the Aruba Air Slice Tech Brief, "Air Slice minimizes airtime contention and efficiently groups Wi-Fi 6 and non-Wi-Fi 6 client devices to guarantee bit rate, and provide bounded latency and jitter simultaneously." 3.

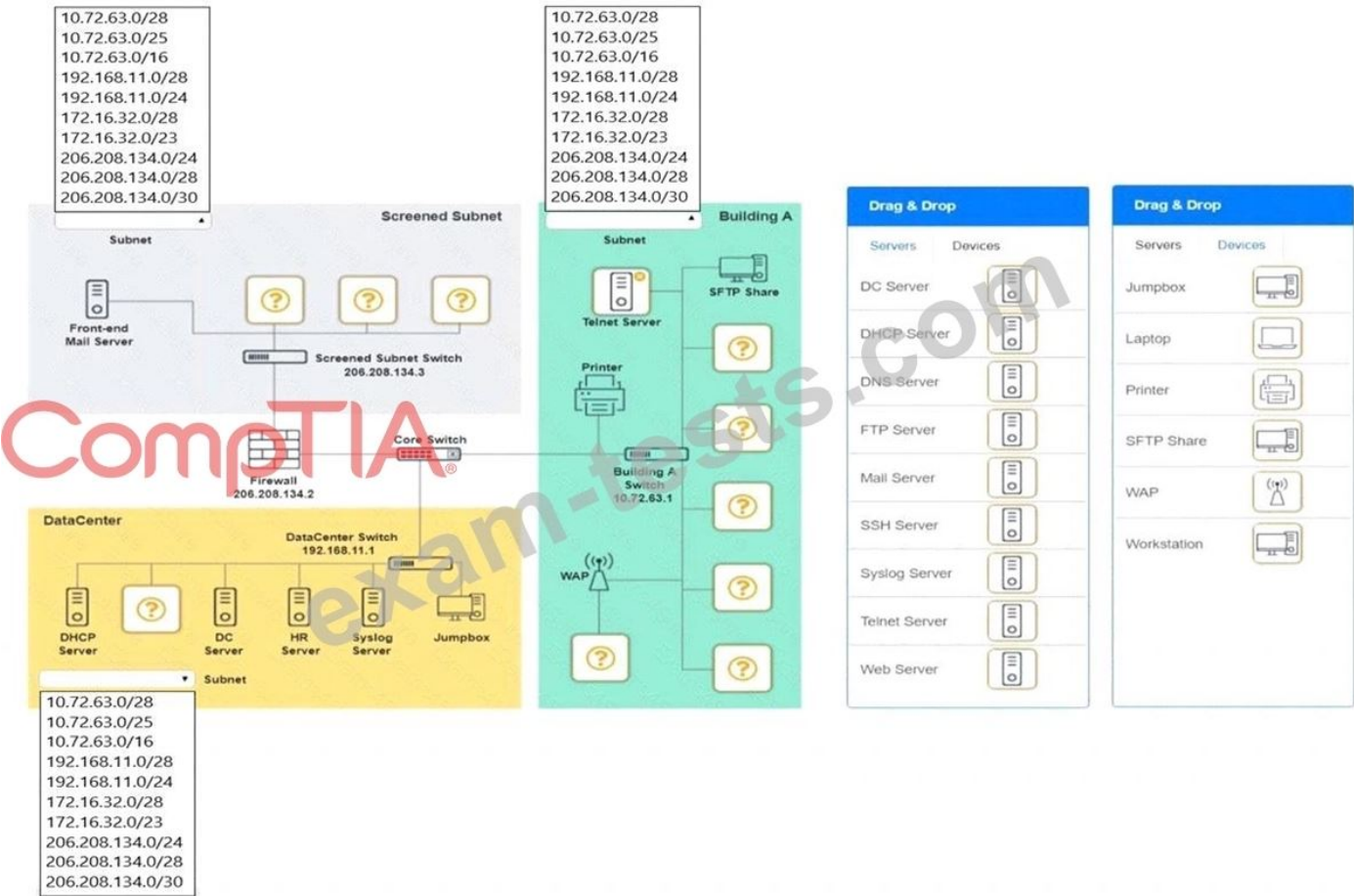
NEW QUESTION: 328

You are tasked with verifying the following requirements are met in order to ensure network security.

Requirements:

Datacenter

- Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
 - Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic Building A
 - Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
 - Provide devices to support 5 additional different office users
 - Add an additional mobile user
 - Replace the Telnet server with a more secure solution
 - Screened subnet
 - Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
 - Provide a server to handle external 80/443 traffic
 - Provide a server to handle port 20/21 traffic
- INSTRUCTIONS Drag and drop objects onto the appropriate locations. Objects can be used multiple times and not all placeholders need to be filled.
- Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.
- If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



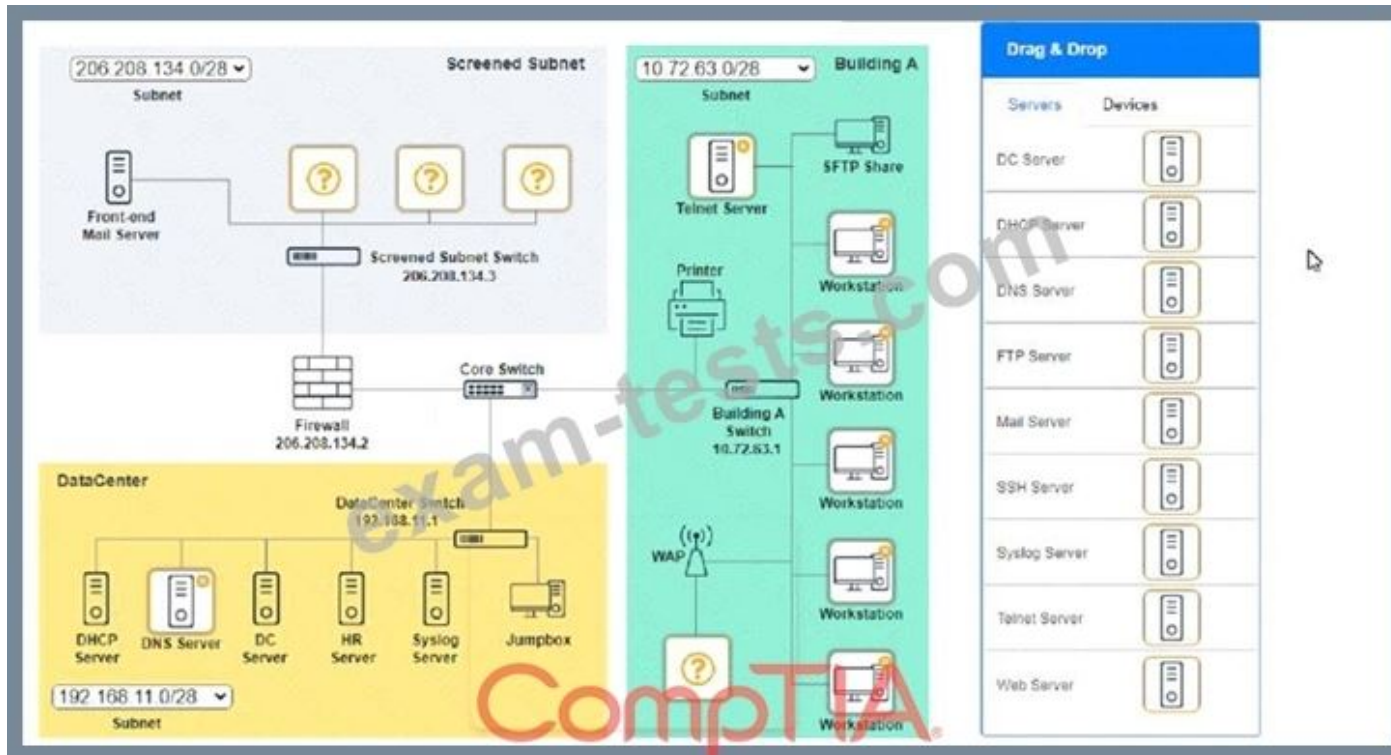
Answer:

See explanation below.

Explanation

Screened Subnet devices - Web server, FTP server

Building A devices - SSH server top left, workstations on all 5 on the right, laptop on bottom left DataCenter devices - DNS server.



NEW QUESTION: 329

The results of a recently completed site survey indicate a significant, undesired RSSI in the parking lot and other exterior areas near the building like to mitigate access to the wireless network in exterior access areas. The current access point settings are listed in the following table:

Which of the following is the BEST step for the technician to take to resolve the issue?

- A. Reconfigure AP2 and AP3 for non-overlapping channels
- B. Implement directional antennas on AP1 and AP2.
- C. Raise the power settings on AP2 and AP3.
- D. Change the SSID on AP1 and AP2.

Answer: B (LEAVE A REPLY)

Implementing directional antennas on AP1 and AP2 is the best step for the technician to take to resolve the issue of undesired RSSI in the parking lot and other exterior areas near the building. RSSI stands for received signal strength indicator, which is a measure of how well a device can receive a wireless signal from an access point (AP). An AP is a device that provides wireless connectivity to a network. An antenna is a device that radiates or receives electromagnetic waves. A directional antenna is an antenna that focuses the wireless signal in a specific direction, resulting in higher gain and longer range. By using directional antennas on AP1 and AP2, which are located near the exterior walls of the building, the technician can reduce the wireless signal leakage to the outside areas and improve the wireless coverage inside the building. Reference: [CompTIA Network+ Certification Exam

Objectives], What Is RSSI and How Does It Affect Wireless Networks?, Directional Antennas: Everything You Need to Know

NEW QUESTION: 330

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: (SHOW ANSWER)

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: 331

An organization set up its offices so that a desktop is connected to the network through a VoIP phone. The VoIP vendor requested that voice traffic be segmented separately from non-voice traffic. Which of the following would allow the organization to configure multiple devices with network isolation on a single switch port?

- A. Subinterfaces
- B. Link aggregation
- C. Load balancing
- D. Tunneling

Answer: (SHOW ANSWER)

- * Subinterfaces are logical divisions of a physical interface that can be assigned different VLANs, IP addresses, and security policies¹².
- * Subinterfaces allow the organization to configure multiple devices with network isolation on a single switch port by creating separate VLANs for voice and data traffic¹².
- * Subinterfaces can also be used to implement inter-VLAN routing, which enables communication between different VLANs on the same switch or router¹².
- * Link aggregation is the process of combining multiple physical links into a single logical link for increased bandwidth, redundancy, and load balancing³. It does not provide network isolation or VLAN segmentation.
- * Load balancing is the distribution of network traffic across multiple servers or paths to optimize performance, availability, and reliability. It does not provide network isolation or VLAN segmentation.
- * Tunneling is the encapsulation of one protocol within another protocol, usually to provide secure or private communication over a public network. It does not provide network isolation or VLAN segmentation on a single switch port. References:

- * [CompTIA Network+ N10-008 Certification Study Guide], Chapter 3: Network Components, Section: Subinterfaces
- * [Professor Messer's CompTIA N10-008 Network+ Course Notes], Page 23: Subinterfaces
- * [CompTIA Network+ N10-008 Certification Study Guide], Chapter 3: Network Components, Section: Link Aggregation
- * [Professor Messer's CompTIA N10-008 Network+ Course Notes], Page 24: Link Aggregation
- * [CompTIA Network+ N10-008 Certification Study Guide], Chapter 3: Network Components, Section: Load Balancing
- * [Professor Messer's CompTIA N10-008 Network+ Course Notes], Page 25: Load Balancing
- * [CompTIA Network+ N10-008 Certification Study Guide], Chapter 4: TCP/IP, Section: Tunneling
- * [Professor Messer's CompTIA N10-008 Network+ Course Notes], Page 32: Tunneling

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!
 BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 332

A user is unable to perform a reverse DNS lookup of an IP address to a hostname. Which of the following DNS record types is missing?

- A. PTR
- B. CNAME
- C. SOA
- D. AAAA

Answer: A (LEAVE A REPLY)

When a user is unable to perform a reverse DNS lookup of an IP address to a hostname, the missing DNS record type is the PTR (Pointer) record. Here's what you need to know:

PTR (Pointer) Record:

The PTR record maps an IP address to a hostname (reverse DNS lookup).

It is used to resolve IP addresses back to domain names.

For example, if you have an IP address (e.g., 192.168.1.10), the PTR record would provide the corresponding hostname (e.g., server.example.com).

NEW QUESTION: 333

A network security engineer is responding to a security incident. The engineer suspects that an attacker used an authorized administrator account to make configuration changes to the boundary firewall. Which of the following should the network security engineer review?

- A. Network traffic logs

- B. Audit logs
- C. Syslogs
- D. Event logs

Answer: B (LEAVE A REPLY)

Explanation

Audit logs are records of the actions performed by users or processes on a system or network device. They can provide information about who made what changes, when, and why. Audit logs are essential for detecting and investigating security incidents, as well as for ensuring compliance with policies and regulations. Audit logs can help the network security engineer to identify the source of the unauthorized configuration changes to the boundary firewall, as well as the scope and impact of the changes.

References1 - Changes to Cyber Essentials requirements - April 2021 update2 - 8 Firewall Best Practices for Securing the Network3 - How to secure your network boundaries with a firewall

NEW QUESTION: 334

Which of the following is the first step a network administrator should take in the troubleshooting methodology?

- A. Establish a plan of action.
- B. Document findings and outcomes.
- C. Test the theory to determine cause.
- D. Identify the problem.

Answer: D (LEAVE A REPLY)

According to the network troubleshooting methodology, the first step a network administrator should take is to identify the problem. This involves gathering information from the users, the network devices, and the symptoms of the issue. Identifying the problem helps to narrow down the scope and the possible causes of the network issue.

References

- * 1: Network troubleshooting methodology | CompTIA Network+ N10-008 ...
- * 2: Chapter 21. A Network Troubleshooting Methodology - CompTIA Network+ ...
- * 3: Network Troubleshooting Methodology - N10-008 CompTIA Network+ : 5.1

NEW QUESTION: 335

A global company has acquired a local company. The companies are geographically separate. The IP address ranges for the two companies are as follows:

- Global company: 10.0.0.0/16
- Local company: 10.0.0.0/24

Which of the following can the network engineer do to quickly connect the two companies?

- A. Assign an overlapping IP address range to both companies.
- B. Assign a NAT range to the local company.
- C. Assign static routing to advertise the local company's network
- D. Assign a new IP address range to the local company.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 336

Which of the following diagrams would most likely include specifications about fiber connector types?

- A. Logical
- B. Physical
- C. Rack
- D. Routing

Answer: B ([LEAVE A REPLY](#))

Explanation

A physical diagram is a type of diagram that shows the physical layout and connections of the network devices and components, such as routers, switches, cables, and connectors. A physical diagram may include specifications about the fiber connector types, such as LC, SC, FC, ST, MPO, etc., that are used to link the fiber optic cables and devices. A physical diagram can help to visualize the network topology, troubleshoot network problems, and plan network changes

NEW QUESTION: 337

Which of the following is an advantage of using the cloud as a redundant data center?

- A. The process of changing cloud providers is easy.
- B. Better security for company data is provided.
- C. The initial capital expenses are lower.
- D. The need for backups is eliminated.

Answer: C ([LEAVE A REPLY](#))

Using the cloud as a redundant data center means that the company does not need to invest in building and maintaining a physical backup site, which can be costly and time-consuming. Instead, the company can pay for the cloud services as needed, which can reduce the initial capital expenses and operational costs. However, this does not mean that the other options are true. Changing cloud providers may not be easy due to compatibility, contractual, or regulatory issues. Security for company data may not be better in the cloud, depending on the cloud provider's policies and practices. The need for backups is not eliminated, as the cloud data still needs to be protected from loss, corruption, or unauthorized access.

References:

* Part 1 of current page talks about how Bing is your AI-powered copilot for the web and provides various examples of how it can help you with different tasks, such as writing a joke, creating a table, or

* summarizing research. However, it does not mention anything about using the cloud as a redundant data center.

* Part 2 of current page shows the search results for "ai powered search bing chat", which include web, image, and news results. However, none of these results seem to be relevant to the question, as they are mostly about Bing's features, products, or announcements, not about cloud computing or data centers.

* Therefore, I cannot find the answer or the explanation from the current page. I have to use my own knowledge and information from other sources to verify the answer and provide a short but comprehensive explanation. I will cite these sources using numerical references.

* : CompTIA Network+ Certification Exam Objectives, Version 8.0, Domain 3.0: Network Operations, Objective 3.4: Given a scenario, use appropriate resources to support configuration management, Subobjective 3.4.2: Cloud-based configuration management,

<https://www.comptia.jp/pdf/comptia-network-n10-008-exam-objectives.pdf>

* : Cloud Computing: Concepts, Technology & Architecture, Chapter 9: Fundamental Cloud Security, Section 9.1: Cloud Security Threats,

<https://ptgmedia.pearsoncmg.com/images/9780133387520/samplepages/9780133387520.pdf>

* : Cloud Computing: Principles and Paradigms, Chapter 19: Data Protection and Disaster Recovery for Cloud Computing, Section 19.1: Introduction,

<https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470940105.ch19>

NEW QUESTION: 338

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

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

Answer: A (LEAVE A REPLY)

Your internet service provider will send a data signal through the coaxial cable or coax cable to your modem. A coaxial cable helps cable internet service providers transmit data between servers.

NEW QUESTION: 339

Which of the following is used to purposely attack a system to exploit vulnerabilities?

- A. Honeypot
- B. Vulnerability scan
- C. Device hardening
- D. Penetration testing

Answer: D (LEAVE A REPLY)

Honeypot is used to capture information from unauthorized intruders. Basically, they do not allow users into their networks. They allow them into a fake network that looks like it is a part of their actual network.

Penetration testing is where you are purposely attacking to see any vulnerabilities.

NEW QUESTION: 340

A technician is troubleshooting a client's report about poor wireless performance. Using a client monitor, the technician notes the following information:

SSID	Signal (RSSI)	Channel
Corporate	-50	9
Corporate	-69	10
Corporate	-67	11
Corporate	-63	6

Which of the following is MOST likely the cause of the issue?

- A. Poor signal
- B. Channel overlap
- C. Wrong antenna type
- D. Incorrect power settings

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 341

A technician is troubleshooting a report about network connectivity issues on a workstation. Upon investigation, the technician notes the workstation is showing an APIPA address on the network interface. The technician verifies that the VLAN assignment is correct and that the network interface has connectivity. Which of the following is MOST likely the issue the workstation is experiencing?

- A. DHCP exhaustion
- B. A rogue DHCP server
- C. A DNS server outage
- D. An incorrect subnet mask

Answer: A ([LEAVE A REPLY](#))

Each DHCP request with a different MAC address is regarded by the DHCP server as a new network client request. If the attacker sends an ample number of requests, the server's address pool will ultimately be exhausted. Hence, new network clients will be denied the DHCP service and will be unable to join the network.

NEW QUESTION: 342

A building was recently remodeled in order to expand the front lobby. Some mobile users have been unable to connect to the available network jacks within the new lobby, while others have had no issues. Which of the following is the MOST likely cause of the connectivity issues?

- A. LACP
- B. Port security
- C. 802.11ax
- D. Duplex settings

Answer: ([SHOW ANSWER](#))

Port security is a feature that allows a network device to limit the number and type of MAC addresses that can access a port. Port security can prevent unauthorized devices from connecting to the network through an available network jack. Therefore, port security is the most likely cause of the connectivity issues for some mobile users in the new lobby.

NEW QUESTION: 343

A network administrator is trying to add network redundancy for the server farm. Which of the following can the network administrator configure to BEST provide this capability?

- A. RPO
- B. UPS
- C. VRRP
- D. DNS

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 344

A network technician has determined the cause of a network disruption. Which of the following is the NEXT step for the technician to perform?

- A. Validate the findings in a top-to-bottom approach
- B. Duplicate the issue, if possible
- C. Establish a plan of action to resolve the issue
- D. Document the findings and actions

Answer: C ([LEAVE A REPLY](#))

A network technician should follow a network troubleshooting methodology to systematically identify and resolve network problems¹².

A network troubleshooting methodology consists of several steps, such as identifying the problem, establishing a theory of probable cause, testing the theory, implementing a solution, verifying functionality, and documenting the results¹².

In this scenario, the network technician has determined the cause of a network disruption, which means that they have completed the steps of identifying the problem, establishing a theory of probable cause, and testing the theory¹².

The NEXT step for the technician to perform is to establish a plan of action to resolve the issue, which means that they should define the steps, resources, and tools needed to implement a solution that can fix the network disruption¹².

Establishing a plan of action to resolve the issue is the next step, because it can help the technician to prepare for the implementation, avoid potential risks or complications, and communicate the plan to the stakeholders¹².

The other options are not the next step for the technician to perform, because they are either previous or subsequent steps in the network troubleshooting methodology¹²:

A . Validating the findings in a top-to-bottom approach is a previous step, which is part of testing the theory of probable cause, where the technician should verify the network functionality and connectivity from the physical layer to the application layer¹².

B . Duplicating the issue, if possible, is a previous step, which is part of identifying the problem, where the technician should reproduce the symptoms and scope of the problem to confirm its existence and impact¹².
D . Documenting the findings and actions is a subsequent step, which is part of verifying functionality and preventing recurrence, where the technician should record the problem description, solution, and outcome for future reference and improvement¹².

Reference:

1: Network Troubleshooting Methodology - N10-008 CompTIA Network+ : 5.1

2: CompTIA Network+ N10-008 Full Course for Beginners - Network Troubleshooting Methodology (5.1)

NEW QUESTION: 345

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

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 346

Which of the following ports is commonly used by VoIP phones?

- A. 20
- B. 143
- C. 445
- D. 5060

Answer: (SHOW ANSWER)

VoIP uses UDP port 5060 unsecured and UDP port 5061 secured.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 347

Which of the following should a junior security administrator recommend implementing to mitigate malicious network activity?

- A. Load balancer
- B. Access logging
- C. Endpoint encryption

D. Intrusion prevention system

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 348

A company is reviewing ways to cut the overall cost of its IT budget. A network technician suggests removing various computer programs from the IT budget and only providing these programs on an as-needed basis. Which of the following models would meet this requirement?

A. Multitenancy

B. IaaS

C. SaaS

D. VPN

Answer: C ([LEAVE A REPLY](#))

SaaS stands for Software as a Service and is a cloud computing model where software applications are hosted and delivered over the internet by a service provider. SaaS can help the company cut the overall cost of its IT budget by eliminating the need to purchase, install, update, and maintain various computer programs on its own devices. The company can access the programs on an as-needed basis and pay only for what it uses.

Multitenancy is a feature of cloud computing where multiple customers share the same physical or virtual resources. IaaS stands for Infrastructure as a Service and is a cloud computing model where computing resources such as servers, storage, and networking are provided over the internet by a service provider. VPN stands for Virtual Private Network and is a technology that creates a secure and encrypted connection over a public network.

NEW QUESTION: 349

Users in a branch can access an In-house database server, but it 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. QoS

C. Syslog

D. Traffic shaping

E. Link state

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 350

A network administrator installed an additional IDF during a building expansion project. Which of the following documents need to be updated to reflect the change? (Select TWO).

A. Data loss prevention policy

B. Physical network diagram

C. BYOD policy

D. Disaster recovery plan

E. Non-disclosure agreement

F. Acceptable use policy

Answer: A,B ([LEAVE A REPLY](#))

NEW QUESTION: 351

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: ([SHOW ANSWER](#))

Explanation

TACACS+ (Terminal Access Controller Access Control System Plus) can be used to centrally manage credentials for various types of administrative privileges on configured network devices. This protocol separates authentication, authorization, and accounting (AAA) functions, providing more granular control over access to network resources.

References:

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

NEW QUESTION: 352

To access production applications and data, developers must first connect remotely to a different server. From there, the developers are able to access production data. Which of the following does this BEST represent?

A. A management plane

B. A proxy server

C. An out-of-band management device

D. A site-to-site VPN

E. A jump box

Answer: ([SHOW ANSWER](#))

To access production applications and data, developers must first connect remotely to a different server. From there, the developers are able to access production data. This best represents a jump box, which is a system on a network used to access and manage devices in a separate security zone. A jump box is a hardened and monitored device that spans two dissimilar security zones and provides a controlled means of access between them. A jump box is often used to provide transparent management of devices on a DMZ or a production environment once a remote session has been established. The jump box acts as a single audit point for traffic and also a single place where user accounts can be managed. A prospective administrator or developer must log into the jump box in order to gain access to the production assets and all access can be logged for later audit. The other options do not best represent the scenario. A management plane is a logical part of a network device that provides administrative functions such as configuration, monitoring, and troubleshooting. A proxy server is a device that acts as an intermediary between a client and a server, providing functions such as caching, filtering,

or load balancing³ An out-of-band management device is a device that provides a separate and dedicated channel for network management, such as a console port or a modem. A site-to-site VPN is a secure connection between two or more networks over the internet, using encryption and tunneling protocols.

Reference:

https://en.wikipedia.org/wiki/Jump_server

NEW QUESTION: 353

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: (SHOW ANSWER)

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: 354

A security analyst found the following vulnerability on the company's website: `<INPUT TYPE="IMAGE" SRC="javascript : alert ('test') ; ">`

Which of the following should be implemented to prevent this type of attack in the future?

- A. Input sanitization
- B. Output encoding
- C. Code obfuscation
- D. Prepared statements

Answer: A (LEAVE A REPLY)

Explanation

Input sanitization is the process of validating and filtering the user input to prevent malicious code or commands from being executed on the web server or the web browser. Input sanitization can prevent this type of attack, which is called cross-site scripting (XSS), by removing or escaping any special characters or scripts that are not expected or allowed in the input field. Input sanitization can be implemented on the server-side or the client-side, or both, to enhance the security of the web application.

References

- 1: Web Application Attacks - N10-008 CompTIA Network+ : 3.2
- 2: CompTIA Network+ N10-008 Certification Study Guide, page 317
- 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 15
- 4: CompTIA Network+ N10-008 Certification Practice Test, question 6

NEW QUESTION: 355

Which of the following can be used to limit the ability of devices to perform only HTTPS connections to an internet update server without exposing the devices to the public internet?

- A. Create a screened network and move the devices to it.
- B. Allow connections only to an internal proxy server.
- C. Deploy an IDS system and place it in line with the traffic.
- D. Use a host-based network firewall on each device.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 356

Which of the following would be BEST to use to detect a MAC spoofing attack?

- A. Internet Control Message Protocol
- B. Reverse Address Resolution Protocol
- C. Dynamic Host Configuration Protocol
- D. Internet Message Access Protocol

Answer: B ([LEAVE A REPLY](#))

Reverse Address Resolution Protocol (RARP) is a protocol that allows a device to obtain its MAC address from its IP address. A MAC spoofing attack is an attack where a device pretends to have a different MAC address than its actual one. RARP can be used to detect a MAC spoofing attack by comparing the MAC address obtained from RARP with the MAC address obtained from other sources, such as ARP or DHCP.

References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

<https://www.techopedia.com/definition/25597/reverse-address-resolution-protocol-rarp>

NEW QUESTION: 357

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

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 358

The following DHCP scope was configured for a new VLAN dedicated to a large deployment of 325 IoT sensors:

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

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 359

A network administrator received a report stating a critical vulnerability was detected on an application that is exposed to the internet. Which of the following is the appropriate NEXT step?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 360

A technician is troubleshooting a workstation's network connectivity and wants to confirm which switchport corresponds to the wall jack the PC is using. Which of the following concepts would BEST help the technician?

- A. Consistent labeling
- B. Change management
- C. Standard work instructions
- D. Inventory management
- E. Network baseline

Answer: A ([LEAVE A REPLY](#))

Consistent labeling would be the concept that would best help the technician to confirm which switchport corresponds to the wall jack the PC is using. Consistent labeling is a practice of using standardized and descriptive labels for network devices, ports, cables, jacks, and other components. It can help with identifying, locating, and troubleshooting network issues. For example, a technician can use consistent labeling to trace a cable from a PC to a wall jack, and then from a patch panel to a switchport. Reference:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_6.html

NEW QUESTION: 361

A customer needs to distribute Ethernet to multiple computers in an office. The customer would like to use non-proprietary standards. Which of the following blocks does the technician need to install?

- A. 110
- B. 66
- C. BiX
- D. Krone

Answer: A (LEAVE A REPLY)

A 110 block is a type of punch-down block that is used to terminate twisted-pair cables in Ethernet networks. It is a non-proprietary standard that is widely used in structured cabling systems for voice and data applications. A 110 block can support up to 100 MHz of bandwidth and can be used with Cat 3, Cat 5, Cat 5e, and Cat 6 cables¹².

A 66 block is another type of punch-down block that is mainly used for telephone wiring. It is an older and less reliable standard than the 110 block and does not support high-speed data transmission³. A BiX block is a proprietary punch-down block that is developed by NORDX/CDT and is mostly used in Canada. It can support up to 250 MHz of bandwidth and can be used with Cat 5e and Cat 6 cables⁴. A Krone block is another proprietary punch-down block that is developed by ADC Krone and is mostly used in Europe. It can support up to 100 MHz of bandwidth and can be used with Cat 5 and Cat 5e cables.

Therefore, the best option for the customer who wants to use non-proprietary standards is the 110 block.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 362

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

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

Answer: B (LEAVE A REPLY)

* VLAN hopping is a type of network attack that allows an attacker to access network resources or traffic that belong to a different VLAN than the one the attacker is connected to¹².

* VLAN hopping can be performed in two ways: switch spoofing or double tagging¹².

* Switch spoofing is when an attacker configures their device to act as a trunk port and negotiates trunking with the switch, allowing the attacker to access all VLANs on the trunk link¹².

- * Double tagging is when an attacker sends a packet that contains two VLAN tags, one for the attacker's VLAN and one for the target VLAN. The first tag is stripped off by the switch, and the second tag is forwarded to the target VLAN, bypassing the VLAN isolation¹².
- * Double tagging is an example of an attack that utilizes a network packet that contains multiple network tags¹².
- * MAC flooding is a type of network attack that floods the switch's MAC address table with fake or spoofed MAC addresses, causing the switch to enter a fail-open mode and broadcast all traffic to all ports, allowing the attacker to capture or modify the traffic¹². MAC flooding does not involve multiple network tags¹².
- * DNS spoofing is a type of network attack that alters the DNS records or responses to redirect the user to a malicious website or server, instead of the legitimate one¹². DNS spoofing does not involve multiple network tags¹².
- * ARP poisoning is a type of network attack that sends fake or spoofed ARP messages to associate the attacker's MAC address with the IP address of another device, such as the gateway or the server, allowing the attacker to intercept or modify the traffic between the devices¹². ARP poisoning does not involve multiple network tags¹².

References:

- * 1: CompTIA Network+ N10-008 Exam Cram, 6th Edition, Chapter 7: Network Security Concepts and Tools, p. 318-319
- * 2: CompTIA Network+ N10-008 Cert Guide, 1st Edition, Chapter 13: Network Attacks and Mitigation Techniques, p. 615-616

NEW QUESTION: 363

A network engineer performed a detailed network analysis. The engineer has decided to update the STP port cost in order to optimize the network. Which of the following processes should the engineer use to gain approval for the network optimization?

- A. Business continuity
- B. Disaster recovery
- C. Incident response
- D. Change management

Answer: D (LEAVE A REPLY)

The change management process is the correct answer because it ensures that any changes to the network, such as updating the STP (Spanning Tree Protocol) port cost, are reviewed, approved, documented, and communicated to all relevant stakeholders. This process minimizes the risk of unintended disruptions or negative impacts on the network and ensures that all changes are aligned with business objectives.

NEW QUESTION: 364

A network administrator is decommissioning a server. Which of the following will the network administrator MOST likely consult?

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

Answer: (SHOW ANSWER)

NEW QUESTION: 365

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

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

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 366

A network administrator replaced a faulty NIC in a printer, but the printer is still not reachable. The printer is configured with the correct IP address, mask, and gateway, and a link light is lit on the switch port that the printer is attached to. Which of the following is the best command for the administrator to run first on the switch?

- A. show vlan
- B. show route
- C. show arp
- D. show config

Answer: (SHOW ANSWER)

The best command for the administrator to run first on the switch is show vlan, which displays the VLAN configuration information on the switch, such as the VLAN IDs, names, and ports. The show vlan command can help the administrator to verify if the printer is assigned to the correct VLAN, and if there is any mismatch or misconfiguration that prevents the printer from being reachable. The show route command displays the routing table on the switch, which is not relevant for the printer connectivity, as the printer is configured with the correct gateway. The show arp command displays the ARP cache on the switch, which maps the IP addresses to the MAC addresses of the devices. The show arp command can help the administrator to check if the switch has learned the MAC address of the printer, but it is not the best command to run first, as the ARP cache can be cleared or updated frequently. The show config command displays the running configuration on the switch, which includes the VLAN configuration, but it also includes other information that is not related to the printer issue, such as the hostname, the interface settings, the security settings, and so on. The show config command can be overwhelming and time-consuming to analyze, so it is not the best command to run first.

References

- * 1: VLANs and Trunking - N10-008 CompTIA Network+ : 2.3
- * 2: N10-008 CompTIA Network+ : 5.5
- * 3: Interface Configurations - N10-008 CompTIA Network+ : 2.3
- * 4: Configuring VLANs - CompTIA Network+ N10-006 - 2.6

NEW QUESTION: 367

A technician notices that equipment is being moved around and misplaced in the server room, even though the room has locked doors and cabinets. Which of the following would be the BEST solution to identify who is responsible?

- A. Install motion detection
- B. Install cameras.
- C. Install tamper detection.
- D. Hire a security guard.

Answer: [\(SHOW ANSWER\)](#)

Installing cameras in the server room is the best solution to identify who is responsible for the equipment being moved and misplaced. Cameras provide a way to monitor the server room in real time and can be used to identify suspicious activity. Additionally, they provide a way to review past activity and allow you to review footage to determine who may be responsible for the misplacement of equipment.

NEW QUESTION: 368

An IT director is setting up new disaster and HA policies for a company. Limited downtime is critical to operations. To meet corporate requirements, the director set up two different datacenters across the country that will stay current on data and applications. In the event of an outage, the company can immediately switch from one datacenter to another. Which of the following does this BEST describe?

- A. A warm site
- B. Data mirroring
- C. Multipathing
- D. Load balancing
- E. A hot site

Answer: [E \(LEAVE A REPLY\)](#)

A hot site is a fully redundant site that can take over operations immediately if the primary site goes down. In this scenario, the company has set up two different datacenters across the country that are current on data and applications, and they can immediately switch from one datacenter to another in case of an outage. Reference: Network+ N10-008 Objectives: 1.5 Compare and contrast disaster recovery concepts and methodologies.

NEW QUESTION: 369

A customer is hosting an internal database server. None of the users are able to connect to the server, even though it appears to be working properly. Which of the following is the best way to verify traffic to and from the server?

- A. Protocol analyzer
- B. nmap
- C. ipconfig
- D. Speed test

Answer: [A \(LEAVE A REPLY\)](#)

A protocol analyzer is the best way to verify traffic to and from the server. A protocol analyzer, also known as a packet sniffer or network analyzer, is a tool that captures and analyzes the network packets that are sent and received by a device. A protocol analyzer can show the source and destination IP addresses, ports, protocols,

and payload of each packet, as well as any errors or anomalies in the network communication. A protocol analyzer can help troubleshoot network connectivity issues by identifying the root cause of the problem, such as misconfigured firewall rules, incorrect routing, or faulty network devices¹².

To use a protocol analyzer to verify traffic to and from the server, the customer can follow these steps:

Install a protocol analyzer tool on a device that is connected to the same network as the server, such as Wireshark³ or Microsoft Network Monitor⁴.

Select the network interface that is used to communicate with the server, and start capturing the network traffic.

Filter the captured traffic by using the IP address or hostname of the server, or by using a specific port or protocol that is used by the database service.

Analyze the filtered traffic and look for any signs of successful or failed connection attempts, such as TCP SYN, ACK, or RST packets, or ICMP messages.

If there are no connection attempts to or from the server, then there may be a problem with the network configuration or device settings that prevent the traffic from reaching the server.

If there are connection attempts but they are rejected or dropped by the server, then there may be a problem with the server configuration or service settings that prevent the traffic from being accepted by the server.

The other options are not the best ways to verify traffic to and from the server. nmap is a tool that can scan a network and discover hosts and services, but it cannot capture and analyze the network packets in detail. ipconfig is a command that can display and configure the IP settings of a device, but it cannot monitor or test the network communication with another device. Speed test is a tool that can measure the bandwidth and latency of a network connection, but it cannot diagnose or troubleshoot specific network problems.

NEW QUESTION: 370

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: (SHOW ANSWER)

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.

NEW QUESTION: 371

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 ([LEAVE A REPLY](#))

Short The switch feature that is most likely to be used to assist with logging IPv6 and MAC addresses of devices on a network segment is Neighbor Discovery Protocol (NDP). NDP is used by IPv6 to discover and maintain information about other nodes on the network, including their IPv6 and MAC addresses. By periodically querying NDP, the administrator can log this information for auditing purposes.

Reference:

CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.1: Compare and contrast TCP and UDP ports, protocols, and their purposes.

NEW QUESTION: 372

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

Ethernet Adapter:

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

Which of the following is misconfigured?

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

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 373

A company is reviewing ways to cut the overall cost of its IT budget. A network technician suggests removing various computer programs from the IT budget and only providing these programs on an as-needed basis. Which of the following models would meet this requirement?

- A. SaaS
- B. VPN

C. IaaS

D. Multitenancy

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 374

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

A. A landing page

B. An access control vestibule

C. A smart locker

D. A firewall

Answer: ([SHOW ANSWER](#))

Reference: [https://en.wikipedia.org/wiki/Mantrap_\(access_control\)](https://en.wikipedia.org/wiki/Mantrap_(access_control))

NEW QUESTION: 375

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

A. Warm site

B. Cloud site

C. Hot site

D. Cold site

Answer: B ([LEAVE A REPLY](#))

For many companies, the most cost-effective solution is to move processing and data storage to a cloud site.

NEW QUESTION: 376

Which of the following provides guidance to an employee about restricting non-business access to the company's videoconferencing solution?

A. Acceptable use policy

B. Data loss prevention

C. Remote access policy

D. Standard operating procedure

Answer: A ([LEAVE A REPLY](#))

Explanation

An acceptable use policy (AUP) is a set of rules that outline the proper and improper use of an organization's resources, such as its videoconferencing solution. An AUP can provide guidance to employees about what is expected of them when using the organization's videoconferencing solution, including restricting non-business access to it.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam

questions have been updated and answers have been corrected get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 377

A technician is configuring a wireless access point in a public space for guests to use. Which of the following should the technician configure so that only approved connections are allowed?

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

Answer: (SHOW ANSWER)

NEW QUESTION: 378

A network consultant is setting up a new wireless infrastructure. The new infrastructure is primarily focused on supporting legacy equipment that does not support the newest standards. Which of the following frequency ranges will the consultant most likely have to support?

- A. 2.4GHz
- B. 5GHz
- C. 5.9GHz
- D. 6GHz

Answer: A (LEAVE A REPLY)

Explanation

The most likely frequency range that the network consultant will have to support is 2.4GHz. This is because the most common legacy wireless standards, 802.11b and 802.11g, use the 2.4GHz range¹. IEEE 802.11a uses 5GHz exclusively, and 5.9GHz and 6GHz are not widely used by legacy equipment. Therefore, A. 2.4GHz is the correct answer.

<https://www.networkcomputing.com/networking/wireless-beginners-part-1-rf-and-waves>

NEW QUESTION: 379

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

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

Answer: D,E (LEAVE A REPLY)

A layer 3 switch is a device that can perform both switching and routing functions. It can forward packets based on the destination IP address, which is the information used to identify different subnetworks. A layer 3 switch can

also create and manage multiple VLANs, which are logical subnetworks within a physical network. Therefore, a layer 3 switch can allow communication between two different subnetworks.

A router is a device that connects multiple IP networks and forwards packets based on the destination IP address. A router can also perform network address translation (NAT), which allows devices with private IP addresses to communicate with devices with public IP addresses. Therefore, a router can allow communication between two different subnetworks, especially if they use different address spaces.

An IDS (intrusion detection system) is a device that monitors network traffic and detects malicious or anomalous activities. An IDS does not forward packets or allow communication between subnetworks, but rather alerts the network administrator or takes preventive actions when a threat is detected.

An access point is a device that allows wireless devices to connect to a wired network. An access point does not forward packets or allow communication between subnetworks, but rather acts as a bridge between the wireless and wired segments of the network.

A layer 2 switch is a device that forwards frames based on the destination MAC address, which is the information used to identify devices within the same subnetwork. A layer 2 switch does not perform routing or network segmentation, and therefore cannot allow communication between different subnetworks.

A media converter is a device that converts signals between different types of media, such as copper and fiber. A media converter does not forward packets or allow communication between subnetworks, but rather enables devices with different physical interfaces to connect to the same network.

Reference:

Network Devices

Routing and Switching Essentials

CompTIA Network+ N10-008 Study Guide, Chapter 2: Devices and Infrastructure, pages 58-63, 72-75.

NEW QUESTION: 380

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

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

Answer: ([SHOW ANSWER](#))

LC (local connector) is the most likely fiber connector type to be used on a network interface card, because it is a small form factor connector that can fit more interfaces on a single card. LC connectors use square connectors that have a locking mechanism on the top, similar to an RJ45 copper connector. LC connectors are also compatible with SFP (small form-factor pluggable) modules that are often used to link a gigabit Ethernet port with a fiber network¹².

References:

* Optical Fiber Connectors - CompTIA Network+ N10-007 - 2.11

* CompTIA Network+ Certification Exam Objectives²

NEW QUESTION: 381

A network administrator is troubleshooting an issue on a newly configured college campus network. A Linux workstation can connect to the internet, but it fails to connect to the campus intranet, which is located on another campus. Which of the following commands should the administrator run next to troubleshoot the connection?

- A. ifconfig
- B. dig
- C. traceroute
- D. nmap

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 382

A company cell phone was stolen from a technician's vehicle. The cell phone has a passcode, but it contains sensitive information about clients and vendors. Which of the following should also be enabled?

- A. Autolock
- B. Encryption
- C. Factory reset
- D. Two-factor authentication

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 383

A network technician receives a report from the server team that a server's network connection is not working correctly. The server team confirms the server is operating correctly except for the network connection. The technician checks the switchport connected to the server and reviews the following data;

Metric	Value
Bytes input	441,164,698
Bytes output	2,625,115,257
Runts	0
CRCs	5,489
Collisions	1
MDIX	On
Speed	1,000
Duplex	Full

Which of the following should the network technician perform to correct the issue?

- A. Replace the Cat 5 patch cable with a Cat 6 cable
- B. Install a crossover cable between the server and the switch
- C. Reset the switchport configuration.
- D. Use NetFlow data from the switch to isolate the issue.
- E. Disable MDIX on the switchport and reboot the server.

Answer: A (LEAVE A REPLY)

Bad cables, incorrect pinouts, or bent pins: Faulty cables (with electrical characteristics preventing successful transmission) or faulty connectors (which do not properly make connections) can prevent successful data transmission at Layer 1. A bad cable could simply be an incorrect category of cable being used for a specific purpose. For example, using a Cat 5 cable (instead of a Cat 6 or higher cable) to connect two 1000BASE-TX devices would result in data corruption. Bent pins in a connector or incorrect pinouts could also cause data to become corrupted.

NEW QUESTION: 384

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 (LEAVE A REPLY)

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: 385

During a recent security audit, a contracted penetration tester discovered the organization uses a number of insecure protocols. Which of the following ports should be disallowed so only encrypted protocols are allowed? (Choose two.)

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

Answer: E,F (LEAVE A REPLY)

NEW QUESTION: 386

A network technician receives a report from the server team that a server's network connection is not working correctly. The server team confirms the server is operating correctly except for the network connection. The technician checks the switchport connected to the server and reviews the following data;

Metric	Value
Bytes input	441,164,698
Bytes output	2,625,115,257
Runts	0
CRCs	5,489
Collisions	1
MDIX	On
Speed	1,000
Duplex	Full

Which of the following should the network technician perform to correct the issue?

- A. Replace the Cat 5 patch cable with a Cat 6 cable
- B. Install a crossover cable between the server and the switch
- C. Reset the switchport configuration.
- D. Use NetFlow data from the switch to isolate the issue.
- E. Disable MDIX on the switchport and reboot the server.

Answer: A (LEAVE A REPLY)

Explanation

"Bad cables, incorrect pinouts, or bent pins: Faulty cables (with electrical characteristics preventing successful transmission) or faulty connectors (which do not properly make connections) can prevent successful data transmission at Layer 1. A bad cable could simply be an incorrect category of cable being used for a specific purpose. For example, using a Cat 5 cable (instead of a Cat 6 or higher cable) to connect two 1000BASE-TX devices would result in data corruption. Bent pins in a connector or incorrect pinouts could also cause data to become corrupted."

NEW QUESTION: 387

During a risk assessment which of the following should be considered when planning to mitigate high CPU utilization of a firewall?

- A. Recovery time objective
- B. Uninterruptible power supply
- C. NIC teaming
- D. Load balancing

Answer: (SHOW ANSWER)

The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs. This does nothing to help with CPU utilization. Load balancing does this.

NEW QUESTION: 388

A network technician needs to correlate security events to analyze a suspected intrusion. Which of the following should the technician use?

- A. SNMP

- B. Log review
- C. Vulnerability scanning
- D. SIEM

Answer: D (LEAVE A REPLY)

SIEM stands for Security Information and Event Management, which is a tool that collects, analyzes, and correlates data from various network devices and sources to provide alerts and reports on security incidents and events. A network technician can use SIEM to correlate security events to analyze a suspected intrusion, as SIEM can help identify the source, target, method, and impact of an attack, as well as provide recommendations for remediation. References: <https://www.comptia.org/blog/what-is-siem>

NEW QUESTION: 389

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 (LEAVE A REPLY)

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.

Reference: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION: 390

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: (SHOW ANSWER)

Asymmetric routing is a situation in which the path taken by data packets between two points in a network is different in both directions. It can be caused by factors such as unequal cost paths, policy-based routing, load balancing, or network topology changes¹ In this scenario, the network administrator is troubleshooting a connectivity performance issue, which could be affected by asymmetric routing. For example, if one path has more congestion, latency, or packet loss than the other, the performance of the communication between the client and the server will be degraded² To diagnose the issue, the network administrator performs a traceout from the client to the server, and also from the server to the client. A traceout is a tool that shows the route and the number of hops that a packet takes to reach a destination. By comparing the outputs, the network administrator can identify if there is asymmetric routing in the network³ If the outputs show different hops between the hosts, it means that the packets are taking different paths in each direction, which is a sign of asymmetric routing. Therefore, the best answer is A. Asymmetric routing.

The other options are not as likely to explain the findings. A routing loop is a confusion about the reachability of a destination network, which causes packets to loop endlessly between two or more routers⁴ A switch loop is a situation in which there is more than one layer 2 path between two endpoints, which causes broadcast storms and MAC database instability⁵ An incorrect gateway is a configuration error that prevents a device from reaching the intended destination network⁶ None of these options would necessarily result in different hops between the hosts, as they would either cause the packets to be dropped, discarded, or delayed, but not rerouted. Therefore, the best answer is A. Asymmetric routing.

Reference:

https://en.wikipedia.org/wiki/Routing_loop

<https://www.networkstraining.com/what-is-asymmetric-routing/>

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/ip-default-gateway-settings-assigned-incorrectly>

<https://superuser.com/questions/1715808/cant-access-router-settings-default-gateway-not-working-as-expected>

NEW QUESTION: 391

A network engineer is installing hardware in a newly renovated data center. Major concerns that were addressed during the renovation included air circulation, building power redundancy, and the need for continuous monitoring. The network engineer IS creating alerts based on the following operation specifications:

AC input voltage	100 to 240VAC
AC maximum input current	<2.7A at 100V
Redundant power supply	Yes
Operating temperature	32–104°F (0–40°C)
Storage temperature	-4–149°F (-20–65°C)
Operating humidity	10–85%
Storage humidity	5–95%

Which of the following should the network engineer configure?

- A. Environmental monitoring alerts for humidity greater than 95%
- B. SIEM to parse syslog events for a failed power supply

C. SNMP traps to report when the chassis temperature exceeds 95°F (35°C)

D. UPS monitoring to report when input voltage drops below 220VAC

Answer: C (LEAVE A REPLY)

Explanation

The alert that the network engineer should configure based on the operation specifications is SNMP traps to report when the chassis temperature exceeds 95°F (35°C). SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate their status and performance information to a central management system, called an SNMP manager. SNMP traps are messages that are sent by network devices to notify the SNMP manager of an event or condition that requires attention, such as an error, a failure, or a threshold violation. In this case, the network engineer should configure SNMP traps on the network devices to send an alert when their chassis temperature exceeds 95°F (35°C), which is the maximum operating temperature specified in the table. This alert would help the network engineer monitor and troubleshoot any overheating issues that could affect the network performance or availability. References: CompTIA Network+ N10-008 Certification Study Guide, page 228; The Official CompTIA Network+ Student Guide (Exam N10-008), page 8-11.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 392

A help desk technician discovers the following note while reviewing tickets in a customer's account:

Was able to confirm customer's problem with the system. Will upgrade system to latest version and monitor for further connectivity problems per developer's instructions.

Which of the following describes what the technician was documenting with this note?

A. The technician was approaching multiple problems individually.

B. The technician was establishing a plan of action and identifying potential effects.

C. The technician was testing a theory to determine the cause.

D. The technician was identifying the problem by gathering information.

Answer: D (LEAVE A REPLY)

Explanation

The technician was identifying the problem by gathering information with this note. This is the first step of the troubleshooting methodology, which is a systematic process of finding and resolving issues in a network or system. By gathering information, the technician can understand the symptoms, scope, and impact of the problem, as well as collect relevant data from various sources, such as users, logs, tools, or documentation. The note shows that the technician was asking questions to the user, checking the network status and configuration, and reviewing previous tickets to gather information about the problem. References: [CompTIA Network+ Certification Exam Objectives], Troubleshooting Methodology - CompTIA Network+ N10-007 - 1.4 | Professor Messer IT Certification Training Courses

NEW QUESTION: 393

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

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

Answer: C ([LEAVE A REPLY](#))

EIGRP (Enhanced Interior Gateway Routing Protocol) is an advanced distance vector routing protocol that automates routing tables and also uses some features of link-state routing protocols.

It is a Cisco proprietary protocol used in larger networks that require fast convergence and scalability.

NEW QUESTION: 394

A technician is investigating packet loss to a device that has varying data bursts throughout the day. Which of the following will the technician MOST likely configure to resolve the issue?

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

Answer: A ([LEAVE A REPLY](#))

Ethernet flow control is a mechanism for temporarily stopping the transmission of data on Ethernet family computer networks. The goal of this mechanism is to avoid packet loss in the presence of network congestion.

NEW QUESTION: 395

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 ([LEAVE A REPLY](#))

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: 396

A network technician is investigating a trouble ticket for a user who does not have network connectivity. All patch cables between the wall jacks and computers in the building were upgraded over the weekend from Cat 5 to Cat 6. The newly installed cable is crimped with a TIA/EIA 568A on one end and a TIA/EIA 568B on the other end.

Which of the following should the technician do to MOST likely fix the issue?

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

Answer: B ([LEAVE A REPLY](#))

A straight-through cable is a type of twisted pair cable that has the same wiring standard (TIA/EIA 568A or 568B) on both ends. This is the most common type of cable used for connecting devices of different types, such as a computer and a switch. A cable that has different wiring standards on each end (TIA/EIA 568A on one end and 568B on the other) is called a crossover cable, which is used for connecting devices of the same type, such as two computers or two switches. Therefore, the technician should crimp the cable as a straight-through cable to fix the issue.

NEW QUESTION: 397

An organization set up its offices so that a desktop is connected to the network through a VoIP phone. The VoIP vendor requested that voice traffic be segmented separately from non-voice traffic. Which of the following would allow the organization to configure multiple devices with network isolation on a single switch port?

- A. Tunneling
- B. Link aggregation
- C. Load balancing
- D. Subinterfaces

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 398

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

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 399

A network technician crimped a length of UTP with TIA\EIA-568A on one end and TIA\EIA-568B on the other. Which of the following cable types did the technician create?

- A. Twinaxial cable

- B. Crossover cable
- C. Patch cable
- D. Rollover cable

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 400

Which of the following uses the destination IP address to forward packets?

- A. A router
- B. A bridge
- C. A Layer 2 switch
- D. A repeater

Answer: (SHOW ANSWER)

NEW QUESTION: 401

A network administrator is troubleshooting a connection to a remote site. The administrator runs a command and sees the following output:



Tracing route to 10.10.0.22 over a maximum of 30 hops:

Hop	1	2	3	4	5	6	7	8
Time	14ms	20ms	15ms	192.168.1.253	10ms	15ms	12ms	172.16.0.21
IP	10ms	15ms	12ms	10.10.5.3	10ms	15ms	12ms	10.12.2.1
IP	5ms	10ms	10ms	10.10.5.3	10ms	15ms	12ms	10.12.2.1
IP	10ms	15ms	12ms	10.10.5.3	10ms	15ms	12ms	10.12.2.1
IP	5ms	10ms	10ms	10.10.5.3	10ms	15ms	12ms	10.12.2.1
IP	10ms	15ms	12ms	10.10.5.3	10ms	15ms	12ms	10.12.2.1
IP	5ms	10ms	10ms	10.10.5.3	10ms	15ms	12ms	10.12.2.1
IP	10ms	15ms	12ms	10.10.5.3	10ms	15ms	12ms	10.12.2.1

The output shows a routing loop between two routers, 10.12.2.1 and 10.12.2.2, indicating a routing loop.

Which of the following is the cause of the connection issue?

- A. Routing loop
- B. Asymmetrical routing
- C. Broadcast storm
- D. Switching loop

Answer: (SHOW ANSWER)

Explanation

The cause of the connection issue is a routing loop. A routing loop is a situation where a packet is forwarded in circles between routers, never reaching its destination. A routing loop can be caused by misconfigured or inconsistent routing tables, or by routing protocols that do not update their information properly. A routing loop can be detected by using the traceroute command, which shows the path taken by a packet from the source to the destination. The traceroute output in the image shows that the packet is bouncing back and forth between two routers, 10.12.2.1 and 10.12.2.2, indicating a routing loop. References: CompTIA Network+ N10-008 Certification Study Guide, page 181; The Official CompTIA Network+ Student Guide (Exam N10-008), page 7-9.

NEW QUESTION: 402

Which of the following services can provide data storage, hardware options, and scalability to a third-party company that cannot afford new devices?

- A. SaaS
- B. IaaS
- C. PaaS
- D. DaaS

Answer: B ([LEAVE A REPLY](#))

IaaS is the better answer because DaaS require compatible devices thus the scalability is proportional to the availability of these devices. IaaS on the other hand is servers and one can scale those up in the background with just a click of the mouse.

NEW QUESTION: 403

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

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

Answer: (SHOW ANSWER)

The U.U.U.U is suppose to be 0.0.0.0 and A route when no other route matches.

The "gateway of last resort" meaning it needs a DG address.

NEW QUESTION: 404

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 ([LEAVE A REPLY](#))

"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: 405

A network engineer is interested in using wireless technologies in densely forested areas. Which of the following frequencies would be best for this use?

- A. 2.4GHz
- B. 5GHz
- C. 5.9GHz
- D. 6GHz

Answer: ([SHOW ANSWER](#))

2.4GHz frequency has better penetration and range than higher frequencies in forested environments, where there are many obstacles and interference sources.

Reference:

Wireless in The Woods: Experimental Evaluation of IEEE 802.11a/b/g in Forested Environments¹ High-Speed Wireless Access in Forested Rural Areas Using Analog Radio Over Fiber²

NEW QUESTION: 406

Which of the following would be BEST suited for a long cable run with a 40Gbps bandwidth?

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

Answer: ([SHOW ANSWER](#))

Cat 7 is a type of twisted-pair copper cable that supports up to 40 Gbps bandwidth and up to 100 meters cable length. Cat 7 is suitable for long cable runs that require high-speed data transmission. Cat 7 has better shielding and crosstalk prevention than lower categories of cables.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 407

Which of the following would be the MOST likely attack used to bypass an access control vestibule?

- A. Tailgating
- B. Phishing
- C. Evil twin
- D. Brute-force

Answer: A ([LEAVE A REPLY](#))

Tailgating would be the MOST likely attack used to bypass an access control vestibule. An access control vestibule is a physical security measure that requires individuals to go through a controlled space to access a secured area. Tailgating refers to the act of following closely behind someone who has been granted access to the controlled space, in an attempt to gain entry without proper authorization. Tailgating can be done intentionally or unintentionally, but in either case, it allows an unauthorized individual to gain access to the secured area.

NEW QUESTION: 408

To comply with an industry regulation, all communication destined to a secure server should be logged and archived on a storage device. Which of the following can be configured to fulfill this requirement?

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

Answer: B (LEAVE A REPLY)

Port mirroring is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port.

NEW QUESTION: 409

Which of the following situations would require an engineer to configure subinterfaces?

- A. In a router-on-a-stick deployment with multiple VLANs
- B. In order to enable inter-VLAN routing on a multilayer switch
- C. When configuring VLAN trunk links between switches
- D. After connecting a router that does not support 802.1Q VLAN tags

Answer: A (LEAVE A REPLY)

Explanation

A router-on-a-stick is a configuration that allows a single router interface to route traffic between multiple VLANs on a network. A router-on-a-stick requires sub-interfaces to be configured on the router interface, one for each VLAN. Each sub-interface is assigned a VLAN ID and an IP address that belongs to the corresponding VLAN subnet. The router interface is connected to a switch port that is configured as a trunk port, which allows traffic from multiple VLANs to pass through. The router then performs inter-VLAN routing by forwarding packets between the sub-interfaces based on their destination IP addresses.

Inter-VLAN routing is a process that allows devices on different VLANs to communicate with each other.

Inter-VLAN routing can be performed by a router-on-a-stick configuration, as explained above, or by a multilayer switch that has routing capabilities. A multilayer switch does not require sub-interfaces to be configured for inter-VLAN routing; instead, it uses switch virtual interfaces (SVIs) that are associated with each VLAN. An SVI is a logical interface that represents a VLAN on a switch and has an IP address that belongs to the VLAN subnet. The switch then performs inter-VLAN routing by forwarding packets between the SVIs based on their destination IP addresses.

VLAN trunking is a method that allows traffic from multiple VLANs to be carried over a single link between switches or routers. VLAN trunking requires the use of a tagging protocol, such as 802.1Q, that adds a header to each frame that identifies its VLAN ID. VLAN trunking does not require sub-interfaces to be configured on the

switches or routers; instead, it uses trunk ports that are configured to allow or deny traffic from specific VLANs. The switches or routers then forward packets between the trunk ports based on their VLAN IDs.

802.1Q is a standard that defines how VLAN tagging and trunking are performed on Ethernet networks.

802.1Q adds a 4-byte header to each frame that contains a 12-bit field for the VLAN ID and a 3-bit field for the priority level. 802.1Q does not require sub-interfaces to be configured on the switches or routers; instead, it uses trunk ports that are configured to support 802.1Q tagging and untagging. The switches or routers then forward packets between the trunk ports based on their VLAN IDs and priority levels.

NEW QUESTION: 410

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: [\(SHOW ANSWER\)](#)

Jumbo frames are larger than standard frames, fewer frames are needed and therefore CPU processing overhead is reduced. Jumbo frames are packets that are longer than the standard Ethernet (IEEE 802.3) frame size of 1,518 bytes.

NEW QUESTION: 411

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 100MB speed
- D. Full duplex and 100MB speed

Answer: [B \(LEAVE A REPLY\)](#)

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: 412

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

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

Answer: B ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 413

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: (SHOW ANSWER)

192.168.0.0/20 CIDR is in the third octet.

/1-8 (1st octet), /9-16 (2nd octet), /17-24 (3rd octet), /25-32 (4th octet).

/17 = 128

/18 = 192

/19 = 224

/20 = 240 is the answer

/21 = 248

/22 = 252

/23 = 254

/24 = 255

NEW QUESTION: 414

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 415

A technician is troubleshooting a previously encountered issue. Which of the following should the technician reference to find what solution was implemented to resolve the issue?

- A. Standard operating procedures
- B. Configuration baseline documents
- C. Work instructions
- D. Change management documentation

Answer: D (LEAVE A REPLY)

Change management documentation is a record of the changes that have been made to a system or process, including the reason, date, time, and impact of each change. A technician can reference this documentation to find what solution was implemented to resolve a previously encountered issue, as well as any potential side effects or dependencies of the change. References: <https://www.comptia.org/blog/what-is-change-management>

NEW QUESTION: 416

Which of the following technologies are certificates most commonly associated with?

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

Answer: A (LEAVE A REPLY)

Explanation

PKI stands for Public Key Infrastructure, which is a system of processes, technologies, and policies that allows you to encrypt and sign data using digital certificates¹. Digital certificates are issued by Certificate Authorities (CAs) and authenticate the identity of users, devices, or services that communicate online². Digital certificates also provide the means to encrypt and decrypt messages between sender and receiver using public and private keys²

NEW QUESTION: 417

A security engineer is installing a new IDS on the network. The engineer has asked a network administrator to ensure all traffic entering and leaving the router interface is available for the IDS.

Which of the following should the network administrator do?

- A. Install a loopback adapter for the IDS.
- B. Add an additional route on the router for the IDS.
- C. Install a network tap for the IDS
- D. Install an additional NIC into the IDS
- E. Configure ACLs to route traffic to the IDS.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 418

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: [\(SHOW ANSWER\)](#)

All SFP and SFP+ optics require LC connectors so the question becomes when you need single mode fiber or multi mode fiber but the connector type is clear. SC square connectors are too big to fit in a SFP or SFP+.

NEW QUESTION: 419

Which of the following record types would be used to define where SIP is found?

- A. SRV
- B. CNAME
- C. A
- D. MX

Answer: [C \(LEAVE A REPLY\)](#)

Explanation

The record type that would be used to define where SIP (Session Initiation Protocol) is found is A (Address). A record is a type of DNS (Domain Name System) record that maps a domain name to an IPv4 address. SIP is a protocol that enables voice over IP (VoIP) communication, such as voice calls or video conferencing. SIP uses domain names to identify endpoints or servers involved in a communication session. Therefore, an A record is needed to resolve the domain name of a SIP endpoint or server to its IPv4 address. References: CompTIA Network+ N10-008 Certification Study Guide, page 154; The Official CompTIA Network+ Student Guide (Exam N10-008), page 6-8.

NEW QUESTION: 420

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

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

Answer: [D \(LEAVE A REPLY\)](#)

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

NEW QUESTION: 421

A help desk technician discovers the following note while reviewing tickets in a customer's account:

Was able to confirm customer's problem with the system. Will upgrade system to latest version and monitor for further connectivity problems per developer's instructions.

Which of the following describes what the technician was documenting with this note?

- A. The technician was approaching multiple problems individually.
- B. The technician was establishing a plan of action and identifying potential effects.

- C. The technician was testing a theory to determine the cause.
- D. The technician was identifying the problem by gathering information.

Answer: D (LEAVE A REPLY)

Explanation

The technician was identifying the problem by gathering information with this note. This is the first step of the troubleshooting methodology, which is a systematic process of finding and resolving issues in a network or system. By gathering information, the technician can understand the symptoms, scope, and impact of the problem, as well as collect relevant data from various sources, such as users, logs, tools, or documentation. The note shows that the technician was asking questions to the user, checking the network status and configuration, and reviewing previous tickets to gather information about the problem. References: [CompTIA Network+ Certification Exam Objectives], Troubleshooting Methodology - CompTIA Network+ N10-007 - 1.4 | Professor Messer IT Certification Training Courses

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 422

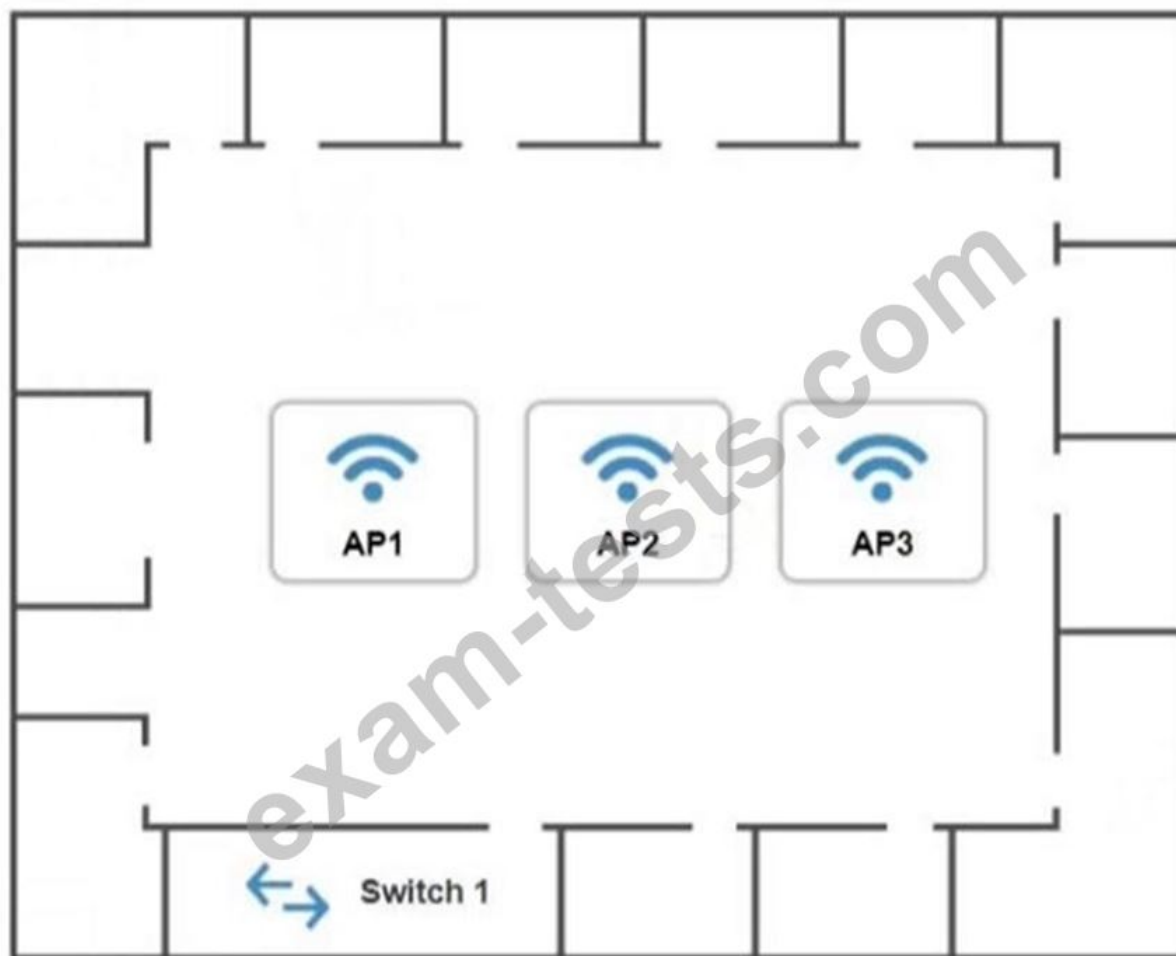
SIMULATION

You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

The SSIDs need to be configured as CorpNet with a key of S3cr3t!

The wireless signals should not interfere with each other

The subnet the Access Points and switch are on should only support 30 devices maximum The Access Points should be configured to only support TKIP clients at a maximum speed INSTRUCTIONS Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



192.168.1.2
Speed: Auto
Duplex: Auto

CompTIA®

AP1 Configuration



https://ap1.setup.do

Basic Configuration

Access Point Name

IP Address /

Gateway

SSID

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

Channel

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

AP2 Configuration



https://ap2.setup.do

Basic Configuration

Access Point Name

AP2

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast



Yes



No

Wireless

Mode

B
G

Channel

1
2
3
4
5
6
7
8
9
10
11

Wired

Speed



Auto



100



1000

Duplex



Auto



Half



Full

Security Configuration

Security Settings



None



WEP



WPA



WPA2



WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

AP3 Configuration



https://ap3.setup.do

Basic Configuration

Access Point Name

AP3

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B
G

Channel

1
2
3
4
5
6
7
8
9
10
11

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

CompTIA

Answer:

See explanation below.

Explanation

On the first exhibit, the layout should be as follows

AP1 Configuration

https://ap1.setup.do

Basic Configuration

Access Point Name

AP1

IP Address

192.168.1.32

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

Yes

No

Wireless

Mode

B

Channel

3

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Graphical user interface, text, application, chat or text message Description automatically generated

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

S3cr3t

Graphical user interface Description automatically generated

AP1 Configuration

https://ap1.setup.do

IP Address

192.168.1.32

/

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

Yes

No

Wireless

Mode

B

Channel

3

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

S3cr3t

Graphical user interface, text, application, chat or text message Description automatically generated

Graphical user interface Description automatically generated

AP1 Configuration **CompTIA**

https://ap1.setup.do

IP Address 192.168.1.3 / 27

Gateway 192.168.1.1

SSID CorpNet

SSID Broadcast ☒ Yes ☐ No

Wireless

Mode G

Channel 3

Wired

Speed ☒ Auto ☐ 100 ☐ 1000

Duplex ☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings ☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase S3cr3t!

Reset to Default Save Close

Exhibit 2 as follows

Access Point Name AP2

Graphical user interface Description automatically generated

AP2 Configuration

https://ap2.setup.do

Basic Configuration

Access Point Name: AP2

IP Address: 192.168.1.64 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☐ Yes ☐ No

Wireless

Mode: B

Channel: 6

Wired

Speed: ☐ Auto ☒ 100 ☐ 1000

Duplex: ☐ Auto ☐ Half ☒ Full

Security Configuration

Reset to Default Save Close

Graphical user interface, text, application, chat or text message Description automatically generated

Security Configuration

Security Settings: ☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase: S3cr3t

Graphical user interface Description automatically generated

AP2 Configuration

←

→

↻

https://ap2.setup.do

IP Address

192.168.1.4 / 27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes

☐ No

Wireless

Mode

G

Channel

6

Wired

Speed

☒ Auto

☐ 100

☐ 1000

Duplex

☒ Auto

☐ Half

☐ Full

Security Configuration

Security Settings

☐ None

☐ WEP

☒ WPA

☐ WPA2

☐ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Reset to Default

Save

Close

Exhibit 3 as follows

Access Point Name AP3

Graphical user interface Description automatically generated

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name: AP3

IP Address: 192.168.1.96 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode: B

Channel: 9

Wired

Speed: ☐ Auto ☒ 100 ☐ 1000

Duplex: ☐ Auto ☐ Half ☒ Full

Security Configuration

Reset to Default Save Close

Graphical user interface, text, application, chat or text message Description automatically generated

Security Configuration

Security Settings: ☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase: S3cr3t

Graphical user interface Description automatically generated

AP3 Configuration

https://ap3.setup.do

IP Address: 192.168.1.5 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode: G

Channel: 9

Wired

Speed: ☒ Auto ☐ 100 ☐ 1000

Duplex: ☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings: ☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase: S3cr3t!

Reset to Default Save Close

NEW QUESTION: 423

Which of the following attacks becomes more effective because of global leakages of users' passwords?

- A. Deauthentication
- B. Brute-force
- C. Dictionary
- D. Phishing

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 424

A customer needs to distribute Ethernet to multiple computers in an office. The customer would like to use non-proprietary standards. Which of the following blocks does the technician need to install?

110

66

- A. BiX
- B. Krone

Answer: A (LEAVE A REPLY)

Explanation

A 110 block is a type of punch-down block that is used to terminate twisted-pair cables in Ethernet networks. It is a non-proprietary standard that is widely used in structured cabling systems for voice and data applications. A 110 block can support up to 100 MHz of bandwidth and can be used with Cat 3, Cat 5, Cat 5e, and Cat 6 cables¹².

A 66 block is another type of punch-down block that is mainly used for telephone wiring. It is an older and less reliable standard than the 110 block and does not support high-speed data transmission³. A BiX block is a proprietary punch-down block that is developed by NORDX/CDT and is mostly used in Canada. It can support up to 250 MHz of bandwidth and can be used with Cat 5e and Cat 6 cables⁴. A Krone block is another proprietary punch-down block that is developed by ADC Krone and is mostly used in Europe. It can support up to 100 MHz of bandwidth and can be used with Cat 5 and Cat 5e cables.

Therefore, the best option for the customer who wants to use non-proprietary standards is the 110 block.

NEW QUESTION: 425

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. VLAN
- C. Errors
- D. Duplex

Answer: A (LEAVE A REPLY)

NEW QUESTION: 426

A security administrator is trying to prevent incorrect IP addresses from being assigned to clients on the network. Which of the following would MOST likely prevent this and allow the network to continue to operate?

- A. Configuring DHCP snooping on the switch
- B. Preventing broadcast messages leaving the client network
- C. Blocking ports 67/68 on the client network
- D. Enabling port security on access ports

Answer: A (LEAVE A REPLY)

To prevent incorrect IP addresses from being assigned to clients on the network and allow the network to continue to operate, the security administrator should consider configuring DHCP (Dynamic Host Configuration Protocol) snooping on the switch. DHCP snooping is a security feature that is used to prevent unauthorized DHCP servers from operating on a network. It works by allowing the switch to monitor and validate DHCP traffic on the network, ensuring that only legitimate DHCP messages are forwarded to clients. This can help to prevent

incorrect IP addresses from being assigned to clients, as it ensures that only authorized DHCP servers are able to provide IP addresses to clients on the network.

NEW QUESTION: 427

Which of the following steps of the troubleshooting methodology would most likely include checking through each level of the OSI model after the problem has been identified?

- A. Establish a theory.
- B. Verify functionality
- C. Implement the solution.
- D. Create a plan of action.

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 428

A network technician is troubleshooting internet connectivity issues with users in a subnet. From a host, the technician runs `nslookup` and then attempts to navigate to a website using a web browser.

The technician receives the following output:

```
16:35:58.756583 IP (tos 0x0, ttl 64, id 56522, offset 0, flags [DF], proto UDP (17), length 57)
  192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
16:35:58.835371 IP (tos 0x0, ttl 64, id 56523, offset 0, flags [DF], proto UDP (17), length 57)
  192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
16:35:59.652312 IP (tos 0x0, ttl 64, id 56524, offset 0, flags [DF], proto UDP (17), length 57)
  192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
16:36:00.765212 IP (tos 0x0, ttl 64, id 56525, offset 0, flags [DF], proto UDP (17), length 57)
  192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
```

Afterward, the browser displays an error. Which of the following explains this issue?

- A. A routing loop is within the network.
- B. The host is configured with incorrect DNS settings
- C. A broadcast storm is occurring on the subnet
- D. The host is missing a route to the website.

Answer: [B \(LEAVE A REPLY\)](#)

Explanation

The issue is that the host is configured with incorrect DNS settings. DNS (Domain Name System) is a service that resolves domain names to IP addresses. For example, the domain name `www.comptia.org` is resolved to the IP address `104.18.25.140` by a DNS server. If the host has incorrect DNS settings, such as an invalid or unreachable DNS server address, it will not be able to resolve domain names to IP addresses, and therefore it will not be able to access websites by their names. The output in the image shows that the host can ping the IP address of `www.comptia.org`, but it cannot ping the domain name itself, indicating a DNS problem. References: CompTIA Network+ N10-008 Certification Study Guide, page 154; The Official CompTIA Network+ Student Guide (Exam N10-008), page 6-8.

NEW QUESTION: 429

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 ([LEAVE A REPLY](#))

TACACS+ (Terminal Access Controller Access Control System Plus) can be used to centrally manage credentials for various types of administrative privileges on configured network devices. This protocol separates authentication, authorization, and accounting (AAA) functions, providing more granular control over access to network resources.

References:

* Network+ N10-007 Certification Exam Objectives, Objective 4.2: Given a scenario, implement secure network administration principles.

NEW QUESTION: 430

A firewall administrator is implementing a rule that directs HTTP traffic to an internal server listening on a non-standard socket.

Which of the following types of rules is the administrator implementing?

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

Answer: ([SHOW ANSWER](#)**)**

Static Network Address Translation (SNAT) would be used to translate from one address to another. The question asks how to convert from one port to another; this is called Port Address Translation (PAT).

NEW QUESTION: 431

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 ([LEAVE A REPLY](#))

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: 432

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 of 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: [\(SHOW ANSWER\)](#)

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.

NEW QUESTION: 433

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

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

Answer: A [\(LEAVE A REPLY\)](#)

NEW QUESTION: 434

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

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

Answer: D [\(LEAVE A REPLY\)](#)

A cold site is a recovery solution that provides a physical location with minimal or no equipment, power, or network connectivity. It is the cheapest option among the four choices, but it also requires the most time and effort to restore the applications and data in the event of a disaster¹².

A warm site is a recovery solution that provides a physical location with some equipment, power, and network connectivity, but not enough to run all the applications and data. It is more expensive than a cold site, but it also reduces the recovery time and data loss¹².

A hot site is a recovery solution that provides a physical location with fully functional equipment, power, and network connectivity, as well as a replica of the applications and data. It is the most expensive option among the four choices, but it also offers the fastest recovery time and minimal data loss¹².

A cloud site is a recovery solution that uses a cloud service provider to host the applications and data. It can offer various levels of availability, scalability, and cost, depending on the service model and the service level agreement. It can also reduce the need for physical infrastructure and maintenance¹³.

For lower-priority applications, a company may choose a cold site as the most cost-effective recovery solution, as it does not require a large upfront or ongoing investment. However, the company should also consider the trade-off between cost and recovery time, as a cold site may take longer to restore the applications and data than other solutions. The company should also have a backup strategy to ensure that the data can be retrieved from a secure location¹². Reference:

- 1: CompTIA Network+ N10-008 Certification Study Guide, Chapter 11: Network Operations, Section 11.4: Disaster Recovery²
- 2: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 51: Disaster Recovery⁴
- 3: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 52: Cloud Computing⁴
- 4: Professor Messer's CompTIA Network+ N10-008 Training Course⁵

NEW QUESTION: 435

A company is upgrading the network switches at its backup data center, which is geographically separated from the main data center. The company hired a contractor to physically install and cable the new switches in their cabinets. Which of the following should the network engineering team provide to ensure the job is completed accurately?

- A. Logical diagram
- B. Rack diagram
- C. Site survey
- D. IDF diagram

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 436

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 receiving too many packets.
- B. The switchport does not have enough CRCs

- C. The connected device is exceeding the configured MTU.
- D. The connected device is sending too many packets
- E. The switchport has been up for too long

Answer: ([SHOW ANSWER](#))

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 437

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.

A company is moving to a new building designed with a guest waiting area that has existing network ports. Which of the following practices would BEST secure the network?

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

Answer: B ([LEAVE A REPLY](#))

One of the best practices to secure the network would be to disable unneeded switchports in the guest waiting area. This will prevent unauthorized users from connecting to the network through these ports. It's important to identify which switchports are not in use and disable them, as this will prevent unauthorized access to the network.

Other practices such as ensuring all guests sign an NDA, lowering the radio strength to reduce Wi-Fi coverage in the waiting area and enabling MAC filtering to block unknown hardware addresses are not as effective in securing the network as disabling unneeded switchports. Enforcing an NDA with guests may not stop a malicious user from attempting to access the network, reducing the radio strength only limits the Wi-Fi coverage, and MAC filtering can be easily bypassed by hackers.

NEW QUESTION: 438

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 ([LEAVE A REPLY](#))

Neighbor Discovery Protocol is similar to ARP but retrieves the IPV6 address. ARP retrieves IPv4.

NEW QUESTION: 439

Which of the following refers to a weakness in a mechanism or technical process?

- A. Vulnerability
- B. Risk
- C. Exploit
- D. Threat

Answer: ([SHOW ANSWER](#))

The term that refers to a weakness in a mechanism or technical process is vulnerability. A vulnerability is a flaw or gap in a system's security that can be exploited by an attacker to gain unauthorized access, compromise data, or cause damage. A vulnerability can be caused by design errors, configuration errors, software bugs, human errors, or environmental factors. For example, an outdated software version that has known security holes is a vulnerability that can be exploited by malware or hackers. References: CompTIA Network+ N10-008 Certification Study Guide, page 342; The Official CompTIA Network+ Student Guide (Exam N10-008), page 13-7.

NEW QUESTION: 440

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

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

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 441

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 ([LEAVE A REPLY](#))

Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

NEW QUESTION: 442

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

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

Answer: D ([LEAVE A REPLY](#))

Explanation

A split-tunnel VPN is a configuration where only specific traffic is routed through a VPN, while the remaining data is sent directly over the internet. This can reduce the bandwidth consumption and cost of the company's internet connection, as cloud-based traffic does not need to pass through the VPN tunnel. A web filter, monitoring, and security are not advantages of a split-tunnel VPN, as they may require all traffic to go through the VPN.

<https://www.auvik.com/franklyit/blog/vpn-split-tunneling/>

NEW QUESTION: 443

A technician is troubleshooting a network switch that seems to stop responding to requests intermittently whenever the logging level is set for debugging. Which of the following metrics should the technician check to begin troubleshooting the issue?

- A. Audit logs
- B. Jitter
- C. CPU utilization
- D. CRC errors

Answer: (SHOW ANSWER)

NEW QUESTION: 444

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

```
Ethernet Adapter:
Physical Address    AB-CD-EF-12-34-56
DHCP Enabled       No
IPv4 Address       192.168.1.55
Subnet Mask        225.225.225.224
Default Gateway    192.168.1.1
DHCP Server        192.168.1.1
DNS Server         192.168.1.1
```

Which of the following is misconfigured?

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

Answer: A ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 445

A user reports that the internet seems slow on a workstation, but no other users have reported any issues. The server team confirms the servers are functioning normally. A technician suspects something specific to the user's computer is overutilizing bandwidth. Which of the following commands should the technician use to further investigate the issue?

- A. nmap
- B. tcpdump
- C. netstat
- D. nslookup

Answer: C ([LEAVE A REPLY](#))

netstat is a command-line tool that displays network connections, routing tables, interface statistics, and more. It can help the technician identify which processes or applications are using the network bandwidth on the user's computer. netstat can also show the current bandwidth usage in bytes per second for each network interface.

References

- * netstat - Wikipedia provides an overview of the netstat tool and its features.
- * How to get current bandwidth usage from command line using built-in Linux tools? - Super User explains how to use netstat and other tools to monitor bandwidth usage on Linux systems.
- * Get network utilization from command line - Super User shows how to use typeperf and other tools to monitor bandwidth usage on Windows systems.

NEW QUESTION: 446

An organization has experienced an increase in malicious spear-phishing campaigns and wants to mitigate the risk of hyperlinks from inbound emails.

Which of the following appliances would best enable this capability?

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

Answer: A ([LEAVE A REPLY](#))

Sandbox

Explanation:

An email protection gateway is an appliance that can filter and block malicious emails and attachments before they reach the recipients. An email protection gateway can mitigate the risk of hyperlinks from inbound emails by scanning the links for malicious content, rewriting the links to point to a safe domain, or blocking the links altogether. An email protection gateway can also perform other functions such as spam filtering, antivirus scanning, encryption, and data loss prevention. A DNS server, a proxy server, an endpoint email client, and a sandbox are not appliances that can enable this capability, as they have different purposes and functions.

Reference

1: CompTIA Network+ N10-008 Certification Study Guide, page 304

2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 15

3: CompTIA Network+ N10-008 Certification Practice Test, question 5

4: Email Protection Gateway - N10-008 CompTIA Network+ : 3.2

NEW QUESTION: 447

Which of the following documents dictates the uptimes that were agreed upon by the involved parties?

- A. MOU
- B. BYOD
- C. SLA
- D. NDA

Answer: C (LEAVE A REPLY)

An SLA (Service Level Agreement) is a document that defines the expected level of service and performance guaranteed by a service provider to a customer. It usually specifies metrics such as uptime, availability, reliability, response time, and compensation or penalties for not meeting the agreed standards. An SLA is a way of ensuring that both parties are clear about their roles and responsibilities, and that the customer receives the quality of service they paid for.

NEW QUESTION: 448

A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio.

Which of the following antenna types should the AP utilize?

- A. Omni
- B. Directional
- C. Yagi
- D. Parabolic

Answer: A (LEAVE A REPLY)

Explanation

An omni antenna should be used by the AP to provide service in a radius surrounding a radio. An omni antenna is a type of antenna that has a 360-degree horizontal radiation pattern. It can provide wireless coverage in all directions from the antenna with varying degrees of vertical coverage. It is suitable for indoor environments where users are located around the AP

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html> 1

NEW QUESTION: 449

A company that uses VoIP telephones is experiencing intermittent issues with one-way audio and dropped conversations. The manufacturer says the system will work if ping times are less than 50ms. The company has recorded the following ping times:

10ms	10ms	10ms	100ms	70ms	5ms	5ms	80ms	100ms	5ms	5ms

Which of the following is MOST likely causing the issue?

- A. Attenuation
- B. Latency
- C. VLAN mismatch
- D. Jitter

Answer: (SHOW ANSWER)

Explanation

Jitter is most likely causing the issue of intermittent one-way audio and dropped conversations for the company that uses VoIP telephones. Jitter is a variation in delay of packets arriving at the destination. It can cause choppy or distorted audio quality for VoIP applications, especially over WAN links that have limited bandwidth and high latency. The recommended jitter for VoIP is less than 10ms¹. The company has recorded ping times that exceed 50ms, which indicates high jitter and latency on their network. References:

<https://www.voip-info.org/voip-jitter/> 1

NEW QUESTION: 450

An administrator would like to create a fault-tolerant ring between three switches within a Layer 2 network.

Which of the following Ethernet features should the administrator employ?

- A. Spanning Tree Protocol
- B. Open Shortest Path First
- C. Port mirroring
- D. An interior gateway protocol

Answer: A (LEAVE A REPLY)

Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology in Ethernet networks by actively blocking certain links and enabling others. STP prevents loops by putting some of the links in a blocking state, effectively creating a loop-free topology. This ensures that there is only one active path between two devices, which helps prevent network loops and the associated problems (such as broadcast storms) that can result from them. STP is used to create a fault-tolerant ring between three switches within a Layer 2 network.

NEW QUESTION: 451

An engineer is using a tool to run an ICMP sweep of a network to find devices that are online. When reviewing the results, the engineer notices a number of workstations that are currently verified as being online are not listed in the report.

The tool was configured to scan using the following information:

Network address: 172.28.16.0

CIDR: /22

The engineer collected the following information from the client workstation:

IP address: 172.28.17.206

Subnet mask: 255.255.252.0

Which of the following MOST likely explains why the tool is failing to detect some workstations?

- A. The scanned network range is incorrect.
- B. The subnet mask on the client is misconfigured.
- C. The workstation has a firewall enabled.
- D. The tool is unable to scan remote networks.

Answer: C (LEAVE A REPLY)

Explanation

A firewall is a device or software that filters and controls the incoming and outgoing network traffic based on predefined rules. A firewall can block ICMP packets, which are used for ping and other diagnostic tools. If the workstation has a firewall enabled, it may not respond to the ICMP sweep and appear as offline. The engineer should check the firewall settings on the workstation and allow ICMP traffic if needed.

References: Network+ Study Guide Objective 4.1: Given a scenario, use the appropriate tool.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 452

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

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

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

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

Answer: A,D (LEAVE A REPLY)

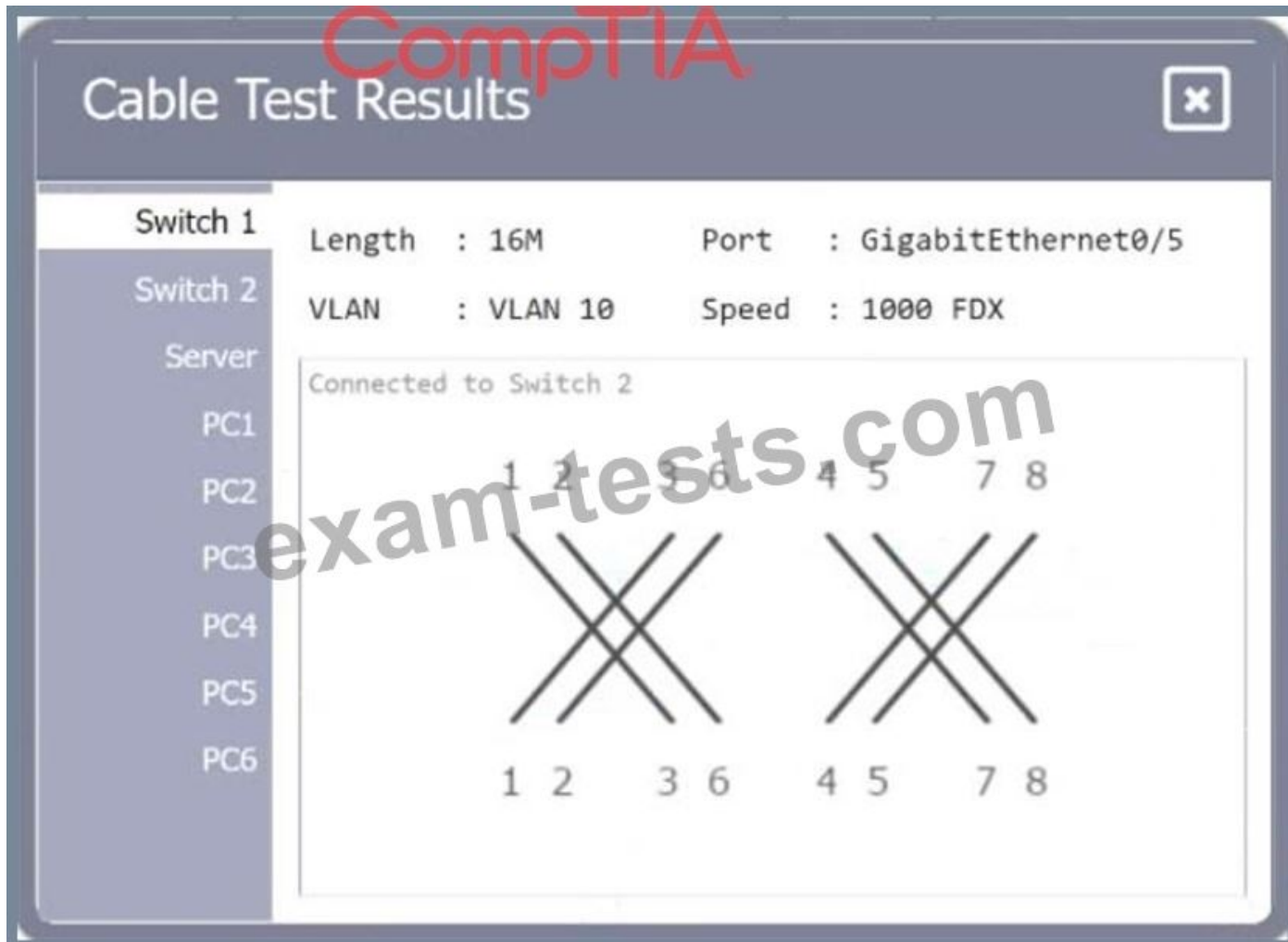
NEW QUESTION: 453

A network technician needs to resolve some issues with a customer's SOHO network. The customer reports that some of the PCs are not connecting to the network, while others appear to be working as intended.

INSTRUCTIONS

Review the cable test results first, then diagnose by clicking on the appropriate PC, server, and Layer 2 switch. Identify any components with a problem and recommend a solution to correct each problem.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Cable Test Results



Switch 1

Length : 42M

Port : GigabitEthernet0/2

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

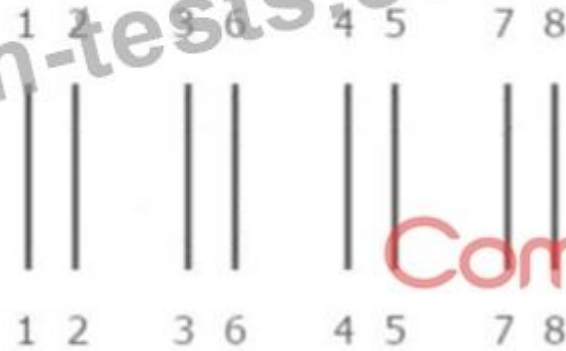
PC2

PC3

PC4

PC5

PC6



Cable Test Results



Switch 1

Length : 12M

Port : GigabitEthernet0/1

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

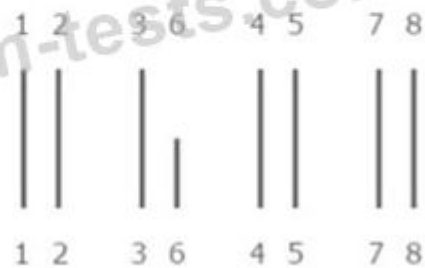
PC2

PC3

PC4

PC5

PC6



Cable Test Results

CompTIA

Switch 1

Switch 2

Server

PC1

PC2

PC3

PC4

PC5

PC6

Length : 20M

Port : GigabitEthernet0/2

VLAN : VLAN 10

Speed : 1000 FDX

1 2 3 6 4 5 7 8

1 2 3 6 4 5 7 8

Cable Test Results

CompTIA

Switch 1

Switch 2

Server

PC1

PC2

PC3

PC4

PC5

PC6

Length : 18M

Port : GigabitEthernet0/3

VLAN : VLAN 11

Speed : 1000 FDX

1 2 3 6 4 5 7 8

1 2 3 6 4 5 7 8

Cable Test Results



Switch 1

Length : 33M

Port : GigabitEthernet0/4

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

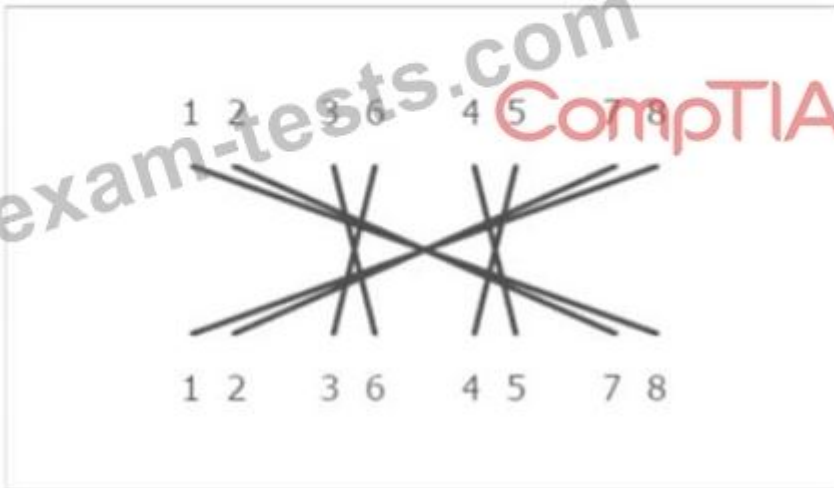
PC2

PC3

PC4

PC5

PC6



Cable Test Results



Switch 1

Length : 90M

Port : GigabitEthernet0/3

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

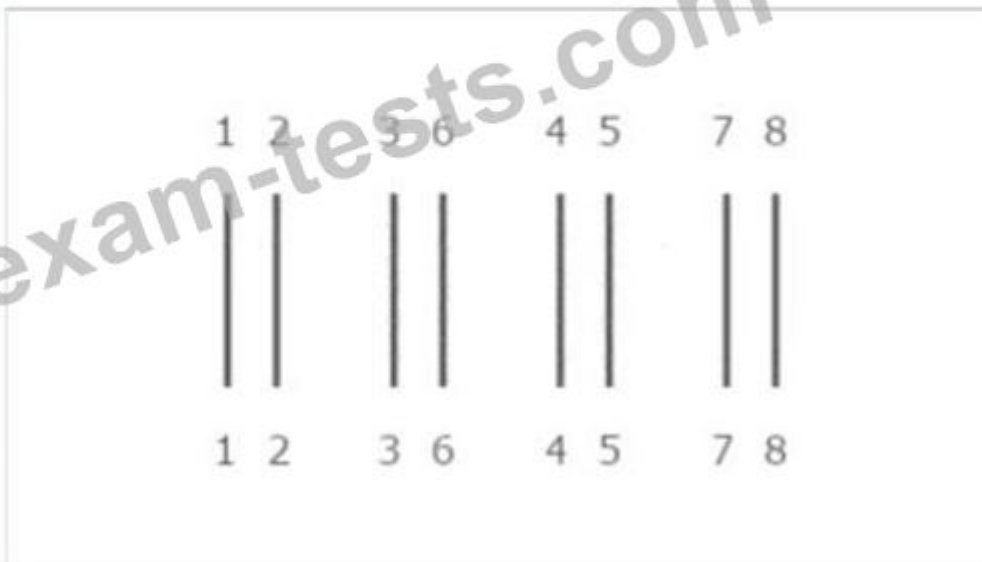
PC2

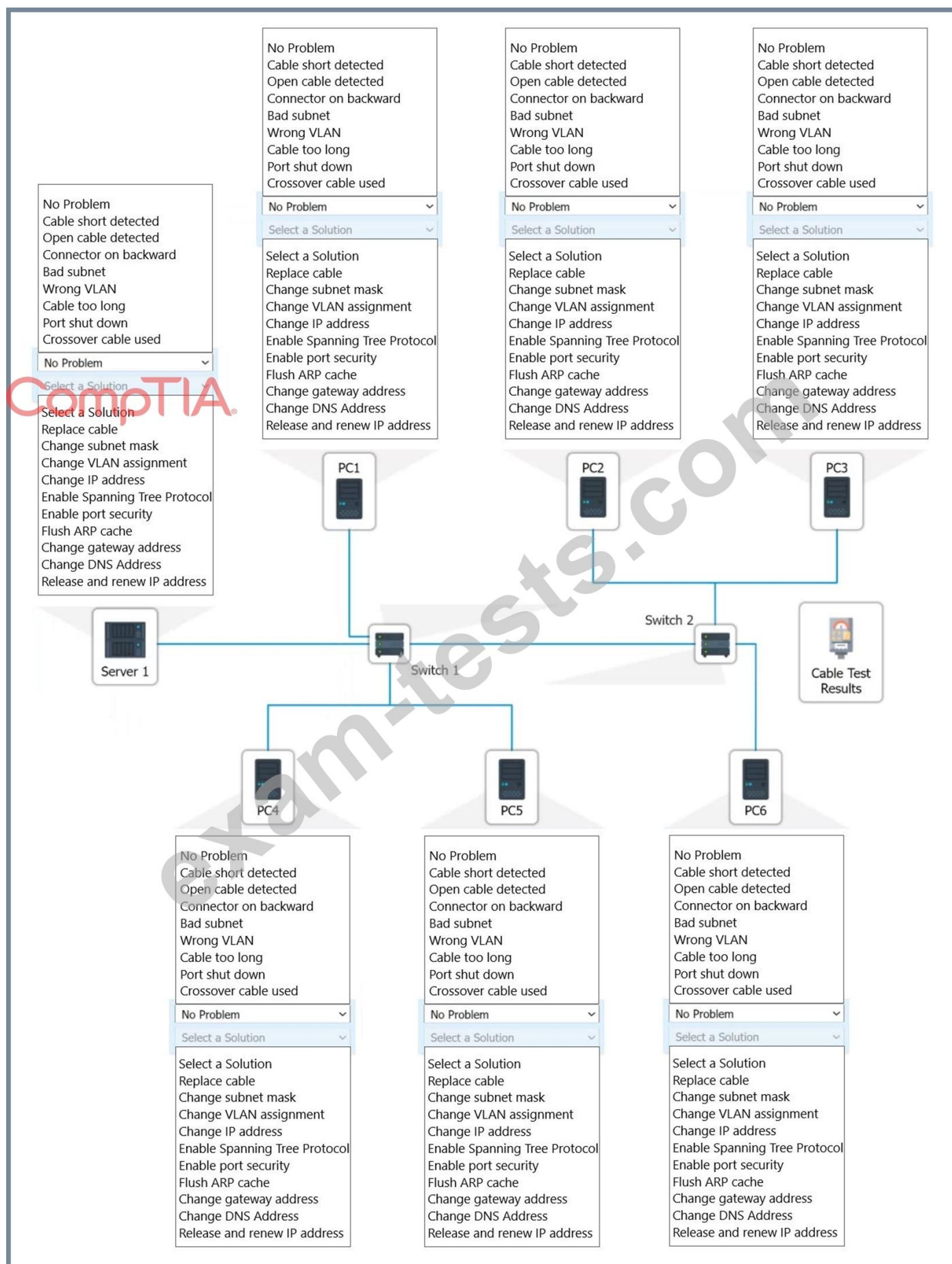
PC3

PC4

PC5

PC6

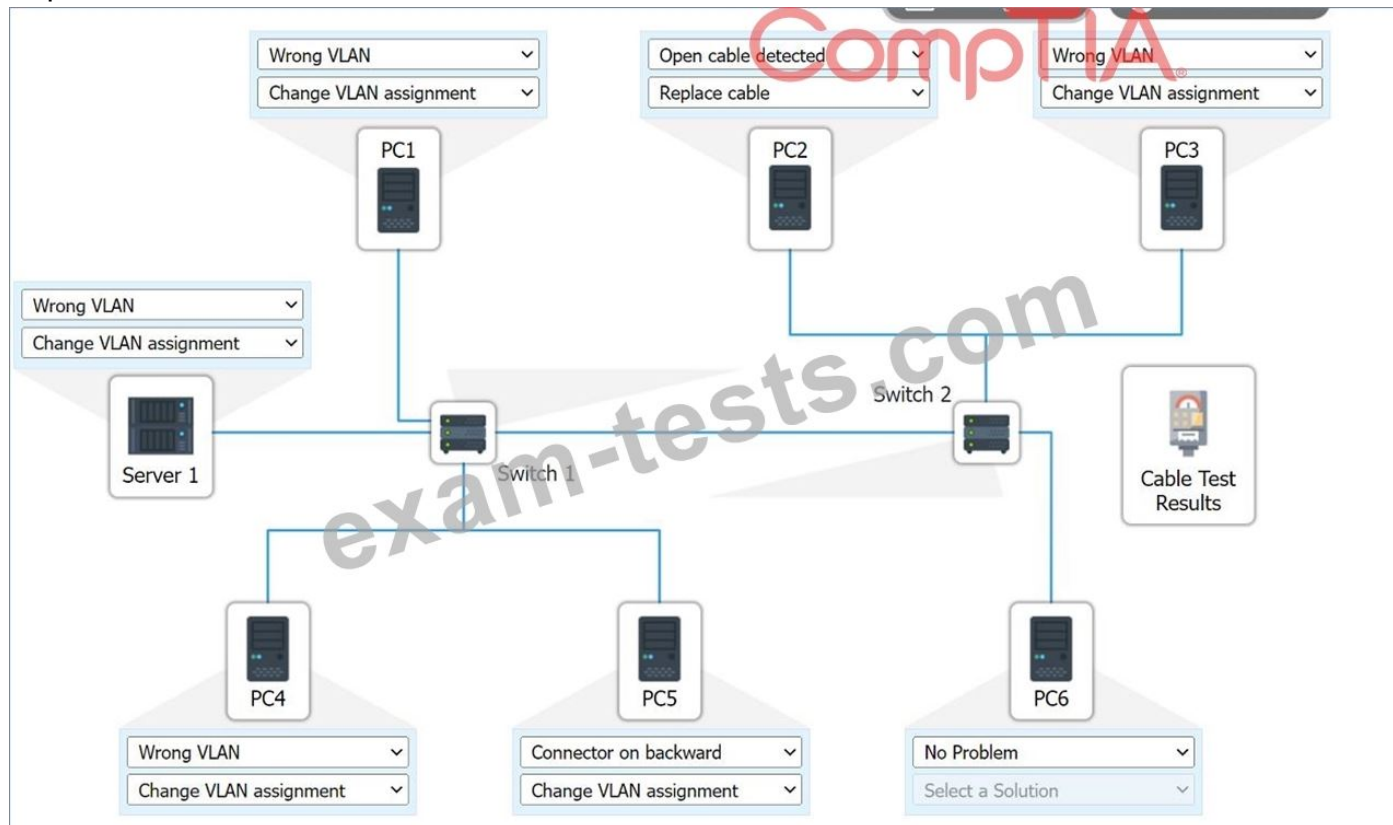




Answer:

See the solution configuration below in Explanation

Explanation:



NEW QUESTION: 454

A company is contracting a new third-party organization that will handle storage of the company's critical data. Which of the following policies would ensure the data remains confidential?

- A. BYOD
- B. MOU
- C. NDA
- D. SLA

Answer: (SHOW ANSWER)

NEW QUESTION: 455

A network administrator is installing a new server in the data center. The administrator is concerned the amount of traffic generated will exceed 1GB, and higher-throughput NiCs are not available for installation. Which of the following is the BEST solution for this issue?

- A. Remove some of the applications from the server.
- B. Install an additional NIC and configure LACP.
- C. Configure the NIC to use full duplex
- D. Install a SSD to decrease data processing time.
- E. Configure port mirroring to send traffic to another server.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 456

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

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

Answer: ([SHOW ANSWER](#))

ipconfig = IP address, Subnet, Gateway, and DNS PREFIX

ipconfig /all = IP address, Subnet, Gateway, AND DNS ADDRESS.

NEW QUESTION: 457

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

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

Answer: ([SHOW ANSWER](#))

https://www.cisco.com/c/en/us/td/docs/optical/cpt/r9_3/command/reference/cpt93_cr/cpt93_cr_chapter_01000.html

NEW QUESTION: 458

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

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

Answer: A ([LEAVE A REPLY](#))

Explanation

RDP (Remote Desktop Protocol) is the best option for a network technician to use when installing new software on a Windows-based server in a different geographical location. This protocol allows the technician to connect to the server remotely and control it as if they were physically present.

References:

Network+ N10-007 Certification Exam Objectives, Objective 2.2: Given a scenario, implement the appropriate network-based security and troubleshoot common connectivity issues.

NEW QUESTION: 459

Which of the following protocols can be routed?

- A. FCoE
- B. Fibre Channel
- C. iSCSI

D. NetBEUI

Answer: C ([LEAVE A REPLY](#))

iSCSI is a routable protocol that uses TCP/IP to transport SCSI commands over IP networks.

FCoE and Fibre Channel are non-routable protocols that use Ethernet or optical fiber to transport SCSI commands over LANs or SANs. NetBEUI is a non-routable protocol that uses broadcasts to transport NetBIOS commands over LANs.

NEW QUESTION: 460

Which of the following must be functioning properly in order for a network administrator to create an accurate timeline during a troubleshooting process?

A. NTP

B. IP helper

C. Syslog

D. MySQL

Answer: ([SHOW ANSWER](#))

* The Network Time Protocol (NTP) is a protocol that synchronizes the clocks of network devices and servers over the internet or a local network¹². NTP uses a hierarchical system of time sources, where the most accurate and authoritative time servers are at the top level (stratum 0) and lower-level servers (stratum 1 to 15) obtain and distribute time information from them³⁴.

* NTP is essential for creating an accurate timeline during a troubleshooting process, because it ensures that all network devices and servers have the same and correct time settings⁵⁶. This allows the network administrator to correlate and analyze the logs, events, and alerts from different sources and identify the root cause and impact of the network issues⁷⁸.

* The other options are not relevant for creating an accurate timeline during a troubleshooting process. The IP helper is a feature that allows a router to forward DHCP requests from clients to a DHCP server on a different network segment⁹. The Syslog is a standard for logging and monitoring network events and messages from different devices and applications. The MySQL is a relational database management system that can store and manipulate data from various sources. These options do not affect the time synchronization of the network devices and servers, which is the key factor for creating an accurate timeline.

References:

* 1: CompTIA Network+ N10-008 Certification Study Guide, page 213

* 2: CompTIA Network+ Certification Exam Objectives, page 9

* 3: [What is Network Time Protocol (NTP)? - Definition from WhatIs.com]

* 4: [Network Time Protocol (NTP) | CompTIA IT Certifications]

* 5: [Why is NTP Important? | Network Time Foundation]

* 6: [Why NTP is important for network troubleshooting | Network World]

* 7: [How to Troubleshoot Network Problems with NTP and Chrony | Linux Journal]

* 8: [Network Troubleshooting Using NTP | Pluralsight]

* 9: CompTIA Network+ N10-008 Certification Study Guide, page 216

* : [What is IP Helper? - Definition from Techopedia]

* : CompTIA Network+ N10-008 Certification Study Guide, page 217

- * : [What is Syslog? - Definition from WhatIs.com]
- * : [What is MySQL? - Definition from WhatIs.com]
- * : [MySQL | CompTIA IT Certifications]

NEW QUESTION: 461

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 (LEAVE A REPLY)

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: 462

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 (LEAVE A REPLY)

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: 463

Which of the following types of datacenter architectures will MOST likely be used in a large SDN and can be extended beyond the datacenter? (Choose two.)

- A. Spine and leaf
- B. iSCSI

- C. FCoE
- D. Three-tiered network
- E. Top-of-rack switching

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 464

Which of the following is used to elect an STP root?

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

Answer: B ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 465

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

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

Answer: C ([LEAVE A REPLY](#))

Option A (disabling the SSID broadcast on the WAP in the patio area) would not necessarily improve connectivity in the patio, and it could make it more difficult for users to connect to the wireless network. Option B (enabling 5GHz only within the patio area) might improve connectivity for devices that support the 5GHz frequency band, but it would not help devices that only support the 2.4GHz frequency band. Option D (installing a repeater on the back wall of the patio area) might help to extend the range of the wireless network, but it would not necessarily improve connectivity for users in the patio.

NEW QUESTION: 466

A network administrator is installing a wireless network at a client's office. Which of the following IEEE 802.11 standards would be BEST to use for multiple simultaneous client access?

- A. CDMA
- B. CSMA/CD
- C. CSMA/CA

D. GSM

Answer: ([SHOW ANSWER](#))

Explanation

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is an IEEE 802.11 standard that would be best to use for multiple simultaneous client access on a wireless network. CSMA/CA is a media access control method that allows multiple devices to share the same wireless channel without causing collisions or interference. It works by having each device sense the channel before transmitting data and waiting for an acknowledgment from the receiver after each transmission. If the channel is busy or no acknowledgment is received, the device will back off and retry later with a random delay. References:

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-csma-ca.html>

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 467

An administrator is investigating reports of network slowness in a building. While looking at the uplink interface statistics in the switch's CLI, the administrator discovers the uplink is at 100% utilization. However, the administrator is unsure how to identify what traffic is causing the saturation. Which of the following tools should the administrator utilize to identify the source and destination addresses of the traffic?

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

Answer: ([SHOW ANSWER](#))

Explanation

To identify the source and destination addresses of the traffic causing network saturation, the network administrator should use a network protocol analyzer that supports the NetFlow protocol. NetFlow is a network protocol that collects IP traffic information as it enters or exits an interface and sends it to a NetFlow collector for analysis. This data includes the source and destination addresses of the traffic, the ports used, and the number of bytes and packets transferred.

Therefore, the correct answer is option D, NetFlow.

Reference: CompTIA Network+ Study Guide, Exam N10-007, Fourth Edition, by Todd Lammle (Chapter 6: Network Devices)

NEW QUESTION: 468

Which of the following technologies allows traffic to be sent through two different ISPs to increase performance?

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 469

A network device is configured to send critical events to a syslog server; however, the following alerts are not being received:

Severity 5 LINK-UPDOWN: Interface 1/1, changed state to down

Severity 5 LINK-UPDOWN: Interface 1/3, changed state to down

Which of the following describes the reason why the events are not being received?

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

Answer: A ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 470

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

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

Answer: C ([LEAVE A REPLY](#))

Explanation

Port mirroring is a feature that can be used to enable monitoring of all packets arriving at an interface. This feature is used to direct a copy of all traffic passing through the switch to a monitoring device, such as a network analyzer. This allows the switch to be monitored with the network analyzer in order to identify any malicious or suspicious activity. Additionally, port mirroring can be used to troubleshoot network issues, such as latency or poor performance.

NEW QUESTION: 471

Which of the following 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: ([SHOW ANSWER](#))

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: 472

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

- A. Secure Socket Shell
- B. Site-to-site VPN
- C. In-band connection
- D. Virtual network computing

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 473

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: ([SHOW ANSWER](#))

* The firewall logs are the best source of information to determine whether an internal server was accessed by hosts on the internet, as they record all the traffic that passes through the firewall, including the source and destination IP addresses, ports, protocols, and actions taken by the firewall rules.

* The server's syslog is a file that records events and messages related to the server's operation, such as system errors, warnings, or notifications. It may not contain information about the network traffic to and from the server, especially if the server was shut down during the investigation.

* The NetFlow statistics are a network protocol that collects and analyzes data about the network traffic flows, such as the volume, type, and direction of the traffic. It can provide useful information about the network performance and utilization, but it may not show the details of the individual packets or the firewall actions.

* The audit logs on the core switch are a record of the configuration changes and commands executed on the switch, such as adding, deleting, or modifying VLANs, ports, or routing protocols. They can help troubleshoot or verify the switch's operation, but they may not show the network traffic to and from the server.

References:

- * CompTIA Network+ N10-008 Study Guide, Chapter 7: Network Security, Section 7.2: Network Security Devices and Technologies, p. 372-373
- * Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 5.1: Network Monitoring Tools, p. 51
- * Professor Messer's CompTIA N10-008 Network+ Training Course, Video 5.1: Network Monitoring Tools, 12:28-14:02

NEW QUESTION: 474

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 ([LEAVE A REPLY](#))

A CIDR notation of /26 refers to the number of bits used for the network prefix. In this case, the network prefix is 26 bits long, which leaves 6 bits for the host addresses. In a CIDR notation /26, the first 26 bits of the IP address represent the network and the last 6 bits represent the host addresses.

In this case, the IP address range is 80.87.78.0 - 80.87.78.63 and the network address is 80.87.78.0, so the first usable IP address for devices is 80.87.78.1 and the last usable IP address is 80.87.78.62.

NEW QUESTION: 475

Which of the following OSI model layers will ensure messages are transmitted to their destinations and no data is duplicated?

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

Answer: D ([LEAVE A REPLY](#))

Explanation

The transport layer is the fourth layer of the OSI model, and it is responsible for end-to-end delivery of data over a network. It uses standard protocols such as TCP, UDP, and DCCP to enhance its functionalities. One of the main functions of the transport layer is to ensure that messages are transmitted to their destinations reliably and in the correct order. It also prevents data duplication by using sequence numbers, acknowledgments, and retransmission mechanisms

NEW QUESTION: 476

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

- A. Increased device temperature

- B. Increased CRC errors
- C. Increased switching loops
- D. Increased giants and runts

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 477

A network security engineer is investigating a potentially malicious Insider on the network. The network security engineer would like to view all traffic coming from the user's PC to the switch without interrupting any traffic or having any downtime. Which of the following should the network security engineer do?

- A. Turn on port security.
- B. Implement dynamic ARP inspection.
- C. Configure 802.1Q.
- D. Enable port mirroring.

Answer: D ([LEAVE A REPLY](#))

Port mirroring is a feature that allows a network switch to copy the traffic from one or more ports to another port for monitoring purposes. Port mirroring can be used to analyze the network traffic from a specific source, destination, or protocol without affecting the normal operation of the network. Port mirroring can also help to detect and troubleshoot network problems, such as performance issues, security breaches, or policy violations.

The other options are not correct because they do not meet the requirements of the question. They are:

Turn on port security. Port security is a feature that restricts the number and type of devices that can connect to a switch port. Port security can help to prevent unauthorized access, MAC address spoofing, or MAC flooding attacks. However, port security does not allow the network security engineer to view the traffic from the user's PC to the switch.

Implement dynamic ARP inspection. Dynamic ARP inspection (DAI) is a feature that validates the ARP packets on a network and prevents ARP spoofing attacks. DAI can help to protect the network from man-in-the-middle, denial-of-service, or data interception attacks. However, DAI does not allow the network security engineer to view the traffic from the user's PC to the switch.

Configure 802.1Q. 802.1Q is a standard that defines how to create and manage virtual LANs (VLANs) on a network. VLANs can help to segment the network into logical groups based on function, security, or performance. However, 802.1Q does not allow the network security engineer to view the traffic from the user's PC to the switch.

Reference 1: Port Mirroring - an overview | ScienceDirect Topics 2: Network+ (Plus) Certification | CompTIA IT Certifications 3: Port Security - an overview | ScienceDirect Topics 4: Dynamic ARP Inspection - an overview | ScienceDirect Topics 5: 802.1Q - an overview | ScienceDirect Topics

NEW QUESTION: 478

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

- A. Site-to-site VPNs between the two city locations and client-to-site software on the employee's laptop for all other remote access

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

Answer: A (LEAVE A REPLY)

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

<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html>

NEW QUESTION: 479

Which of the following would be BEST to use to detect a MAC spoofing attack?

- A.** Internet Control Message Protocol
- B.** Reverse Address Resolution Protocol
- C.** Dynamic Host Configuration Protocol
- D.** Internet Message Access Protocol

Answer: B (LEAVE A REPLY)

A MAC spoofing attack consists of changing the MAC address of a network device (network card). A client computer can use Reverse Address Resolution Protocol to request its Internet Protocol (IPv4) address and MAC address from a computer network to check its accuracy.

NEW QUESTION: 480

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

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

Answer: A (LEAVE A REPLY)

An Optical Time Domain Reflectometer (OTDR) is a device that tests the integrity of a fiber cable and is used for the building, certifying, maintaining, and troubleshooting fiber optic systems.

Fusion Splicing is a preferred way to join two fibers together by using heat. Whether the fiber was broken or not long enough, a fusion splicer will make your job easier. You would do this after finding where the break is.

NEW QUESTION: 481

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

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

Answer: A (LEAVE A REPLY)

Traps are unsolicited messages sent by network devices to a network management system (NMS) when an event or a change in status occurs. Traps can help notify the network management team of any issues or problems on the network, such as a link failure or a device reboot. Traps can also trigger actions or alerts on the NMS, such as sending an email or logging the event. MIB stands for Management Information Base and is a database of information that can be accessed and managed by an NMS using SNMP (Simple Network Management Protocol). OID stands for Object Identifier and is a unique name that identifies a specific variable in the MIB. Baselines are measurements of normal network performance and behavior that can be used for comparison and analysis.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 482

An organization has a security staff shortage and must prioritize efforts in areas where the staff will have the most impact. In particular, the focus is to avoid expending resources on identifying non-relevant events. A security analyst is reviewing web server logs and sees the following:

202.180.155.1 - [14/Jan/2021:04:12:28 -0200] "GET /img/us.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:28 -0200] "GET /img/org.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:29 -0200] "GET /img/org2.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:29 -0200] "GET /img/org3.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:30 -0200] "GET /img/org4.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:31 -0200] "GET /img/directors.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:31 -0200] "GET /img/directors2.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:32 -0200] "GET /img/directors3.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:33 -0200] "GET /img/directors4.gif" 404 295

Which of the following should the analyst recommend?

- A. Configuring the web server log to filter out 404 errors on image files
- B. Updating firewall rules to block 202.180.155.1
- C. Resyncing the network time server and monitoring logs for future anomalous behavior
- D. Checking with the penetration testing team to see if the team ran any scans on January 14, 2021

Answer: A (LEAVE A REPLY)

Explanation

This answer will help the organization to avoid expending resources on identifying non-relevant events, as the 404 errors on image files are not indicative of any security threat or issue, but rather a misconfiguration or a broken link on the web server. The 404 errors on image files are also very frequent and repetitive, as shown by the web server log, which can clutter the log and make it harder to spot any relevant events. By filtering out these errors, the analyst can focus on more important events and reduce the noise in the log.

The other answers are not as good as A, because they either do not address the problem of identifying non-relevant events, or they are based on incorrect assumptions or information. For example:

B: Updating firewall rules to block 202.180.155.1 is not a good answer, because the IP address 202.180.155.1 is not doing anything malicious or suspicious, but rather requesting image files that do not exist on the web server. Blocking this IP address will not improve the security of the web server, but rather create unnecessary firewall rules and possibly deny legitimate access to the web server.

C; Resyncing the network time server and monitoring logs for future anomalous behavior is not a good answer, because there is no evidence that the network time server is out of sync or causing any problems. The web server log shows that the entries are all within a few minutes of each other, which is normal and expected. Resyncing the network time server will not help the analyst to identify non-relevant events, but rather waste time and resources on an unrelated task.

D: Checking with the penetration testing team to see if the team ran any scans on January 14, 2021 is not a good answer, because the web server log does not show any signs of a penetration test or a scan. The log shows only 404 errors on image files, which are not typical of a penetration test or a scan, which would usually target different types of files, ports, or vulnerabilities. Checking with the penetration testing team will not help the analyst to identify non-relevant events, but rather distract the analyst from the actual events and possibly create false alarms.

<https://www.professormesser.com/network-plus/n10-008/n10-008-video/general-network-troubleshooting-n10-0>

NEW QUESTION: 483

Which of the following ports is commonly used by VoIP phones?

- A. 20

- B. 143
- C. 445
- D. 5060

Answer: ([SHOW ANSWER](#))

TCP/UDP port 5060 is commonly used by VoIP phones. It is the default port for SIP (Session Initiation Protocol), which is a signaling protocol that establishes, modifies, and terminates multimedia sessions over IP networks. SIP is widely used for VoIP applications such as voice and video calls. References:
<https://www.voip-info.org/session-initiation-protocol/>

NEW QUESTION: 484

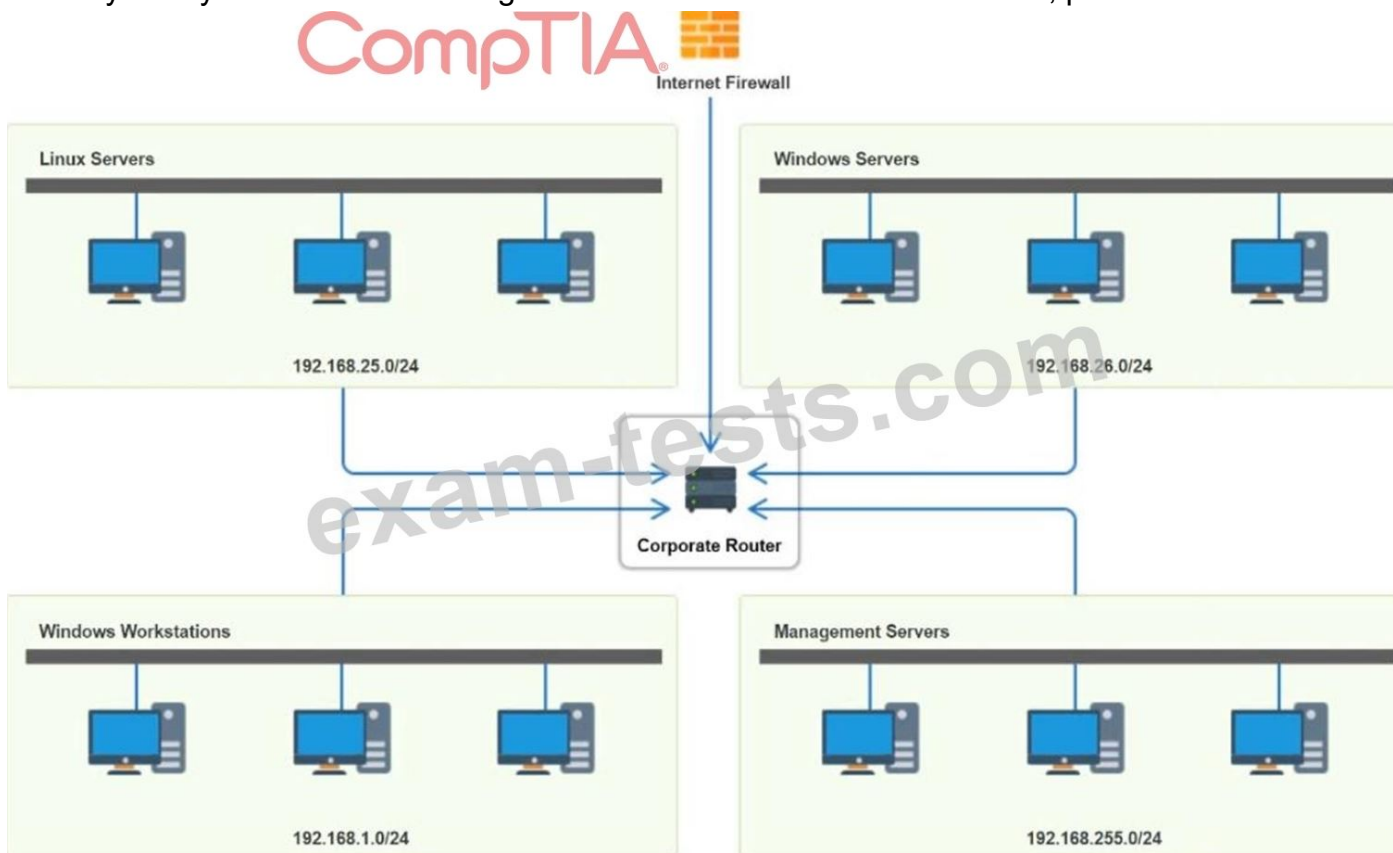
You have been tasked with implementing an ACL on the router that will:

1. Permit the most commonly used secure remote access technologies from the management network to all other local network segments
2. Ensure the user subnet cannot use the most commonly used remote access technologies in the Linux and Windows Server segments.
3. Prohibit any traffic that has not been specifically allowed.

INSTRUCTIONS

Use the drop-downs to complete the ACL

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Router Access Control List



Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
2	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
3	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
7	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	Any	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny

Answer:

See the solution configuration below in Explanation

Explanation:

Router Access Control List					
Rule	Source	Destination	Protocol	Service	Action
1	192.168.255.0	192.168.26.0	TCP	SSH	Allow
2	192.168.255.0	192.168.25.0	TCP	SSH	Allow
3	192.168.255.0	192.168.1.0	TCP	SSH	Allow
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0	Any	TCP	RDP	Deny
7	192.168.1.0	Any	TCP	VNC	Deny
8	192.168.1.0	Any	Any	Any	Allow
9	Any	Any	Any	Any	Deny

NEW QUESTION: 485

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: (SHOW ANSWER)

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.

NEW QUESTION: 486

A technician is troubleshooting a workstation's network connectivity and wants to confirm which switchport corresponds to the wall jack the PC is using Which of the following concepts would BEST help the technician?

- A. Standard work instructions
- B. Inventory management
- C. Change management
- D. Network baseline

E. Consistent labeling

Answer: E ([LEAVE A REPLY](#))

NEW QUESTION: 487

SIMULATION

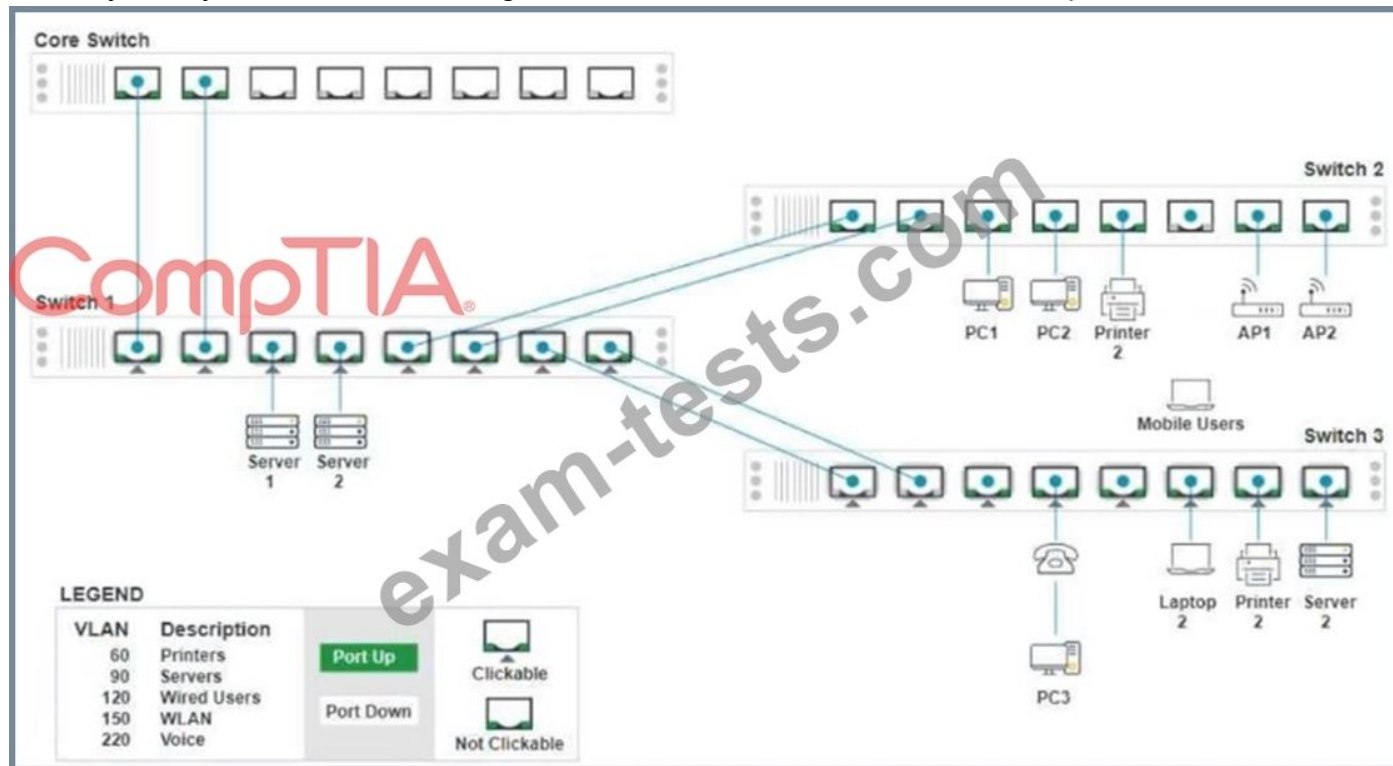
A network technician replaced a switch and needs to reconfigure it to allow the connected devices to connect to the correct networks.

INSTRUCTIONS

Click on the appropriate port(s) on Switch 1 and Switch 3 to verify or reconfigure the correct settings:

- * Ensure each device accesses only its correctly associated network
- * Disable all unused switch ports
- * Require fault-tolerant connections between the switches
- * Only make necessary changes to complete the above requirements

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Switch 3 - Port 8 Configuration

Status

Port ☒ Enabled

LACP ☐ Disabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN1

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1

VLAN 60

VLAN 90

VLAN 120

VLAN 150

VLAN 220

Reset to Default

Save

Close

Switch 3 - Port 7 Configuration

Status

Port ☒ Enabled

LACP ☐ Disabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN1

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1

VLAN 60

VLAN 90

VLAN 120

VLAN 150

VLAN 220

Reset to Default

Save

Close

Switch 3 - Port 6 Configuration

Status

Port ☒ Enabled

LACP ☐ Disabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN150

Port Tagging

Untagged

Tagged

UnTagged

VLAN 1

VLAN 60

VLAN 90

VLAN 120

VLAN 150

VLAN 220

Reset to Default

Save

Close

Switch 3 - Port 4 Configuration

Status

Port

☒ Enabled

LACP

☐ Disabled

Wired

Speed

☐ Auto ☐ 100 ☒ 1000

Duplex

☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN1

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1

VLAN 60

VLAN 90

VLAN 120

VLAN 150

VLAN 220

Reset to Default

Save

Close

Switch 3 - Port 1 Configuration

Status

Port ☒ Enabled

LACP ☐ Disabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN1

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1

VLAN 60

VLAN 90

VLAN 120

VLAN 150

VLAN 220

Reset to Default

Save

Close

Switch 1 - Port 7 Configuration

Status

Port ☒ Enabled

LACP ☒ Enabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN60

Port Tagging

Tagged

VLAN90

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

VLAN220

Port Tagging

Tagged

Reset to Default

Save

Close

Switch 1 - Port 8 Configuration



Status

Port ☒ Enabled

LACP ☒ Enabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN60

Port Tagging

Tagged

VLAN90

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

VLAN220

Port Tagging

Tagged

Reset to Default

Save

Close

Switch 1 - Port 6 Configuration



Status

Port ☒ Enabled

LACP ☒ Enabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN60



Port Tagging

Tagged



VLAN120



Port Tagging

Tagged



VLAN150



Port Tagging

Tagged



Reset to Default

Save

Close

Switch 1 - Port 2 Configuration

Status

Port ☒ Enabled

LACP ☒ Enabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN60 Port Tagging Tagged	VLAN90 Port Tagging Tagged	VLAN120 Port Tagging Tagged
VLAN150 Port Tagging Tagged	VLAN220 Port Tagging Tagged	

Reset to Default Save Close

Switch 1 - Port 1 Configuration

Status

Port ☒ Enabled

LACP ☒ Enabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN60 Port Tagging Tagged	VLAN90 Port Tagging Tagged	VLAN120 Port Tagging Tagged
VLAN150 Port Tagging Tagged	VLAN220 Port Tagging Tagged	

Reset to Default Save Close

Switch 1 - Port 5 Configuration

Status

Port ☒ Enabled

LACP ☒ Enabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN60

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

Reset to Default

Save

Close

Switch 1 - Port 4 Configuration

Status

Port ☒ Enabled

LACP ☐ Disabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN90

Port Tagging

UnTagged

VLAN1

VLAN60

VLAN90

VLAN120

VLAN150

VLAN220

Reset to Default

Save

Close

Switch 1 - Port 3 Configuration

Status

Port ☒ Enabled

LACP ☐ Disabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN90

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220

Reset to Default

Save

Close

Switch 3 - Port 2 Configuration

Status

Port ☒ Enabled

LACP ☐ Disabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN90

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1

VLAN 60

VLAN 90

VLAN 120

VLAN 150

VLAN 220

Reset to Default Save Close

Answer:

See the explanation for this solution.

Explanation

Switch 1 and Switch 2 is the only two switches that can be configured. Only switches linked together with there switch ports needs to be "tagged" and "LACP" needs to be enabled. The other ports must be untagged with no LACP enabled. You only need to assign the correct vlan via each port. 'Speed and Duplex' needs to be Speed=1000 and Duplex=Full, with is by default.

<https://resources.infosecinstitute.com/topic/what-are-tagged-and-untagged-ports/>

NEW QUESTION: 488

A technician discovered that some information on the local database server was changed during a tile transfer to a remote server. Which of the following should concern the technician the MOST?

- A. Confidentiality
- B. Integrity
- C. DDoS
- D. On-path attack

Answer: B (LEAVE A REPLY)

The technician should be most concerned about data integrity and security. If information on the local database server was changed during a file transfer to a remote server, it could indicate that unauthorized access or modifications were made to the data. It could also indicate a failure in the file transfer process, which could result in data loss or corruption. The technician should investigate the cause of the changes and take steps to prevent it from happening again in the future. Additionally, they should verify the integrity of the data and restore it from a backup if necessary to ensure that the correct and complete data is available. The technician should also take appropriate actions such as notifying the system administrator and management of the incident, and following the incident management process to minimize the damage caused by the incident.

NEW QUESTION: 489

A network technician wants to deploy a new wireless access point to reduce user latency. Currently, the organization has the following deployed:

Device	Channel
Patio 1	1
Patio 2	6

Which of the following channels should the new device broadcast on?

- A. Channel 3
- B. Channel 9
- C. Channel 10
- D. Channel 11

Answer: D (LEAVE A REPLY)

Explanation

The best channel for a new wireless access point is one that does not overlap with the existing channels used by other devices. Overlapping channels can cause interference and degrade the performance of the wireless network. According to the web search results, the 2.4 GHz band has 11 channels in the U.S., but only channels 1, 6, and 11 are non-overlapping. Since the existing devices are using channels 1 and 6, the new device should use channel 11 to avoid adjacent-channel interference

References1: Why Channels 1, 6 and 11? | MetaGeek
2: How to Choose the Best Wi-Fi Channels for Your Network - Lifewire

NEW QUESTION: 490

A network administrator wants to improve the security of the management console on the company's switches and ensure configuration changes made can be correlated to the administrator who conformed them Which of the following should the network administrator implement?

- A. TACACS+
- B. Port security
- C. Local authentication

D. Access control list

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 491

A technician is setting up DNS records on local servers for the company's cloud DNS to enable access by hostname. Which of the following records should be used?

A. A

B. MX

C. CNAME

D. NS

Answer: A ([LEAVE A REPLY](#))

An A record, also known as an address record, is a type of DNS record that maps a hostname to an IPv4 address. An A record is used to resolve a domain name to an IP address, so that clients can connect to the server or service by using the domain name instead of the IP address. For example, an A record can map `www.example.com` to `192.0.2.1`.

An A record is the most common type of DNS record for cloud DNS, as it allows the company to use a custom domain name for their cloud services, such as web hosting, email, or storage. An A record can also be used to create subdomains, such as `blog.example.com` or `mail.example.com`, that point to different IP addresses or servers.

The other options are not correct because they are not the best type of DNS record for cloud DNS. They are:

* MX. MX stands for mail exchange, and it is a type of DNS record that specifies the mail servers that are responsible for receiving and delivering email messages for a domain name. MX records are used for email services, but they are not sufficient for cloud DNS, as they do not map a hostname to an IP address.

* CNAME. CNAME stands for canonical name, and it is a type of DNS record that specifies an alias name for another domain name. CNAME records are used to create multiple names for the same IP address or server, such as `www.example.com` and `example.com`. CNAME records are useful for cloud DNS, but they are not the best type, as they depend on another A record to resolve the IP address.

* NS. NS stands for name server, and it is a type of DNS record that delegates a DNS zone to an authoritative server. NS records are used to specify which DNS servers are responsible for answering queries for a domain name or a subdomain. NS records are essential for cloud DNS, but they are not the best type, as they do not map a hostname to an IP address.

References1: DNS records overview | Google Cloud2: Network+ (Plus) Certification | CompTIA IT Certifications3: CloudDNS: What is a DNS record?

NEW QUESTION: 492

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

A. F-type connector

B. TIA/EIA-568-B

C. LC

D. SC

Answer: B (LEAVE A REPLY)

The termination that the technician should use when running a cable from the ISP's port to the front desk is B. TIA/EIA-568-B. This is a standard pin-out for Cat 6 cables that is used for Ethernet and other network physical layers¹.

It specifies how to arrange the eight wires in an RJ45 connector, which is a common type of connector for network cables.

NEW QUESTION: 493

Which of the following is most closely associated with attempting to actively prevent network intrusion?

A. VPN

B. Firewall

C. IPS

D. IDS

Answer: C (LEAVE A REPLY)

NEW QUESTION: 494

A network technician must connect a newly installed access switch in a warehouse to the distribution switch in the telecommunications closet. The distance between the two switches is 1,640ft (500m). Which of the following is the best cable choice?

A. Fiber

B. Cat 5e

C. Cat 6a

D. Coaxial

Answer: A (LEAVE A REPLY)

Fiber is the best cable choice for long distances, as it can transmit data over 1,640ft (500m) without significant signal loss or interference. Fiber is also immune to electromagnetic interference and can support higher bandwidths than copper cables. Cat 5e and Cat 6a are copper cables that have a maximum distance of 328ft (100m) for Ethernet networks. Coaxial cable is also a copper cable that can reach longer distances, but it is mainly used for cable TV and not for Ethernet networks.

NEW QUESTION: 495

A help desk technician discovers the following note while reviewing tickets in a customer's account:

Was able to confirm customer's problem with the system. Will upgrade system to latest version and monitor for further connectivity problems per developer's instructions.

Which of the following describes what the technician was documenting with this note?

A. The technician was approaching multiple problems individually.

B. The technician was establishing a plan of action and identifying potential effects.

C. The technician was testing a theory to determine the cause.

D. The technician was identifying the problem by gathering information.

Answer: D (LEAVE A REPLY)

Explanation

The technician was identifying the problem by gathering information with this note. This is the first step of the troubleshooting methodology, which is a systematic process of finding and resolving issues in a network or system. By gathering information, the technician can understand the symptoms, scope, and impact of the problem, as well as collect relevant data from various sources, such as users, logs, tools, or documentation. The note shows that the technician was asking questions to the user, checking the network status and configuration, and reviewing previous tickets to gather information about the problem. References: [CompTIA Network+ Certification Exam Objectives], Troubleshooting Methodology - CompTIA Network+ N10-007 - 1.4 | Professor Messer IT Certification Training Courses

NEW QUESTION: 496

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

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

Answer: D (LEAVE A REPLY)

- * The netstat -n command displays active TCP connections, but addresses and port numbers are expressed numerically and no attempt is made to determine names¹². This option can be useful for checking the output in integer form, as well as for avoiding possible delays caused by name resolution¹².
- * The netstat command without any parameters displays active TCP connections, but addresses and port numbers are resolved to their corresponding names, such as hostnames and service names¹². This option can be less informative and more time-consuming than the -n option¹².
- * The netstat -a command displays all active TCP connections and the TCP and UDP ports on which the computer is listening¹². This option can be useful for checking the availability and status of ports, but it does not show the output in integer form¹².
- * The netstat -e command displays Ethernet statistics, such as the number of bytes and packets sent and received¹². This option can be useful for checking the network performance and utilization, but it does not show the network connections or their addresses and port numbers¹².

References:

- * 1: CompTIA Network+ N10-008 Study Guide, Chapter 5: Network Tools and Troubleshooting
- * 2: netstat | Microsoft Learn
- * : 28 Netstat Commands {A Comprehensive List With Examples} - phoenixNAP
- * : How to Use the Netstat Command - Lifewire

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com

N10-008 dumps with Test Engine here: <https://www.braindumps.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 497

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

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

Answer: (SHOW ANSWER)

EIGRP is an advanced distance vector routing protocol that is able to automatically update routing tables and also uses features of link-state routing protocols, such as the ability to send updates about the current topology of the network. EIGRP also has the ability to use a variety of algorithms to determine the best route for a packet to take, allowing for more efficient routing across the network.

NEW QUESTION: 498

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

Switch 1:					
	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	60	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Active	Active	Active	Active
Switch 2:					
	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	60	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Active	Shut down	Active	Active
Switch 3:					
	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	80	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Shut down	Shut down	Shut down	Active

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

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

E. Reconfigure the VLAN on the printer ports on Switch 3.

F. Enable wireless APs on Switch 3.

Answer: A,E ([LEAVE A REPLY](#))

The issue is that new employees are not able to print to the main networked copiers from their workstations after Switch 3 was added to the stack. Looking at the port configurations for Switch 3, we can see that the ports for printers (Ports 13-24) are shut down.

A . Enable the printer ports on Switch 3: This should be done because, as per the configuration shown in the image, these ports are currently shut down. Enabling them would restore connectivity for printing.

E . Reconfigure the VLAN on the printer ports on Switch 3: The VLAN for printers is set to 80 on Switch 3 while it is set to 60 on Switches 1 and 2. Changing VLAN of printer ports on Switch 3 to match with other switches (VLAN60) will ensure that they are all in the same broadcast domain and can communicate effectively.

The duplex settings do not need reconfiguration as they are already set to full duplex across all switches which facilitates efficient two-way communication.

Reference:

CompTIA Network+ N10-008 Certification Study Guide, Chapter 3: Network Devices, page 115-116 CompTIA Network+ Certification Exam Objectives, Domain 2: Network Implementations, Objective 2.1: Given a scenario, install and configure the appropriate networking devices, Sub-objective: Configure switch ports Ace Your CompTIA Network+ Exam: Explore Top Study Resources, Section: CompTIA Network+ Certification Kit: Exam N10-008 6th Edition

NEW QUESTION: 499

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. RADIUS

B. VPN

C. Single sign-on

D. Multifactor authentication

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 500

Users are connected to a switch on an Ethernet interface of a campus router. The service provider is connected to the serial 1 interface on the router. The output of the interfaces is:

E1/0: 192.168.8.1/24

S1: 192.168.7.252/30

After router and device configurations are applied, internet access is not possible. Which of the following is the most likely cause?

A. The Ethernet interface was configured with an incorrect IP address.

B. The router was configured with an incorrect loopback address.

C. The router was configured with an incorrect default gateway.

D. The serial interface was configured with the incorrect subnet mask.

Answer: ([SHOW ANSWER](#))

An incorrect subnet mask on the serial interface would prevent proper communication between the router and the service provider, affecting internet access. The other options are less likely to be the cause: an incorrect Ethernet IP address would affect local network connectivity, an incorrect loopback address does not impact external network access, and an incorrect default gateway is not relevant for serial link configurations.

NEW QUESTION: 501

Which of the following layers is where TCP/IP port numbers identify which network application is receiving the packet and where it is applied?

- A. 3**
- B. 4**
- C. 5**
- D. 6**
- E. 7**

Answer: B (LEAVE A REPLY)

Layer 4 is where TCP/IP port numbers identify which network application is receiving the packet and where it is applied. Layer 4 is also known as the transport layer in the TCP/IP model or the OSI model. The transport layer is responsible for providing reliable or unreliable end-to-end data transmission between hosts on a network. The transport layer uses port numbers to identify and multiplex different applications or processes that communicate over the network. Port numbers are 16-bit numbers that range from 0 to 65535 and are divided into three categories: well-known ports (0-1023), registered ports (1024-49151), and dynamic ports (49152-65535). Some examples of well-known port numbers are 80 for HTTP, 443 for HTTPS, and 25 for SMTP. Reference: [CompTIA Network+ Certification Exam Objectives], Transport Layer - an overview | ScienceDirect Topics

NEW QUESTION: 502

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 (LEAVE A REPLY)

* A redundant cluster of devices is a group of devices that can provide backup or failover functionality in case of a hardware failure or a network attack.

* Layer 2 devices operate at the data link layer of the OSI model and are responsible for forwarding frames based on MAC addresses. They include switches, bridges, and NICs.

* Multiple routers are not Layer 2 devices, but Layer 3 devices that operate at the network layer of the OSI model and are responsible for forwarding packets based on IP addresses. Therefore, option A is incorrect.

* Multiple switches are Layer 2 devices that can provide redundancy and scalability in the network by using protocols such as spanning tree, link aggregation, and VLANs. They can also support Layer 3 functions such as routing and inter-VLAN routing. Therefore, option B is the correct answer.

* Multiple firewalls are not Layer 2 devices, but Layer 4 devices that operate at the transport layer of the OSI model and are responsible for filtering traffic based on ports and protocols. They can also provide security services such as NAT, VPN, and IDS. Therefore, option C is incorrect.

* Multiple budges is a typo and should be multiple bridges. Bridges are Layer 2 devices that can divide a network into segments and reduce collisions. However, they are less efficient and less intelligent than switches, and they are rarely used in modern networks. Therefore, option D is incorrect.

References:

* CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Devices, pages 47-48, 51-52, 55-56, 59-60.

* Professor Messer's Network+ Video Course, Section 1.1: Network Devices, videos 1.1.1 - 1.1.4, 1.1.6, 1.1.7.

* Cisco Press: Fully Redundant Layer 2 and Layer 3 Designs

NEW QUESTION: 503

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 504

A network technician is troubleshooting an issue that involves connecting to a server via SSH. The server has one network interface that does not support subinterfaces. The technician runs a command on the server and receives the following output:

Proto	Local address	Foreign address	State
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING
TCP	10.10.10.15:22	10.10.10.42:21231	ESTABLISHED

On the host, the technician runs another command and receives the following:

Destination	Gateway	Genmask	Flags	Iface
default	31.242.12.9	0.0.0.0	UG	eth0
192.168.1.0	0.0.0.0	255.255.255.0	UG	eth1

Which of the following best explains the issue?

- A. The server is plugged into a trunk port.
- B. The host does not have a route to the server.
- C. The server is not running the SSH daemon.
- D. A firewall is blocking access to the server.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 505

You are tasked with verifying the following requirements are met in order to ensure network security.

Requirements:

Datacenter

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic Building A

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide devices to support 5 additional different office users Add an additional mobile user Replace the Telnet

server with a more secure solution Screened subnet Ensure network is subnetted to allow all devices to

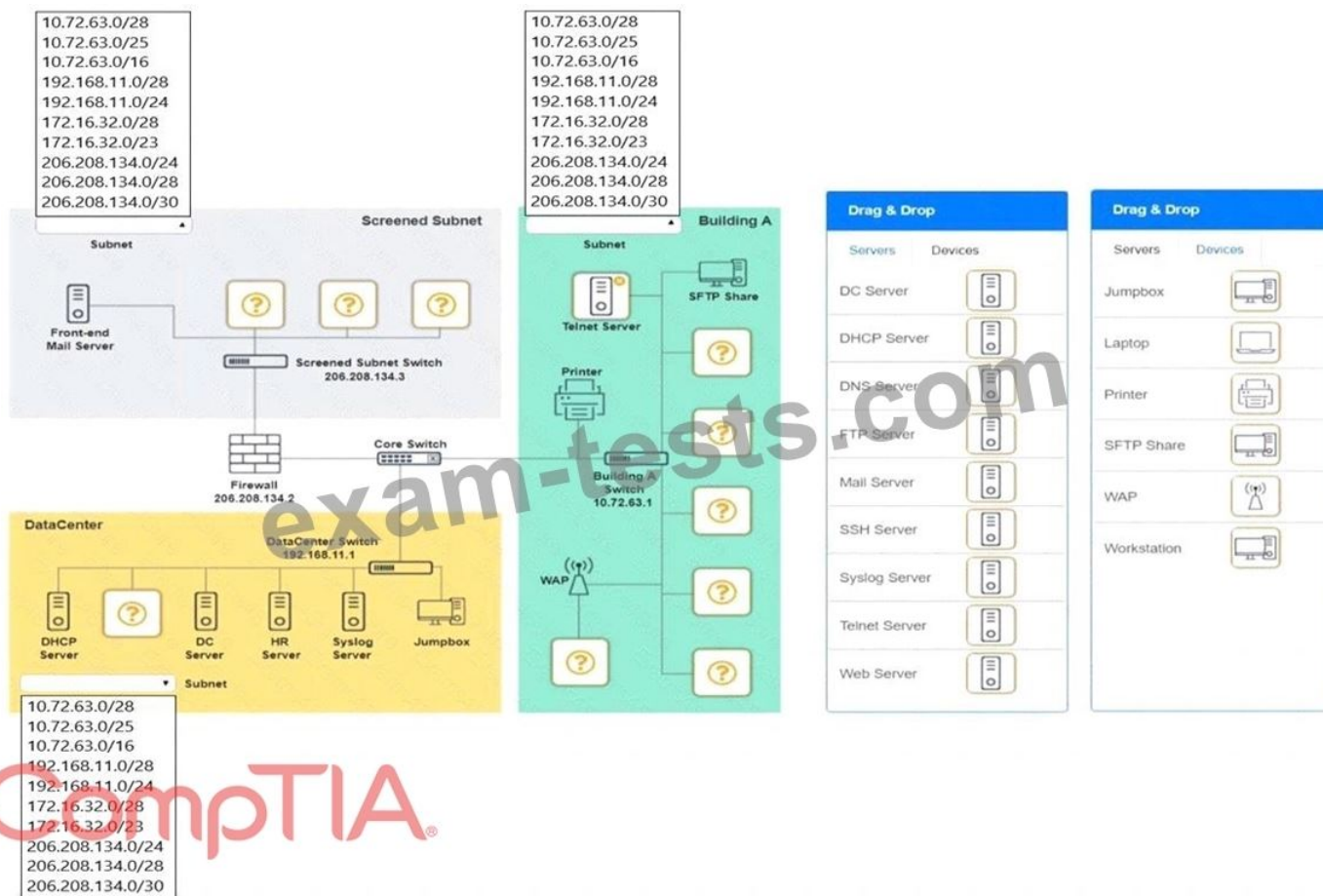
communicate properly while minimizing address space usage Provide a server to handle external 80/443 traffic

Provide a server to handle port 20/21 traffic INSTRUCTIONS Drag and drop objects onto the appropriate

locations. Objects can be used multiple times and not all placeholders need to be filled.

Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:

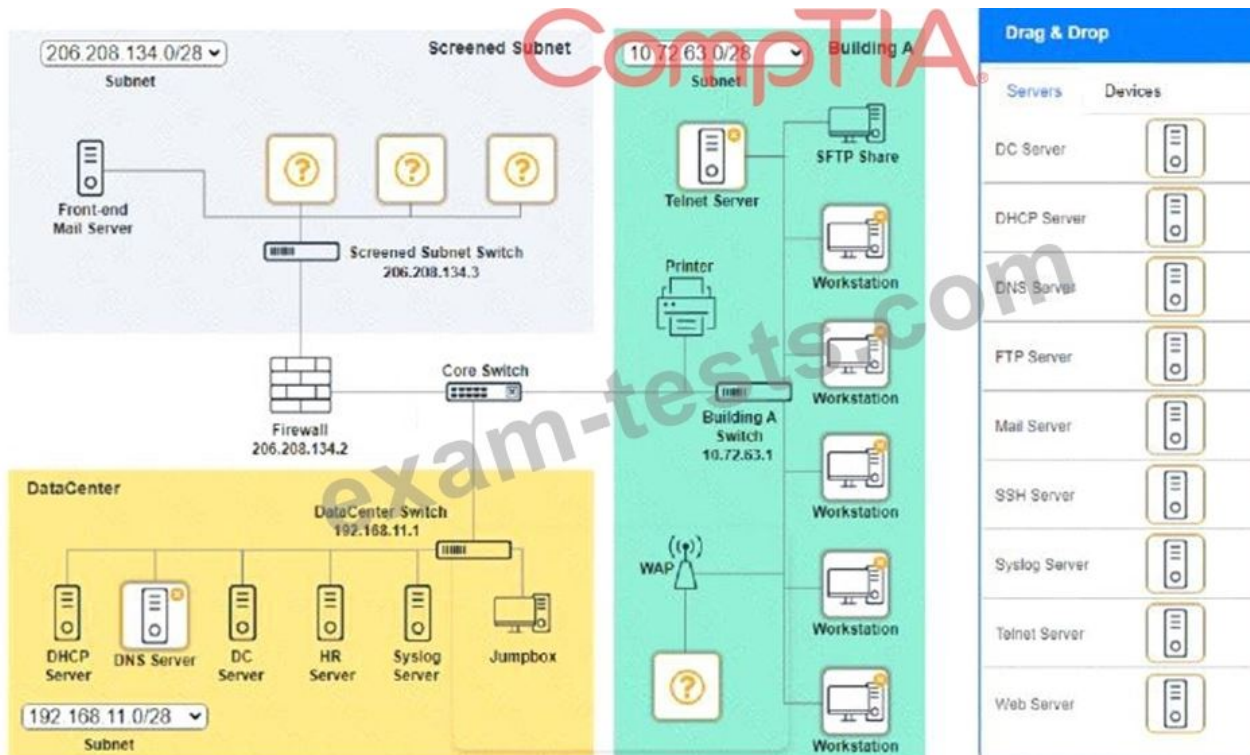
See explanation below.

Explanation

Screened Subnet devices - Web server, FTP server

Building A devices - SSH server top left, workstations on all 5 on the right, laptop on bottom left DataCenter

devices - DNS server.



NEW QUESTION: 506

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:

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

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

Answer: D (LEAVE A REPLY)

NEW QUESTION: 507

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

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

Answer: (SHOW ANSWER)

Explanation

An extended service set (ESS) is a wireless network that consists of multiple access points (APs) that share the same SSID and are connected by a wired network. An ESS allows wireless clients to roam seamlessly between

different APs without losing connectivity. A basic service set (BSS) is a wireless network that consists of a single AP and its associated clients. An independent basic service set (IBSS) is a wireless network that consists of a group of clients that communicate directly without an AP. A unified service set is not a standard term for a wireless network. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

[https://en.wikipedia.org/wiki/Service_set_\(802.11_network\)](https://en.wikipedia.org/wiki/Service_set_(802.11_network))

NEW QUESTION: 508

A network administrator is troubleshooting a client's device that cannot connect to the network. A physical inspection of the switch shows the RJ45 is connected. The NIC shows no activity lights. The network administrator moves the device to another location and connects to the network without issues. Which Of the following tools would be the BEST option for the network administrator to use to further troubleshoot?

- A. Tone generator
- B. Multimeter
- C. Optical time-domain reflectometer
- D. Cable tester

Answer: D (LEAVE A REPLY)

Explanation

A cable tester is a tool that can verify the integrity and functionality of a network cable. It can measure the electrical characteristics of the cable, such as resistance, capacitance, and impedance, and detect any faults or defects, such as shorts, opens, or crosstalk. A cable tester can help the network administrator troubleshoot the problem by determining if the cable is faulty or not. A tone generator is a tool that can send an audible signal through a cable to help locate and identify it. A multimeter is a tool that can measure voltage, current, and resistance of electrical circuits. An optical time-domain reflectometer (OTDR) is a tool that can test the quality and length of fiber optic cables.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.3: Given a scenario, use the appropriate tool to support wired or wireless networks.

NEW QUESTION: 509

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

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

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

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

Answer: D (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 510

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

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

Answer: A ([LEAVE A REPLY](#))

A north-south traffic flow is a term used to describe the communication between a user or device outside the network and a server or service inside the network. For example, a public internet user accessing a published web server is a north-south traffic flow. This type of traffic flow typically crosses the network perimeter and requires security measures such as firewalls and VPNs. References: CompTIA Network+ N10-008 Certification Study Guide, page 16; The Official CompTIA Network+ Student Guide (Exam N10-008), page 1-9.

North-south traffic flow refers to the flow of traffic between the internal network of an organization and the external world. This type of traffic typically flows from the internet to the organization's internal network, and back again.

Examples of north-south traffic flow include:

- * A public internet user accessing a published web server
- * A remote employee connecting to a VPN
- * An email client sending email to an external server
- * A customer connecting to an e-commerce website

References:

- * CompTIA Network+ N10-008 Exam Objectives, Version 5.0, August 2022, page 12
- * CompTIA Network+ Certification Study Guide, Seventh Edition, Todd Lammle, Sybex, 2022, page 17

NEW QUESTION: 511

A network administrator determines that even when optimal wireless coverage is configured, the network users still report constant disconnections. After troubleshooting, the administrator determines that moving from one location to another causes the disconnection. Which of the following settings should provide better network stability?

- A.** Client association timeout
- B.** RSSI roaming threshold
- C.** RF attenuation ratio
- D.** EIRP power setting

Answer: ([SHOW ANSWER](#))

Explanation

In this case, the most likely cause of the constant disconnections when moving from one location to another is likely due to a problem with the roaming functionality of the wireless network. The setting that would likely provide better network stability in this situation is the RSSI roaming threshold, which determines the signal strength required for a client device to remain connected to the wireless network. If the roaming threshold is set too low, the client device may disconnect and reconnect to the network too frequently as it moves between different access points. On the other hand, if the threshold is set too high, the client device may not roam to a new access point when necessary, leading to a loss of connectivity. Adjusting the RSSI roaming threshold to an appropriate value may help to improve the stability of the wireless network in this situation.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 512

A Fortune 500 company would like to move its on-premises corporate email systems to a multitenant product hosted in the cloud where no maintenance of the underlying server OS or platform is required. Which of the following BEST represents the model the company should choose?

- A. Private
- B. Community
- C. Hybrid
- D. Public

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 513

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

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

Answer: B,C ([LEAVE A REPLY](#))

Two-factor authentication (2FA) is a method of verifying a user's identity by requiring two pieces of evidence, such as something the user knows (e.g., a password) and something the user has (e.g., a token or a smartphone). 2FA adds an extra layer of security that makes it harder for hackers to access a user's account by

brute-force programs. Complex passwords are passwords that are long, random, and use a combination of uppercase and lowercase letters, numbers, and symbols. Complex passwords are more resistant to brute-force attacks than simple or common passwords. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

<https://www.csoononline.com/article/3225913/what-is-two-factor-authentication-2fa-how-to-enable-it-and-why-yo>

<https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/>

NEW QUESTION: 514

A MAC address is a part of which of the following OSI model layers?

- A. Transport
- B. Physical
- C. Network
- D. Data Link

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 515

Which of the following can be used to decrease latency during periods of high utilization of a firewall?

- A. Hot site
- B. NIC teaming
- C. HA pair
- D. VRRP

Answer: B ([LEAVE A REPLY](#))

NIC Teaming, also known as load balancing and failover (LBFO), allows multiple network adapters on a computer to be placed into a team for the following purposes: Bandwidth aggregation. Traffic failover to prevent connectivity loss in the event of a network component failure.

NEW QUESTION: 516

Two companies want to build an encrypted tunnel between them and use a PSK for initial authentication.

Which of the following is the BEST protocol for the companies to use?

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

Answer: ([SHOW ANSWER](#)**)**

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

NEW QUESTION: 517

A network technician is troubleshooting a port channel issue. When logging in to one of the switches, the technician sees the following information displayed:

Native VLAN mismatch detected on interface g0/1

Which of the following layers of the OSI model is most likely to be where the issue resides?

- A. Layer 5
- B. Layer 2
- C. Layer 3
- D. Layer 6

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 518

A network administrator installed an additional IDF during a building expansion project. Which of the following documents need to be updated to reflect the change? (Select TWO).

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

Answer: D,F ([LEAVE A REPLY](#))

NEW QUESTION: 519

A technician is setting up DNS records on local servers for the company's cloud DNS to enable access by hostname. Which of the following records should be used?

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

Answer: C ([LEAVE A REPLY](#))

A CNAME record is a type of DNS record that maps a hostname to another hostname. This is useful when you want to use a different hostname for a server than its actual IP address.

In this case, the technician is setting up DNS records on local servers for the company's cloud DNS to enable access by hostname. This means that the users will be able to access the servers by their hostnames, instead of their IP addresses.

To do this, the technician needs to create a CNAME record for each server. The CNAME record will point the hostname to the server's IP address.

NEW QUESTION: 520

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

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 521

The results of a recently completed site survey indicate a significant, undesired RSSI in the parking lot and other exterior areas near the like to mitigate access to the wireless network in exterior access areas. The current access point settings are listed in the following table:

Which of the following is the BEST step for the technician to take to resolve the issue?

- A. Reconfigure AP2 and AP3 for non-overlapping channels
- B. Implement directional antennas on AP1 and AP2.
- C. Raise the power settings on AP2 and AP3.
- D. Change the SSID on AP1 and AP2.

Answer: B (LEAVE A REPLY)

Explanation

Implementing directional antennas on AP1 and AP2 is the best step for the technician to take to resolve the issue of undesired RSSI in the parking lot and other exterior areas near the building. RSSI stands for received signal strength indicator, which is a measure of how well a device can receive a wireless signal from an access point (AP). An AP is a device that provides wireless connectivity to a network. An antenna is a device that radiates or receives electromagnetic waves. A directional antenna is an antenna that focuses the wireless signal in a specific direction, resulting in higher gain and longer range. By using directional antennas on AP1 and AP2, which are located near the exterior walls of the building, the technician can reduce the wireless signal leakage to the outside areas and improve the wireless coverage inside the building. References: [CompTIA Network+ Certification Exam Objectives], What Is RSSI and How Does It Affect Wireless Networks?, Directional Antennas: Everything You Need to Know

NEW QUESTION: 522

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

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

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 523

When accessing corporate network resources, users are required to authenticate to each application they try to access. Which of the following concepts does this BEST represent?

- A. SSO
- B. Zero Trust
- C. VPN
- D. Role-based access control

Answer: (SHOW ANSWER)

- * The concept of Zero Trust is based on the principle of never trust, always verify. It means that every request for accessing network resources, regardless of where it originates from, must be authenticated and authorized before granting access¹².
- * Zero Trust is different from SSO (single sign-on), which allows users to log in once and access multiple applications without re-authenticating³. SSO simplifies the user experience, but does not provide the same level of security as Zero Trust.
- * Zero Trust is also different from VPN (virtual private network), which creates a secure tunnel between a remote device and a network, encrypting the traffic and hiding the device's IP address⁴. VPN provides privacy and protection from external threats, but does not verify the identity and permissions of the device or user accessing the network.
- * Zero Trust is also different from role-based access control (RBAC), which assigns permissions to users or groups based on their roles and responsibilities⁵. RBAC helps to enforce the principle of least privilege, but does not verify the context and conditions of each access request.
- * Therefore, the best answer is B. Zero Trust, which requires authentication and authorization for each application access, regardless of the source or location of the request.

References:

- * 1: What is Zero Trust? A model for more effective security | CSO Online
- * 2: CompTIA Network+ N10-008 Certification Study Guide, page 472
- * 3: [What is Single Sign-On (SSO)? - Definition from WhatIs.com]
- * 4: [What is a VPN? | Virtual Private Networks Explained | Norton]
- * 5: [What is Role-Based Access Control (RBAC)? - Definition from Techopedia]

NEW QUESTION: 524

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

- A. Client-to-site VPN
- B. Third-party VPN service

- C. Site-to-site VPN
- D. Split-tunnel VPN

Answer: ([SHOW ANSWER](#))

A site-to-site VPN is a type of VPN that connects two or more remote offices securely over an untrustworthy network, such as the Internet. A site-to-site VPN allows each office to access network shares and resources at the other site, as if they were on the same local network. A site-to-site VPN encrypts and tunnels the traffic between the offices, ensuring privacy and integrity of the data. Reference: <https://www.comptia.org/blog/what-is-a-site-to-site-vpn>

NEW QUESTION: 525

A client utilizes mobile tablets to view high-resolution images and videos via Wi-Fi within a corporate office building. The previous administrator installed multiple high-density APs with Wi-Fi 5, providing maximum coverage, but the measured performance is still below expected levels. Which of the following would provide the best solution?

- A. Channel bonding
- B. EIRP power settings
- C. Antenna polarization
- D. A directional antenna

Answer: ([SHOW ANSWER](#))

Channel bonding is a technique that allows two or more adjacent channels to be combined into a wider channel, increasing the data rate and throughput of the wireless network. Channel bonding can improve the performance of the Wi-Fi network by utilizing more of the available spectrum and reducing interference from other devices. Channel bonding is supported by Wi-Fi 5 (802.11ac) and Wi-Fi 6 (802.11ax) standards.

References: CompTIA Network+ N10-008 Cert Guide, Chapter 4, Section 4.2

NEW QUESTION: 526

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, the administrator sees the 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 4
- B. Rule 1
- C. Rule 2
- D. Rule 3

Answer: ([SHOW ANSWER](#))

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 527

Users in a remote office report that corporate web server pages are taking a long time to load, whereas users in the main corporate office do not have any issues. Which of the following is the best metric for a network administrator to check?

- A.** Jitter across the network
- B.** Hop-by-hop network latency
- C.** Server interface CRC errors
- D.** Server NetFlow data

Answer: B (LEAVE A REPLY)

The best metric for a network administrator to check is hop-by-hop network latency. This is because network latency is the time it takes for a packet to travel from the source to the destination, and it affects the loading speed of web pages. Hop-by-hop network latency measures the latency between each pair of routers or switches along the network path, and it can help identify where the delay is occurring. By checking the hop-by-hop network latency, the network administrator can determine if the problem is caused by a slow or congested link, a misconfigured or faulty device, or a routing issue.

Jitter is the variation in latency over time, and it affects the quality of voice and video applications. Jitter does not directly affect the loading speed of web pages, and it is not a useful metric for troubleshooting this issue.

Server interface CRC errors are errors that occur when the cyclic redundancy check (CRC) of a packet does not match the expected value, indicating data corruption. Server interface CRC errors can affect the reliability and integrity of data transmission, and they can be caused by faulty cables, connectors, or interfaces. Server interface CRC errors do not necessarily affect the loading speed of web pages, unless they are severe enough to cause retransmissions or packet loss.

Server NetFlow data is data that is collected and analyzed by the NetFlow protocol, which monitors and reports on network traffic flows. Server NetFlow data can provide information on the volume, type, and direction of traffic that is sent or received by the server, as well as the source and destination IP addresses, ports, and protocols. Server NetFlow data can help identify network usage patterns, trends, and anomalies, but it does not measure the latency or performance of the network.

Reference What is Network Latency and How to Measure It How to Troubleshoot Network Latency Issues What is Jitter and How to Measure It What is CRC Error and How to Fix It What is NetFlow and How Does It Work CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION: 528

After a recent power outage, users are reporting performance issues accessing the application servers. Wireless users are also reporting intermittent Internet issues.

INSTRUCTIONS

Click on each tab at the top of the screen. Select a widget to view information, then use the drop-down menus to answer the associated questions. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Health

Device Monitoring

Show Question

Reset All Answers

Wireless Client Distribution

Wireless Users Connected - 24 Hours

Ram Usage

Processor Usage

WAN Health

Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	Jitter
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9.5ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3.9ms

Which WAN station should be preferred for VoIP traffic?

WAN 1

Select WAN

WAN 1

WAN 2

Network Health

Device Monitoring

Device Status

Alert (3)

Up (8)

Warning (2)

Down (1)

Top Hosts

	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb
3	10.1.90.55	12.41 Mp	7	74.68 Gb
4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

Which device is experiencing connectivity issues?

Select Answer

Router A

Router B

WAP1

WAP2

WirelessController

Switch A

Switch B

DHCP Server

Web Server

APP Server

Router A

Which workstation IP is generating the MOST traffic?

Select Answer

10.1.99.28

10.1.99.14

10.1.99.10

10.1.99.22

10.1.99.24

206.208.133.10

206.208.133.9

10.1.50.14

10.1.50.13

10.1.59.81

10.1.90.53

10.1.90.55

206.208.133.9

Answer:

See the answer and solution below

Explanation:

Network Health:

WAN 2 appears to have a lower average latency and loss percentage, which would make it the preferred WAN station for VoIP traffic. VoIP traffic requires low latency and packet loss to ensure good voice quality and

reliability. WAN 1 seems to have higher RAM and processor usage, which could also affect the performance of VoIP traffic.

Here's the summary of the key metrics for WAN 1 and WAN 2 from the image provided:

WAN 1:

Uplink Speed: 10G

Total Usage: 26.969GB Up / 1.748GB Down

Average Throughput: 353MBps Up / 23.42MBps Down

Loss: 2.51%

Average Latency: 24ms

Jitter: 9.5ms

WAN 2:

Uplink Speed: 1G

Total Usage: 930GB Up / 138GB Down

Average Throughput: 12.21MBps Up / 1.82MBps Down

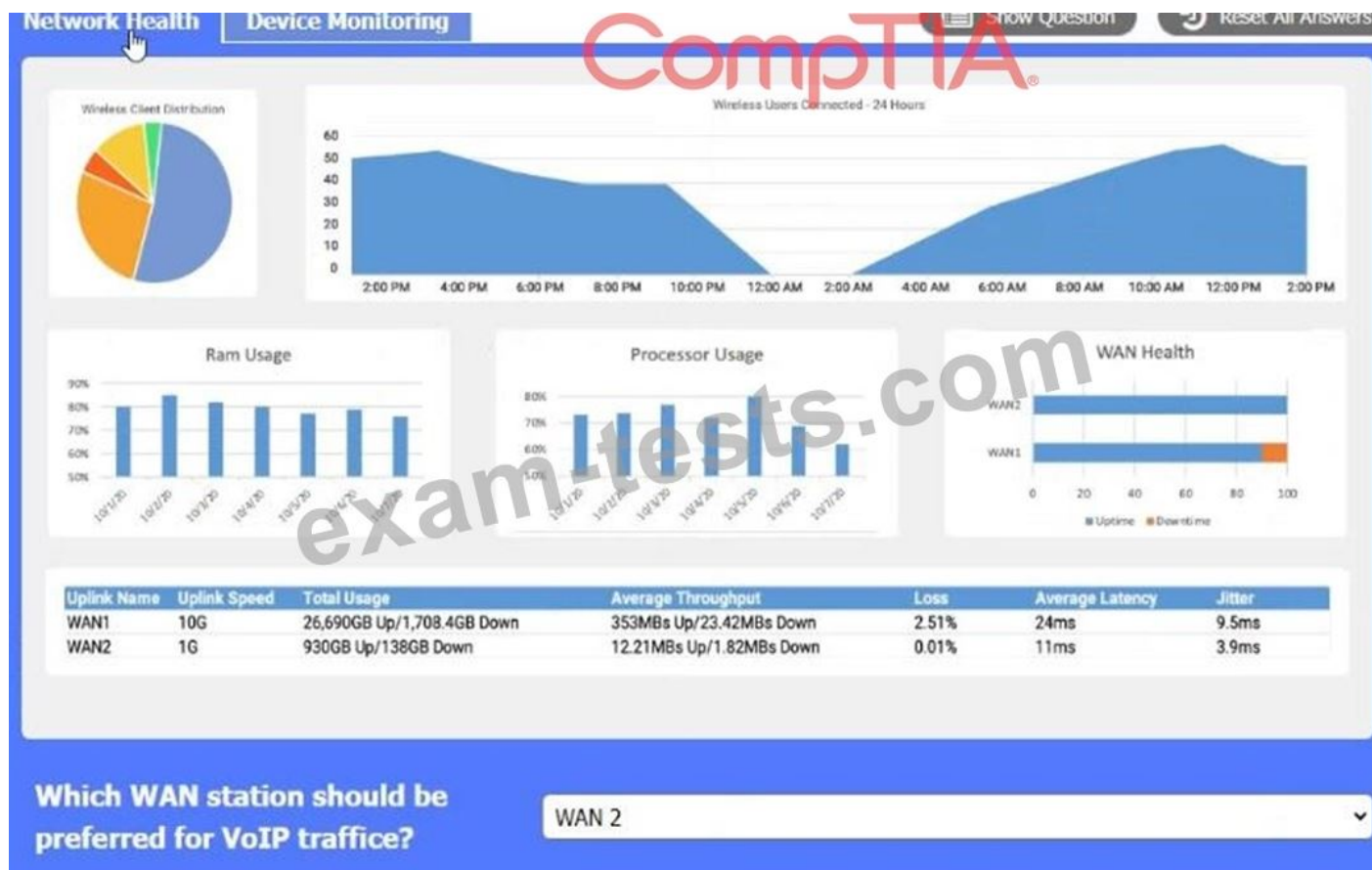
Loss: 0.01%

Average Latency: 11ms

Jitter: 3.9ms

For VoIP traffic, low latency and jitter are particularly important to ensure voice quality. While WAN 1 has higher bandwidth and throughput, it also has higher latency and jitter compared to WAN 2. However, WAN 2 has much lower loss, lower latency, and lower jitter, which are more favorable for VoIP traffic that is sensitive to delays and variation in packet arrival times.

Given this information, WAN 2 would generally be preferred for VoIP traffic due to its lower latency, lower jitter, and significantly lower loss percentage, despite its lower bandwidth compared to WAN 1. The high bandwidth of WAN 1 may be more suitable for other types of traffic that are less sensitive to latency and jitter, such as bulk data transfers.



Device Monitoring:

the device that is experiencing connectivity issues is the APP Server or Router 1, which has a status of Down. This means that the server is not responding to network requests or sending any data. You may want to check the physical connection, power supply, and configuration of the APP Server to troubleshoot the problem.



NEW QUESTION: 529

A company is designing a new complex. The primary and alternate data centers will be in separate buildings 6.2mi (10km) apart and will be connected via fiber. Which of the following types of SFP is the best choice?

- A. 10GBASE-SR
- B. 10000BASE-LX
- C. 10GBASE-LR
- D. 1000BASE-SX

Answer: C ([LEAVE A REPLY](#))

10GBASE-LR SFP transceivers are designed for long-range transmissions over single-mode fiber optics and can support connections over distances of up to 10 kilometers, making them the appropriate choice for this scenario where the data centers are 6.2 miles apart. These transceivers are specifically engineered for longer distances and are suitable for interconnecting data centers across greater distances.

NEW QUESTION: 530

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

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

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 531

A user from a remote office is reporting slow file transfers. Which of the following tools will an engineer MOST likely use to get detailed measurement data?

- A. Packet capture
- B. IPerf
- C. SIEM log review
- D. Internet speed test

Answer: ([SHOW ANSWER](#)**)**

An engineer will most likely use IPerf to get detailed measurement data about the user's slow file transfers. IPerf is a tool used for measuring network performance and bandwidth, and it can be used to measure the speed and throughput of file transfers from the remote office. It can also provide detailed information about the latency and jitter of the connection, which can be used to troubleshoot the slow file transfers. Reference:

CompTIA Network+ Study Manual (Chapter 10, Page 214).

NEW QUESTION: 532

A network administrator is looking for a solution to extend Layer 2 capabilities and replicate backups between sites. Which of the following is the best solution?

- A. Security Service Edge
- B. Data center interconnect
- C. Infrastructure as code

D. Zero trust architecture

Answer: B (LEAVE A REPLY)

Data center interconnect (DCI) is a solution that allows Layer 2 connectivity and data replication between geographically dispersed data centers. DCI can be implemented using various technologies, such as optical networks, MPLS, VPNs, or Ethernet. DCI can provide benefits such as improved disaster recovery, load balancing, resource pooling, and cloud services.

Reference:

Data Center Interconnect - CompTIA Network+ N10-008 Domain 1.4 - YouTube1 CompTIA Network+ Certification Exam Objectives, page 92

NEW QUESTION: 533

A network administrator is investigating a network connectivity issue. The administrator runs a command to view the status of the network cards. The administrator receives the following output:

RX packets:45332 errors: 45332 dropped:0 overruns 0 frame:0

Which of the following should the administrator troubleshoot based on the output?

- A. TCP/IP address settings
- B. Physical layer components
- C. Buffers on the card filling up
- D. VLAN tagging configuration

Answer: B (LEAVE A REPLY)

NEW QUESTION: 534

Which of the following common agreements would a company most likely have an employee sign as a condition of employment?

- A. NDA
- B. ISP
- C. SLA
- D. MOU

Answer: A (LEAVE A REPLY)

An NDA, or non-disclosure agreement, is a legal contract that binds an employee to keep certain information confidential and not share it with unauthorized parties. This information may include trade secrets, intellectual property, business strategies, customer data, or other sensitive or proprietary information that gives the company a competitive advantage. An NDA protects the company's interests and prevents the employee from disclosing or using the information for personal gain or malicious purposes¹.

Reference

1 - 10 Types of Employment Contracts | Indeed.com

NEW QUESTION: 535

Which of the following authentication protocols should be used when securing a basic wireless network? (Choose two.)

- A. RDP

- B. SSL
- C. EAP
- D. WPA2
- E. SNMP
- F. WPA

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 536

A technician needs to set up a wireless connection that utilizes MIMO on non-overlapping channels. Which of the following would be the best choice?

- A. 802.11a
- B. 802.11b
- C. 802.11g
- D. 802.11n

Answer: ([SHOW ANSWER](#))

802.11n is the best choice for setting up a wireless connection that utilizes MIMO on non-overlapping channels. 802.11n is a wireless standard that offers faster speeds and longer range than previous standards. 802.11n uses multiple-input multiple-output (MIMO) technology, which allows multiple antennas to transmit and receive multiple spatial streams of data simultaneously. MIMO can improve wireless performance, reliability, and capacity by exploiting multipath propagation and spatial diversity. 802.11n also uses non-overlapping channels in both the 2.4 GHz and 5 GHz frequency bands to avoid interference and increase bandwidth. Non-overlapping channels are channels that do not share any part of their frequency spectrum with other channels. Reference: [CompTIA Network+ Certification Exam Objectives], 802.11n - Wikipedia

NEW QUESTION: 537

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 ([LEAVE A REPLY](#))

It's very common for ISPs to share common lines and such, especially when they are servicing the same physical location. It's therefore critically important to ensure path diversity, where the lines out of your ISP follow diverse paths to other routers. A common method for path diversity in smaller centers, for example, uses a fiber connection for the primary path and a very fast cellular connection as a failover. Use of both a fiber ISP and a different cable ISP can also lead to path diversity.

NEW QUESTION: 538

Given the following information:

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

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

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

Answer: (SHOW ANSWER)

Attenuation is the weakening of a signal as it travels long distances and is caused when wave signals travel too far without help. As a cable run gets longer, the attenuation increases, and the signal becomes weaker.

NEW QUESTION: 539

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, the administrator sees the 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 (LEAVE A REPLY)

NEW QUESTION: 540

The power company notifies a network administrator that it will be turning off the power to the building over the weekend.

Which of the following is the BEST solution to prevent the servers from going down?

- A. Redundant power supplies
- B. Uninterruptible power supply
- C. Generator
- D. Power distribution unit

Answer: C (LEAVE A REPLY)

UPS is an almost instant battery backup that prevents your devices and power from being interrupted, while generators have a longer start up time. Generators provide a much longer lasting backup power supply and can sustain your business for much longer than a UPS.

NEW QUESTION: 541

A corporation is looking for a method to secure all traffic between a branch office and its data center in order to provide a zero-touch experience for all staff members who work there. Which of the following would BEST meet this requirement?

- A. Site-to-site VPN
- B. VNC
- C. Remote desktop gateway
- D. Virtual LANs

Answer: A ([LEAVE A REPLY](#))

Explanation

A site-to-site VPN is a method that creates a secure and encrypted connection between two internet gateways, such as routers or firewalls, that belong to different networks . A site-to-site VPN can secure all traffic between a branch office and its data center by creating a virtual tunnel that protects the data from interception or tampering. A site-to-site VPN can also provide a zero-touch experience for all staff members who work there, as they do not need to install any software or configure any settings on their devices to access the data center resources. They can simply use their local network as if they were physically connected to the data center network.

VNC (Virtual Network Computing) is a method that allows remote access and control of a computer's desktop from another device over a network . VNC can enable staff members to work remotely by accessing their office computers from their home computers or mobile devices. However, VNC does not secure all traffic between a branch office and its data center, as it only works at the application layer and does not encrypt the network layer. VNC also does not provide a zero-touch experience for staff members, as they need to install software and configure settings on both the host and the client devices.

Remote desktop gateway is a method that allows remote access and control of a computer's desktop from another device over a network using the Remote Desktop Protocol (RDP). Remote desktop gateway can also enable staff members to work remotely by accessing their office computers from their home computers or mobile devices. However, remote desktop gateway does not secure all traffic between a branch office and its data center, as it only works at the application layer and does not encrypt the network layer. Remote desktop gateway also does not provide a zero-touch experience for staff members, as they need to install software and configure settings on both the host and the client devices.

Virtual LANs (VLANs) are methods that create logical subdivisions of a physical network based on criteria such as function, department, or security level. VLANs can improve network performance, security, and management by reducing broadcast domains, isolating traffic, and enforcing policies. However, VLANs do not secure all traffic between a branch office and its data center, as they only work at the data link layer and do not encrypt the network layer. VLANs also do not provide a zero-touch experience for staff members, as they need to configure settings on their network devices to join or leave a VLAN.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com

N10-008 dumps with Test Engine here: <https://www.braindumps.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 542

A network technician is installing an analog desk phone for a new receptionist. After running a new phone line, the technician now needs to crimp on a new connector. Which of the following connectors would MOST likely be used in this case?

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

Answer: ([SHOW ANSWER](#))

RJ11 as discussed before was widely used in analog telephony to connect the phone instrument and the cable.

NEW QUESTION: 543

A network administrator is notified that a user cannot access resources on the network. The network administrator checks the physical connections to the workstation labeled User 3 and sees the Ethernet is properly connected. However, the network interface's indicator lights are not blinking on either the computer or the switch. Which of the following is the most likely cause?

- A. The switch failed.
- B. The default gateway is wrong.
- C. The port is shut down.
- D. The VLAN assignment is incorrect.

Answer: ([SHOW ANSWER](#))

Explanation

If the port is shut down, it means that the switch has disabled the port and is not sending or receiving any traffic on it. This would explain why the network interface's indicator lights are not blinking on either the computer or the switch, and why the user cannot access resources on the network. The port could be shut down manually by the network administrator, or automatically by the switch due to security or error conditions.

References

Port shutdown is one of the common switch configuration options covered in Objective 2.3 of the CompTIA Network+ N10-008 certification exam¹.

Port shutdown can cause the network interface's indicator lights to stop blinking².

Port shutdown can prevent the user from accessing resources on the network³.

1: CompTIA Network+ Certification Exam Objectives, page 5 2: CompTIA Network+ N10-008: Switch not forwarding frames on trunked port³ 3: Cable Management - N10-008 CompTIA Network+ : 1.3

NEW QUESTION: 544

Which of the following policies is MOST commonly used for guest captive portals?

- A. AUP
- B. DLP

C. BYOD

D. NDA

Answer: A (LEAVE A REPLY)

AUP stands for Acceptable Use Policy, which is a policy that defines the rules and guidelines for using a network or service. A guest captive portal is a web page that requires users to agree to the AUP before accessing the Internet or other network resources. This is a common way to enforce security and legal compliance for guest users. Reference: https://www.arubanetworks.com/techdocs/Instant_87_WebHelp/Content/instant-ug/captive-portal/captive-portal.htm

NEW QUESTION: 545

A network engineer needs to enable device monitoring using authentication and encryption. Which of the following protocols offers this option?

A. SNMPv3

B. NetFlow

C. ESP

D. SSLv3

Answer: A (LEAVE A REPLY)

NEW QUESTION: 546

An organization set up its offices so that a desktop is connected to the network through a VoIP phone. The VoIP vendor requested that voice traffic be segmented separately from non-voice traffic. Which of the following would allow the organization to configure multiple devices with network isolation on a single switch port?

A. Subinterfaces

B. Link aggregation

C. Load balancing

D. Tunneling

Answer: (SHOW ANSWER)

It stated "multiple devices with network iSOLATION(separated) on a single switch port".

Therefore, its referring to Subinterfaces. Subinterfaces is a virtual interface that divides one physical interface into multiple logical interface.

NEW QUESTION: 547

Which Network Switch Port My Computer is Connected A network administrator is creating a VLAN that will only allow executives to connect to a data source.

Which of the following is this scenario an example of?

A. Availability

B. Confidentiality

C. Internal threat

D. External threat

E. Integrity

Answer: B (LEAVE A REPLY)

Confidentiality is the principle of preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information¹.

By creating a VLAN that will only allow executives to connect to a data source, the network administrator is implementing a form of network segmentation that enhances the confidentiality of the data.

This prevents unauthorized users or processes from accessing or modifying the data, which could compromise its integrity or availability. Confidentiality is one of the components of the CIA triad, a widely used information security model that guides the efforts and policies aimed at keeping data secure²³⁴.

References: Defending Your Network: A Comprehensive Guide to VLAN Hopping AttacksThe CIA triad:

Definition, components and examples | CSO OnlineExecutive Summary - NIST SP 1800-25 documentationThe

CIA Triad - Confidentiality, Integrity, and Availability ExplainedConfidentiality, Integrity and Availability - DevQA.io

NEW QUESTION: 548

A network administrator is troubleshooting an issue with a new Internet connection.

The ISP is asking detailed questions about the configuration of the router that the network administrator is troubleshooting.

Which of the following commands is the network administrator using? (Select TWO.)

- A. tcpdump
- B. show config
- C. hostname
- D. show route
- E. netstate
- F. show ip arp

Answer: B,D (LEAVE A REPLY)

The show config command (or some variation of it) is used to examine the configuration of a network device. For example, on a Cisco router, the show running-configuration command permits you to see the current configuration of the device, which is stored in the RAM of the device. To view the saved configuration that is loaded when the system is rebooted, you can use the show startup-configuration command.

The show route command (or some variation of it) is used to view the routing table configuration of the network device. On a Cisco router, you can use show ip route to view the IPv4 routing table.

Remember this is on a ROUTER, so netstat (Win/UNIX) does not work.

NEW QUESTION: 549

A network technician receives a report from the server team that a server's network connection is not working correctly. The server team confirms the server is operating correctly except for the network connection. The technician checks the switchport connected to the server and reviews the following data;

Metric	Value
Bytes input	441,164,698
Bytes output	2,625,115,257
Runts	0
CRCs	5,489
Collisions	1
MDIX	On
Speed	1,000
Duplex	Full

Which of the following should the network technician perform to correct the issue?

- A. Replace the Cat 5 patch cable with a Cat 6 cable
- B. Install a crossover cable between the server and the switch
- C. Reset the switchport configuration.
- D. Use NetFlow data from the switch to isolate the issue.
- E. Disable MDIX on the switchport and reboot the server.

Answer: [\(SHOW ANSWER\)](#)

Explanation

"Bad cables, incorrect pinouts, or bent pins: Faulty cables (with electrical characteristics preventing successful transmission) or faulty connectors (which do not properly make connections) can prevent successful data transmission at Layer 1. A bad cable could simply be an incorrect category of cable being used for a specific purpose. For example, using a Cat 5 cable (instead of a Cat 6 or higher cable) to connect two 1000BASE-TX devices would result in data corruption. Bent pins in a connector or incorrect pinouts could also cause data to become corrupted."

NEW QUESTION: 550

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 \(LEAVE A REPLY\)](#)

The MAC address table is a way to map each port to a MAC address. The technician can use the MAC table to find which MAC address is connected to which port.

NEW QUESTION: 551

A network technician needs to install security updates on several switches on the company's network. The management team wants this completed as quickly and efficiently as possible. Which of the following should the technician do to perform the updates?

- A. Upload the security update onto each switch using a terminal emulator and a console cable.
- B. Configure a TFTP server. SSH into each device, and perform the update.
- C. Replace each old switch with new switches that have the updates already performed.

D. Connect a USB memory stick to each switch and perform the update.

Answer: B (LEAVE A REPLY)

The best option to install security updates on multiple switches is to use a TFTP (Trivial File Transfer Protocol) server and SSH (Secure Shell) connections. A TFTP server is a simple and lightweight file server that can host the update files and transfer them to the switches over the network. SSH is a secure and encrypted protocol that can be used to remotely access and configure the switches. The technician can use SSH to log into each switch, download the update file from the TFTP server, and apply the update. This method is faster and more efficient than using a terminal emulator and a console cable, which would require physical access to each switch and a serial connection. It is also more cost-effective and less disruptive than replacing the switches with new ones. Using a USB memory stick is also possible, but it would still require physical access to each switch and a USB port, which may not be available on all models.

Reference:

[CompTIA Network+ N10-008 Certification Study Guide], Chapter 5: Network Operations, Section 5.4: Firmware Updates, pp. 283-284

[Professor Messer's CompTIA N10-008 Network+ Course Notes], Section 5.4: Firmware Updates, p. 71

[Professor Messer's CompTIA N10-008 Network+ Training Course], Video 5.4: Firmware Updates, 9:07 minutes

NEW QUESTION: 552

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 (LEAVE A REPLY)

A change management policy is a document that outlines the procedures and guidelines for making changes to a network or system, including how changes are approved, tested, and implemented. By following a change management policy, organizations can ensure that unnecessary modifications to the network are not permitted and version control is maintained. Reference:

Network+ N10-008 Objectives: 1.6 Given a scenario, implement network configuration and change management best practices.

NEW QUESTION: 553

A company has wireless APS that were deployed with 802.11g. A network engineer has noticed more frequent reports of wireless performance issues during the lunch hour in comparison to the rest of the day. The engineer thinks bandwidth consumption will increase while users are on their breaks, but network utilization logs do not show increased bandwidth numbers. Which Of the following would MOST likely resolve this issue?

- A.** Adding more wireless APS
- B.** Increasing power settings to expand coverage
- C.** Configuring the APS to be compatible with 802.11a
- D.** Changing the wireless channel used

Answer: C (LEAVE A REPLY)

802.11g is an older wireless standard that operates in the 2.4 GHz frequency band and has a maximum data rate of 54 Mbps. 802.11a is a newer wireless standard that operates in the 5 GHz frequency band and has a maximum data rate of 54 Mbps. By configuring the APS to be compatible with 802.11a, the network engineer can reduce interference and congestion in the 2.4 GHz band and improve wireless performance.

References: Network+ Study Guide Objective 2.5: Implement network troubleshooting methodologies

NEW QUESTION: 554

Which of the following security controls indicates unauthorized hardware modifications?

- A. Tamper-evident seals
- B. Biometric authentication
- C. Media device sanitization
- D. Change management policy

Answer: B (LEAVE A REPLY)

NEW QUESTION: 555

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

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

Answer: B (LEAVE A REPLY)

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: 556

A technician is checking network devices to look for opportunities to improve security. Which of the following tools would BEST accomplish this task?

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

Answer: (SHOW ANSWER)

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.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 557

Newly crimped 26ft (8m) STP Cat 6 patch cables were recently installed in one room to replace cables that were damaged by a vacuum cleaner. Now, users in that room are unable to connect to the network. A network technician tests the existing cables first. The 177ft (54m) cable that runs from the core switch to the access switch on the floor is working, as is the 115ft (35m) cable run from the access switch to the wall jack in the office. Which of the following is the MOST likely reason the users cannot connect to the network?

- A. Mixed UTP and STP cables are being used.
- B. The patch cables are not plenum rated.
- C. The cable distance is exceeded.
- D. An incorrect pinout on the patch cable is being used.

Answer: D (LEAVE A REPLY)

STP (Shielded Twisted Pair) cables are used to protect against electromagnetic interference (EMI). The cable distance is not exceeded, as the 26ft (8m) patch cable is within the maximum distance of 100 meters for Cat 6 cables. The patch cables are also plenum rated, which means they can be used in air plenums without emitting harmful fumes.

The most likely reason the users cannot connect to the network is that the pinout on the patch cable is incorrect. The pinout is the order in which the wires in the cable are connected to the RJ-45 connector. If the pinout is incorrect, the data signals will not be transmitted correctly and the user will not be able to connect to the network.

NEW QUESTION: 558

Which of the following is an example of on-demand scalable hardware that is typically housed in the vendor's data center?

- A. DaaS
- B. IaaS
- C. PaaS
- D. SaaS

Answer: B (LEAVE A REPLY)

Explanation

IaaS is an example of on-demand scalable hardware that is typically housed in the vendor's data center. IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing

resources over the internet. IaaS allows customers to rent servers, storage, network devices, and other hardware components from a cloud service provider, rather than purchasing and maintaining them on-premise.

IaaS offers advantages such as scalability, flexibility, cost-effectiveness, and reliability. Customers can adjust their hardware resources according to their needs and pay only for what they use. Customers can also access their hardware resources from anywhere via a web browser or an API. References: [CompTIA Network+ Certification Exam Objectives], What Is Infrastructure as a Service (IaaS)? | IBM

NEW QUESTION: 559

A security vendor needs to add a note to the DNS to validate the ownership of a company domain before services begin. Which of the following records did the security company MOST likely ask the company to configure?

- A.** TXT
- B.** AAAA
- C.** CNAME
- D.** SRV

Answer: [\(SHOW ANSWER\)](#)

TXT stands for Text and is a type of DNS record that can store arbitrary text data associated with a domain name. TXT records can be used for various purposes, such as verifying the ownership of a domain, providing information about a domain, or implementing security mechanisms such as SPF (Sender Policy Framework) or DKIM (DomainKeys Identified Mail). In this scenario, the security company most likely asked the company to configure a TXT record with a specific value that can prove the ownership of the domain. AAAA stands for IPv6 Address and is a type of DNS record that maps a domain name to an IPv6 address. CNAME stands for Canonical Name and is a type of DNS record that maps an alias name to another name. SRV stands for Service and is a type of DNS record that specifies the location of a service on a network.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.8:

Explain the purposes and use cases for advanced networking devices.

NEW QUESTION: 560

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.** 802.1Q
- C.** Duplex
- D.** LACP

Answer: **D** [\(LEAVE A REPLY\)](#)

LACP (Link Aggregation Control Protocol) can be used to increase bandwidth to a server without replacing hardware. LACP allows multiple network connections to be bundled together to increase throughput and provide redundancy. This is also known as link aggregation or NIC teaming. By using LACP, the IT technician can combine multiple gigabit ports on the server to create a single high-bandwidth connection without replacing any hardware. STP (Spanning Tree Protocol), 802.1Q (VLAN tagging), and duplex settings do not increase bandwidth but rather control network topology, network segmentation, and communication speed, respectively.

NEW QUESTION: 561

An IT technician is working on a support ticket regarding an unreachable web-site. The technician has utilized the ping command to the website, but the site is still unreachable. Which of the following tools should the technician use NEXT?

- A. ipconfig
- B. tracert
- C. arp
- D. netstat

Answer: B (LEAVE A REPLY)

Explanation

tracert is a command-line tool that can trace the route of a packet from the source to the destination. It can show the number of hops, the IP address and hostname of each router, and the round-trip time for each hop. tracert can help the technician troubleshoot the unreachable website by identifying where the packet is dropped or delayed along the path. ipconfig is a command-line tool that can display and configure the IP settings of a network interface. arp is a command-line tool that can display and manipulate the Address Resolution Protocol (ARP) cache, which maps IP addresses to MAC addresses. netstat is a command-line tool that can display network connections, routing tables, and statistics.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.4: Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

NEW QUESTION: 562

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

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

Answer: C (LEAVE A REPLY)

A customer needs six usable IP addresses, which means they need a subnet that can accommodate at least six hosts, excluding the network address and the broadcast address¹².

The subnet mask determines how many bits are used for the network prefix and how many bits are used for the host identifier¹². The more bits are used for the network prefix, the fewer bits are available for the host identifier, and vice versa¹².

The number of usable IP addresses in a subnet can be calculated by subtracting two from the number of possible host identifiers, which is $2^{(\text{number of host bits})}$ ¹².

For example, a subnet mask of 255.255.255.0 (/24 in CIDR notation) has 24 bits for the network prefix and 8 bits for the host identifier. Therefore, the number of usable IP addresses in this subnet is $2^8 - 2 = 254$ ¹².

The four options in the question have different subnet masks, which correspond to different numbers of usable IP addresses, as shown in the table below:

Table

Subnet mask

CIDR notation

Number of host bits

Number of usable IP addresses

255.255.255.128

/25

7

126

255.255.255.192

/26

6

62

255.255.255.224

/27

5

30

255.255.255.240

/28

4

14

Therefore, the best option that meets the customer's requirement of six usable IP addresses is C.

255.255.255.224, which has 30 usable IP addresses in the subnet12.

Reference:

1: Subnet Cheat Sheet - 24 Subnet Mask, 30, 26, 27, 29, and other IP Address CIDR Network Reference

2: Network Subnets (CIDR) and Usable IP Addresses Reference Guide

NEW QUESTION: 563

A network administrator needs to implement a solution to mediate access to the internet- Which of the following should the administrator most likely implement?

A. Router

B. Cloud gateway

C. proxy

D. Intrusion prevention system

Answer: ([SHOW ANSWER](#))

A proxy is a solution that can mediate access to the internet. A proxy is a server that acts as an intermediary between a client and a destination server on the internet. A proxy can perform various functions, such as filtering, caching, logging, or modifying requests and responses. A proxy can help improve network performance, security, and privacy by reducing bandwidth consumption, blocking malicious or unwanted content, monitoring network activity, and hiding the client's identity or location. Reference: [CompTIA Network+ Certification Exam Objectives], What Is a Proxy Server? | Proxy Server Definition | Avast

NEW QUESTION: 564

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: ([SHOW ANSWER](#))

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. Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html>

NEW QUESTION: 565

Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

- A. Scope options
- B. Reservation
- C. Dynamic assignment
- D. Exclusion
- E. Static assignment

Answer: ([SHOW ANSWER](#))

Explanation

A reservation should be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP. A reservation is a feature of DHCP that allows an administrator to assign a fixed 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, even if it is powered off or disconnected from the network for a long time. References: <https://docs.microsoft.com/en-us/windows-server/troubleshoot/configure-dhcp-reservations>

NEW QUESTION: 566

An organization has a guest network with a network IP range of 192.168.1.0/28 using a DHCP pool. One visitor reported difficulties connecting and configured a static IP address. Following this action, another visitor reported intermittent connection issues. Which of the following is the most likely reason?

- A. Address pool exhaustion
- B. Duplicate IP addresses
- C. Misconfigured default gateway
- D. Incorrect subnet mask

Answer: B ([LEAVE A REPLY](#))

A duplicate IP address occurs when two devices on the same network have the same IP address assigned to them. This can cause intermittent connection issues, as the network devices may not be able to distinguish between the two conflicting devices. A duplicate IP address can be caused by a visitor manually configuring a static IP address that is already in use by another device on the guest network. The network IP range of 192.168.1.0/28 has only 14 usable host addresses, so the chances of a duplicate IP address are higher than a larger network.

References

- * 1: Troubleshooting IP Configurations - CompTIA Network+ N10-006 - 4.6
- * 2: Troubleshooting Duplicate IP Addresses - CompTIA Network+ N10-005: 2.5
- * 3: Network Address Translation - N10-008 CompTIA Network+ : 1.4

NEW QUESTION: 567

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

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

Answer: C (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 568

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

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 569

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 (LEAVE A REPLY)

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: 570

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

Answer: D (LEAVE A REPLY)

NEW QUESTION: 571

A user reports having intermittent connectivity issues to the company network. The network configuration for the user reveals the following:

IP address: 192.168.1.10

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.254

The network switch shows the following ARP table:

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

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

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

Answer: (SHOW ANSWER)

This is the most likely cause of the user's connection issues, because the ARP table of the switch shows that there are two devices with the same IP address of 192.168.1.10, but different MAC addresses. This indicates that there is an IP address conflict on the network, where two devices are trying to use the same IP address.

This can cause intermittent connectivity issues, as the switch may not be able to forward packets to the correct destination .

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 572

A systems administrator has two network switches that need to be cabled together via copper cabling. Neither of the switches support MDIX. Which of the following types of cables should the administrator use?

- A. Straight
- B. Crossover
- C. Patch cable
- D. Rollover

Answer: (SHOW ANSWER)

A 'crossover cable' is a type of Ethernet cable that has two ends with reversed wiring. This means that the transmit pins on one end are connected to the receive pins on the other end. This type of cable is used to directly connect two similar devices, such as two switches, without the need for a hub or a router.

NEW QUESTION: 573

A technician is writing documentation regarding a company's server farm. The technician needs to confirm the server name for all Linux servers. Which of the following commands should the technician run?

- A. ipconfig
- B. nslookup
- C. arp
- D. route

Answer: ([SHOW ANSWER](#))

Explanation

The nslookup command should be run to confirm the server name for all Linux servers. Nslookup is a tool that queries DNS servers to resolve hostnames to IP addresses or vice versa. It can also provide other information about DNS records, such as MX, NS, SOA, etc. By running nslookup with the IP address of a Linux server, the technician can obtain its hostname. References:

<https://www.howtogeek.com/663056/how-to-use-the-nslookup-command-on-linux/>

NEW QUESTION: 574

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: ([SHOW ANSWER](#))

Network traffic is the amount of data moving across a computer network at any given time. Network traffic is broken down into data packets and sent over a network before being reassembled by the receiving device or computer¹.

Network traffic has two directional flows, north-south and east-west. North-south traffic refers to client-to-server traffic that moves between the data center and the rest of the network (i.e., a location outside of the data center). East-west traffic refers to traffic within a data center, also known as server-to-server traffic².

A data center is a facility that houses computing and networking equipment, such as servers, switches, routers, firewalls, and storage devices. Data centers provide centralized processing, storage, and access to data and applications for organizations and users³.

Data centers need to handle both north-south and east-west traffic efficiently and securely. North-south traffic is typically generated by users or customers who access data or applications hosted in the data center from the internet or other networks. East-west traffic is typically generated by applications or services that communicate with each other within the data center.

The question asks which of the following describes traffic going in and out of a data center from the internet. The correct answer is B. North-South, because this is the type of traffic that flows between the data center and the external network. The other options are incorrect for the following reasons:

A . Demarcation point is the physical point where the responsibility for the network changes from one party to another, such as from a service provider to a customer. It does not describe network traffic.

C . Fibre Channel is a high-speed network technology that connects servers and storage devices in a data center. It does not describe network traffic, but rather a network protocol.

D . Spine and leaf is a network topology that consists of two layers of switches: spine switches that interconnect with leaf switches, and leaf switches that connect to servers and devices. It does not describe network traffic, but rather a network design. Reference:

1: What Is Network Traffic? Definition and How To Monitor It

2: 32 Flashcards | Quizlet

3: Data center - Wikipedia

4: Data Center Traffic Patterns: North-South vs. East-West

5: Demarcation point - Wikipedia

6: Fibre Channel - Wikipedia

7: Spine and leaf - Wikipedia

NEW QUESTION: 575

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

A. 22

B. 53

C. 110

D. 389

E. 995

F. 3389

Answer: B,E ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 576

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

IP address:	196.26.4.30
Subnet mask:	255.255.255.224
Gateway:	196.24.4.1

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

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

Answer: C ([LEAVE A REPLY](#))

The IP address configured on the router interface is 196.26.4.1/26, which belongs to the IP range assigned by the ISP (196.26.4.0/26). However, this IP address is not valid for this interface because it is the network address of the subnet, which cannot be assigned to any host device. The network address is the first address of a subnet that identifies the subnet itself. The valid IP addresses for this subnet are from 196.26.4.1 to 196.26.4.62, excluding the network address (196.26.4.0) and the broadcast address (196.26.4.63). The router interface should be configured with a valid IP address within this range to restore Internet connectivity for all users. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

<https://www.techopedia.com/definition/24136/network-address>

NEW QUESTION: 577

An ISP is unable to provide services to a user in a remote area through cable and DSL. Which of the following is the NEXT best solution to provide services without adding external infrastructure?

- A. Satellite
- B. Leased line
- C. Metro optical
- D. Fiber

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 578

A customer cannot reach a web application on a local server. The network consultant suspects that the server is not accepting the HTTPS connection. Which of the following commands should the consultant run on the server to determine what is occurring?

- A. netstat
- B. arp
- C. route
- D. nmap

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 579

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

- A. Upgrade security via the use of an NFV technology
- B. Increase VPN availability by using a SDWAN technology.
- C. Secure web access to internal corporate resources.

D. Connect two data centers across the internet.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 580

A network technician needs to resolve some issues with a customer's SOHO network.

The customer reports that some of the devices are not connecting to the network, while others appear to work as intended.

INSTRUCTIONS

Troubleshoot all the network components and review the cable test results by Clicking on each device and cable.

Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.



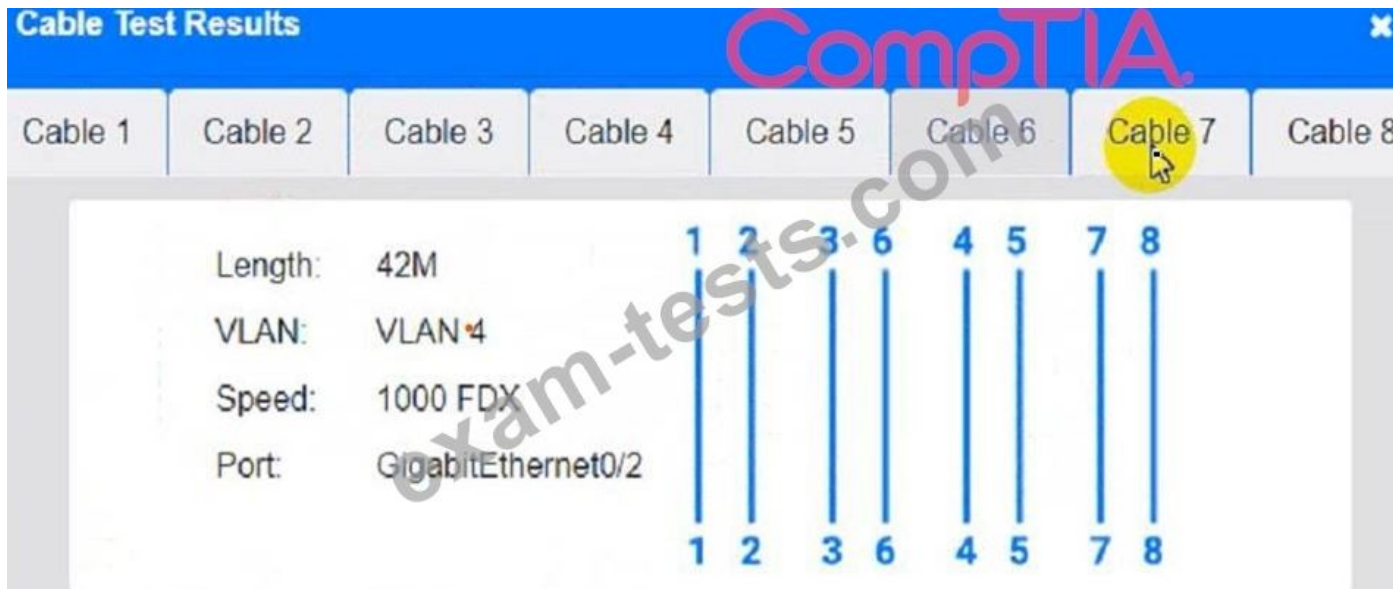
Cable Test Results:

Cable 1:

Cable 2:

Cable 3:

Cable 4:



Answer:

See the Explanation for detailed information on this simulation.

Explanation

(Note: Ips will be change on each simulation task, so we have given example answer for the understanding) To troubleshoot all the network components and review the cable test results, you can use the following steps:

Click on each device and cable to open its information window.

Review the information and identify any problems or errors that may affect the network connectivity or performance.

Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.

Fill in the remediation form using the drop-down menus provided.

Here is an example of how to fill in the remediation form for PC1:

The component with a problem is PC1.

The problem is Incorrect IP address.

The solution is Change the IP address to 192.168.1.10.

You can use the same steps to fill in the remediation form for other components.

To enter commands in each device, you can use the following steps:

Click on the device to open its terminal window.

Enter the command `ipconfig /all` to display the IP configuration of the device, including its IP address, subnet mask, default gateway, and DNS servers.

Enter the command `ping <IP address>` to test the connectivity and reachability to another device on the network by sending and receiving echo packets. Replace `<IP address>` with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.

Enter the command `tracert <IP address>` to trace the route and measure the latency of packets from the device to another device on the network by sending and receiving packets with increasing TTL values.

Replace `<IP address>` with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.

Here is an example of how to enter commands in PC1:

Click on PC1 to open its terminal window.

Enter the command `ipconfig /all` to display the IP configuration of PC1. You should see that PC1 has an incorrect IP address of 192.168.2.10, which belongs to VLAN 2 instead of VLAN 1.

Enter the command `ping 192.168.1.1` to test the connectivity to Core Switch 1. You should see that PC1 is unable to ping Core Switch 1 because they are on different subnets.

Enter the command `tracert 192.168.1.1` to trace the route to Core Switch 1. You should see that PC1 is unable to reach Core Switch 1 because there is no route between them.

You can use the same steps to enter commands in other devices, such as PC3, PC4, PC5, and Server 1.

NEW QUESTION: 581

Which of the following routing protocols is hierarchal by nature and uses the router ID to control convergence?

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

Answer: B (LEAVE A REPLY)

OSPF stands for Open Shortest Path First, which is a link-state routing protocol that is hierarchal by nature and uses the router ID to control convergence. OSPF divides a large network into areas, which are logical groupings of routers that share the same topology information. Each area has a unique identifier and a designated router that connects it to the backbone area (area 0). OSPF uses the router ID, which is a 32-bit number that uniquely identifies each router in the network, to establish adjacencies and exchange routing information. OSPF also uses the router ID to break ties when choosing the best path to a destination. OSPF converges faster than distance-vector routing protocols such as RIP and EIGRP, as it uses the Dijkstra algorithm to calculate the shortest path based on the link cost. BGP, on the other hand, is a path-vector routing protocol that is used to exchange routing information between autonomous systems on the Internet. BGP does not use the router ID to control convergence, but rather uses attributes such as AS path, local preference, and MED to select the best route. BGP is not hierarchal by nature, as it does not divide the network into areas, but rather uses prefixes and policies to control the routing behavior.

References

- * 1: OSPF - N10-008 CompTIA Network+ : 2.1
- * 2: CompTIA Network+ N10-008 Certification Study Guide, page 146-149
- * 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 19
- * 4: CompTIA Network+ N10-008 Certification Practice Test, question 8

NEW QUESTION: 582

A customer called the help desk to report a network issue. The customer recently added a hub between the switch and the router in order to duplicate the traffic flow to a logging device. After adding the hub, all the Other network components that were connected to the switch slowed more than expected. Which Of the following is the MOST likely cause Of the issue?

- A. Duplex mismatch
- B. Flow control failure
- C. STP malfunction

D. 802.1Q disabled

Answer: A (LEAVE A REPLY)

A duplex mismatch is a situation where two devices on a network have different duplex settings, such as full-duplex or half-duplex. Full-duplex means that a device can send and receive data simultaneously, while half-duplex means that a device can only send or receive data at a time. A duplex mismatch can cause performance issues, such as collisions, errors, or slow throughput. In this scenario, the customer added a hub between the switch and the router. A hub is a device that operates at half-duplex and broadcasts all traffic to all ports. A switch and a router are devices that operate at full-duplex and forward traffic to specific ports.

Therefore, adding a hub between the switch and the router can cause a duplex mismatch and slow down all the other network components that were connected to the switch.

References: <https://www.comparitech.com/net-admin/hub-vs-switch-vs-router/>

<https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/10561-3.html>

NEW QUESTION: 583

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: (SHOW ANSWER)

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: 584

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

- A. Cold site
- B. Hot site

C. Warm site

D. Cloud site

Answer: C (LEAVE A REPLY)

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

<https://www.comptia.org/blog/what-is-a-warm-site>

NEW QUESTION: 585

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

A. dig

B. nmap

C. tracert

D. nslookup

Answer: (SHOW ANSWER)

nmap is the tool that would help identify which ports are open on the remote file server. nmap stands for Network Mapper, which is a free and open-source tool that can perform various network scanning and discovery tasks. nmap can help identify which ports are open on a remote device by sending probes or packets to different ports and analyzing the responses. nmap can also provide information about the operating system, services, versions, firewalls, or vulnerabilities of the remote device. nmap can be useful for network administrators, security professionals, or hackers to monitor, audit, or attack network devices. Reference: [CompTIA Network+ Certification Exam Objectives], Nmap - Free Security Scanner For Network Exploration & Security Audits

NEW QUESTION: 586

Which of the following network cables involves bouncing light off of protective cladding?

A. Twinaxial

B. Coaxial

C. Single-mode

D. Multimode

Answer: D (LEAVE A REPLY)

Multimode fiber optic cables use multiple paths of light that bounce off the cladding, which is a layer of glass or plastic that surrounds the core of the cable.

<https://www.explainthatstuff.com/fiberoptics.html>

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 587

Which of the following routing technologies uses a successor and a feasible successor?

- A. IS-IS
- B. OSPF
- C. BGP
- D. EIGRP

Answer: D (LEAVE A REPLY)

EIGRP stands for Enhanced Interior Gateway Routing Protocol, which is a hybrid routing protocol that uses a successor and a feasible successor to determine the best route to a destination. A successor is the next-hop router that has the lowest cost (or metric) to reach the destination, and a feasible successor is a backup router that has a cost that is less than the cost of the successor. EIGRP uses the successor and the feasible successor to achieve fast convergence and load balancing. EIGRP also uses a Diffusing Update Algorithm (DUAL) to maintain the routing table and avoid routing loops. IS-IS, OSPF, and BGP are other routing protocols that do not use a successor and a feasible successor, but rather use different algorithms and criteria to select the best route.

References

- * 1: EIGRP - N10-008 CompTIA Network+ : 2.1
- * 2: CompTIA Network+ N10-008 Certification Study Guide, page 150-151
- * 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 20
- * 4: CompTIA Network+ N10-008 Certification Practice Test, question 9

NEW QUESTION: 588

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 (LEAVE A REPLY)

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: 589

An organization has a security staff shortage and must prioritize efforts in areas where the staff will have the most impact. In particular, the focus is to avoid expending resources on identifying non-relevant events. A security analyst is reviewing web server logs and sees the following:

```
202.180.155.1 - [14/Jan/2021:04:12:28 -0200] "GET /img/us.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:28 -0200] "GET /img/org.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:29 -0200] "GET /img/org2.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:29 -0200] "GET /img/org3.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:30 -0200] "GET /img/org4.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:31 -0200] "GET /img/directors.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:31 -0200] "GET /img/directors2.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:32 -0200] "GET /img/directors3.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:33 -0200] "GET /img/directors4.gif" 404 295
```

Which of the following should the analyst recommend?

- A. Configuring the web server log to filter out 404 errors on image files
- B. Updating firewall rules to block 202.180.155.1
- C. Resyncing the network time server and monitoring logs for future anomalous behavior
- D. Checking with the penetration testing team to see if the team ran any scans on January 14, 2021

Answer: A (LEAVE A REPLY)

This answer will help the organization to avoid expending resources on identifying non-relevant events, as the 404 errors on image files are not indicative of any security threat or issue, but rather a misconfiguration or a broken link on the web server. The 404 errors on image files are also very frequent and repetitive, as shown by the web server log, which can clutter the log and make it harder to spot any relevant events. By filtering out these errors, the analyst can focus on more important events and reduce the noise in the log.

The other answers are not as good as A, because they either do not address the problem of identifying non-relevant events, or they are based on incorrect assumptions or information. For example:

* B. Updating firewall rules to block 202.180.155.1 is not a good answer, because the IP address 202.180.155.1 is not doing anything malicious or suspicious, but rather requesting image files that do not exist on the web server. Blocking this IP address will not improve the security of the web server, but rather create unnecessary firewall rules and possibly deny legitimate access to the web server.

* C. Resyncing the network time server and monitoring logs for future anomalous behavior is not a good answer, because there is no evidence that the network time server is out of sync or causing any problems. The web server log shows that the entries are all within a few minutes of each other, which is normal and expected. Resyncing the network time server will not help the analyst to identify non-relevant events, but rather waste time and resources on an unrelated task.

* D. Checking with the penetration testing team to see if the team ran any scans on January 14, 2021 is not a good answer, because the web server log does not show any signs of a penetration test or a scan. The log shows only 404 errors on image files, which are not typical of a penetration test or a scan, which would usually target different types of files, ports, or vulnerabilities. Checking with the penetration testing team will not help the analyst to identify non-relevant events, but rather distract the analyst from the actual events and possibly create false alarms.

<https://www.professormesser.com/network-plus/n10-008/n10-008-video/general-network-troubleshooting-n10-0>

NEW QUESTION: 590

An administrator needs to connect two laptops directly to each other using 802.11ac but does not have an AP available. Which of the following describes this configuration?

- A. Basic service set
- B. Extended service set
- C. Independent basic service set
- D. MU-MIMO

Answer: C ([LEAVE A REPLY](#))

A basic service set (BSS) is a group of wireless devices that share the same service set identifier (SSID) and communicate with each other through a single access point (AP). A BSS is also known as an infrastructure mode network¹.

An extended service set (ESS) is a group of two or more BSSs that are connected by a distribution system (DS), such as a switch or a router. An ESS allows wireless devices to roam between different APs and maintain network connectivity. An ESS is also known as a wireless LAN (WLAN)².

An independent basic service set (IBSS) is a group of wireless devices that communicate with each other directly without using an AP or a DS. An IBSS is also known as an ad hoc network or a peer-to-peer network³.

MU-MIMO (Multi-User Multiple-Input Multiple-Output) is a technology that allows an AP to transmit data to multiple wireless devices simultaneously using multiple antennas and spatial streams. MU-MIMO can improve the network efficiency and performance by reducing the waiting time and increasing the throughput⁴.

The scenario described in the question is an example of an IBSS, as the two laptops are connected directly to each other using 802.11ac without an AP. Therefore, the correct answer is C.

Reference:

- 1: BSS
- 2: ESS
- 3: IBSS
- 4: MU-MIMO

NEW QUESTION: 591

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

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

Answer: ([SHOW ANSWER](#)**)**

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

NEW QUESTION: 592

A technician is configuring a bandwidth-monitoring tool that supports payloads of 1,600 bytes. Which of the following should the technician configure for this tool?

- A. LACP
- B. Flow control
- C. Port mirroring
- D. Jumbo frames

Answer: D (LEAVE A REPLY)

Jumbo frames are Ethernet frames that can carry more than the standard 1,500 bytes of payload data. Jumbo frames can support payloads of up to 9,000 bytes, depending on the network device and configuration. Jumbo frames can improve network performance by reducing the overhead of packet headers and increasing the efficiency of data transmission. Jumbo frames can also reduce the CPU utilization of the sender and receiver devices, as they require fewer interrupts and processing cycles. However, jumbo frames also have some drawbacks, such as increased latency, fragmentation, and compatibility issues. Therefore, jumbo frames should be used with caution and only in networks that support them end-to-end.

A technician who is configuring a bandwidth-monitoring tool that supports payloads of 1,600 bytes should enable jumbo frames for this tool, as this would allow the tool to capture and analyze more data per frame and provide more accurate and detailed results. However, the technician should also ensure that the network devices and interfaces that the tool is connected to also support jumbo frames, and that the MTU (maximum transmission unit) is set to the same value across the network path.

Reference

What are Jumbo Frames?

How to Enable Jumbo Frames

CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION: 593

A network administrator needs to create a way to redirect a network resource that has been on the local network but is now hosted as a SaaS solution. Which of the following records should be used to accomplish the task?

- A. TXT
- B. AAA
- C. PTR
- D. CNAME

Answer: D (LEAVE A REPLY)

Explanation

CNAME stands for Canonical Name, and it is a type of DNS record that creates an alias for another domain name. A CNAME record can be used to redirect a network resource that has been moved to a different location, such as a SaaS solution. For example, if a web server that was previously hosted on the local network with the domain name `www.example.com` is now hosted by a SaaS provider with the domain name `www.saasprovider.com`, a CNAME record can be created to point `www.example.com` to `www.saasprovider.com`. This way, the users can still access the web server using the original domain name, and the DNS server will resolve it to the new domain name.

References

CNAME is one of the common DNS record types covered in Objective 1.6 of the CompTIA Network+ N10-008 certification exam1.

CNAME can be used to redirect a network resource that has been moved to a different location²³.

CNAME creates an alias for another domain name²³.

1: CompTIA Network+ Certification Exam Objectives, page 4 2: DNS Record Types - N10-008 CompTIA Network+ : 1.6 3: The Official CompTIA Network+ Student Guide (Exam N10-008), Chapter 1, page 32

NEW QUESTION: 594

A network administrator is trying to create a subnet, which is the most efficient size possible, for 31 laptops. Which of the following network subnets would be best in this situation?

- A.** 10.10.10.0/24
- B.** 10.10.10.0/25
- C.** 10.10.10.0/26
- D.** 10.10.10.0/27

Answer: ([SHOW ANSWER](#))

A /27 subnet mask has 32 IP addresses, of which 30 are usable for hosts. This is the smallest subnet that can accommodate 31 laptops, as the other options have either too few or too many IP addresses. A /27 subnet mask is equivalent to 255.255.255.224 in decimal notation, and has a wildcard mask of 0.0.0.31. The network address is 10.10.10.0, and the broadcast address is 10.10.10.31. The usable host range is 10.10.10.1 to 10.10.10.30.

References

1: Subnet Cheat Sheet - 24 Subnet Mask, 30, 26, 27, 29, and other IP Address CIDR Network References
2: IP Subnet Calculator

NEW QUESTION: 595

A network is experiencing a number of CRC errors during normal network communication. At which of the following layers of the OSI model will the administrator MOST likely start to troubleshoot?

- A.** Layer 1
- B.** Layer 2
- C.** Layer 3
- D.** Layer 4
- E.** Layer 5
- F.** Layer 6
- G.** Layer 7

Answer: ([SHOW ANSWER](#))

CRC errors are cyclic redundancy check errors that occur when data is corrupted during transmission. CRC errors are usually caused by physical layer issues such as faulty cables, connectors, ports, or interference. The network administrator will most likely start to troubleshoot at layer 1 of the OSI model, which is the physical layer that deals with the transmission of bits over a medium. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 4.0 Network Troubleshooting and Tools, Objective 4.1 Given a scenario, implement network troubleshooting methodology.

NEW QUESTION: 596

In a data center, data traffic that moves east-west is flowing between:

- A. the top-of-rack and distribution switches.
- B. the server and the cloud.
- C. the top-of-rack and core switches.
- D. top-of-rack switches.

Answer: D (LEAVE A REPLY)

East-west data traffic in a data center refers to the traffic that flows laterally within the data center, typically between servers within the same data center. This type of traffic usually flows between top-of-rack (ToR) switches, which connect multiple servers or devices in the same rack to each other or to other racks without necessarily routing through the core or distribution layers of the network architecture. This is opposed to north-south traffic, which typically flows in and out of the data center to the wider network or internet. Therefore, the correct answer is "top-of-rack switches".

NEW QUESTION: 597

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

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

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

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 598

A network technician is configuring a wireless network that consists of multiple APS for better coverage and allows roaming between the APS. Which of the following types of SSIDs should the technician configure?

- A. Basic Service Set
- B. Independent Basic Service Set
- C. Extended Service Set
- D. Distribution System Service

Answer: C (LEAVE A REPLY)

An extended service set (ESS) is a type of SSID that allows multiple access points (APs) to share the same SSID and provide seamless roaming for wireless clients. An ESS consists of two or more basic service sets (BSSs), which are individual APs with their own SSIDs. A distribution system (DS), such as a wired Ethernet LAN, connects the BSSs and enables data transfer between them. A wireless client can associate with any AP in the ESS and move from one BSS to another without losing connectivity or reauthenticating.

Reference:

CompTIA Network+ N10-008 Certification Exam Objectives, page 51

CompTIA Network+ Cert Guide: Wireless Networking, page 12

NEW QUESTION: 599

A technician is troubleshooting intermittent connectivity between devices and viewing the following syslog entries from a switch:

```
21 Feb 2022 16:02:0231 NOTIFICATION %LINK-I-DOWN: G1/10
21 Feb 2022 16:02:0262 NOTIFICATION %LINK-I-UP: G1/10
21 Feb 2022 16:03:5321 NOTIFICATION %LINK-I-DOWN: G1/10
21 Feb 2022 16:03:7873 NOTIFICATION %LINK-I-UP: G1/10
```

Which of the following are these entries indicative of?

- A. DDoS attack
- B. Jitter
- C. Latency
- D. Link flapping

Answer: D ([LEAVE A REPLY](#))

The syslog entries are indicative of link flapping, which is when a switch port rapidly transitions between the up and down states. This can cause intermittent connectivity issues, network instability, and increased CPU utilization on the switch. Link flapping can be caused by various factors, such as faulty cables, misconfigured interfaces, duplex mismatches, or network attacks. To troubleshoot link flapping, the technician should check the physical layer, verify the interface settings, and monitor the network traffic for anomalies.

Reference:

What is Link Flapping? - CompTIA1

Troubleshooting Switch Port and Interface Problems - Cisco2

Network Troubleshooting - N10-008 CompTIA Network+ : 4.1 - YouTube3

NEW QUESTION: 600

Which of the following WAN technologies utilizes an optical SONET carrier and has a maximum bandwidth of 155.54Mbps?

- A. DS3
- B. OC3
- C. T3
- D. E3

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 601

A technician is consolidating a topology with multiple SSIDs 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 (LEAVE A REPLY)

A service set identifier (SSID) is a name that identifies a wireless network¹².

A wireless network can have multiple SSIDs, each with different settings and security parameters, to create separate logical networks for different purposes or users¹².

However, having multiple SSIDs can also create some challenges, such as increased management overhead, reduced bandwidth, and interference¹².

A technician can consolidate a topology with multiple SSIDs into one unique SSID deployment, by using a single SSID for the entire wireless network and applying different policies or profiles based on other criteria, such as user roles, device types, or locations¹².

One of the benefits of having a unique SSID deployment is that it enables seamless roaming, which is the ability of a wireless device to move from one access point (AP) to another without losing connectivity or experiencing delays¹².

Seamless roaming is possible after this new configuration, because the device does not need to scan for and authenticate with different SSIDs as it moves across the network, but can simply switch to the best available AP that shares the same SSID¹².

The other options are not features that will be possible after this new configuration, because they are either unrelated or unaffected by the SSID deployment:

B . A basic service set (BSS) is a group of wireless devices that communicate with a single AP³. It is not a feature that will be possible after this new configuration, because it is a basic unit of a wireless network that does not depend on the SSID deployment³.

Wi-Fi Protected Access (WPA) is a security protocol that encrypts and authenticates wireless data transmissions⁴. It is not a feature that will be possible after this new configuration, because it is a security option that can be applied to any SSID deployment, regardless of the number of SSIDs⁴.

D . Multi-user multiple-input multiple-output (MU-MIMO) is a technology that allows an AP to transmit data to multiple devices simultaneously, increasing the network efficiency and performance. It is not a feature that will be possible after this new configuration, because it is a technology option that can be supported by any SSID deployment, as long as the AP and the devices are compatible with it.

Reference:

1: Wireless LAN Topologies - N10-008 CompTIA Network+ : 3.1

2: CompTIA Network+ N10-008 Full Course for Beginners - Wireless LAN Topologies (3.1)

3: Wireless Network Types - N10-008 CompTIA Network+ : 3.1

4: Wireless Security Protocols - N10-008 CompTIA Network+ : 3.2

[5]: Wireless Technologies - N10-008 CompTIA Network+ : 3.3

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam

questions have been updated and answers have been corrected get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 602

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: (SHOW ANSWER)

Twisted cable, also known as twisted pair cable, is a type of copper cable that consists of two or more insulated wires twisted together to reduce crosstalk and electromagnetic interference. Twisted cable is classified into different categories based on its performance and bandwidth. Category 5e (Cat 5e) is a common type of twisted cable that supports data transmission up to 1000 Mbps (1 Gbps) and has a maximum length of 100 meters. Cat 5e is a cost-effective alternative that provides proper cabling and supports gigabit Ethernet devices, such as switches, routers, and computers.

The other options are not as cost-effective or suitable for gigabit Ethernet devices as twisted cable with a minimum Cat 5e certification. Multimode fiber is a type of optical fiber that uses multiple light paths to transmit data over short distances. It requires expensive connectors, such as SC (Subscriber Connector), and specialized equipment, such as media converters, to connect to Ethernet devices. Twinaxial cabling is a type of coaxial cable that has two inner conductors and a common shield. It is mainly used for short-range, high-speed connections, such as Serial Attached SCSI (SAS) or 10 Gigabit Ethernet (10GbE). It uses different connectors, such as F-type, than Ethernet devices. Cable termination is the process of attaching a connector to the end of a cable.

TIA/EIA-568-B is a standard that specifies the wiring scheme and pinout for twisted cable connectors, such as RJ-45. Cable termination does not affect the type or performance of the cable itself.

References:

* [CompTIA Network+ N10-008 Certification Study Guide], Chapter 3: Network Components, Section 3.1: Cabling Solutions, pp. 113-116

* [Professor Messer's CompTIA N10-008 Network+ Course Notes], Section 3.1: Cabling Solutions, pp. 28-29

* [Professor Messer's CompTIA N10-008 Network+ Training Course], Video 3.1: Cabling Solutions, 17:34 minutes

NEW QUESTION: 603

A network security engineer locates an unapproved wireless bridge connected to the corporate LAN that is broadcasting a hidden SSID, providing unauthenticated access to internal resources. Which of the following types of attacks BEST describes this finding?

- A.** Rogue access point Most Voted
- B.** Evil twin

C. ARP spoofing

D. VLAN hopping

Answer: (SHOW ANSWER)

A rogue access point is an unauthorized wireless device that is connected to a network without the knowledge or consent of the network administrator¹². It can provide unauthorized access to internal resources, bypass security policies, and expose the network to various attacks¹².

A hidden SSID is a wireless network name that is not broadcasted by the access point. It is intended to increase security by preventing unauthorized users from discovering the network, but it can also be used by rogue access points to avoid detection³.

A wireless bridge is a device that connects two or more wireless networks or segments. It can extend the range of a wireless network, but it can also be used by rogue access points to connect to the corporate LAN.

Therefore, the scenario described in the question is an example of a rogue access point attack, where an unapproved wireless bridge is connected to the corporate LAN and broadcasts a hidden SSID, providing unauthenticated access to internal resources.

The other options are not correct because:

An evil twin is a malicious access point that mimics a legitimate one, usually by using the same SSID and security settings. It is used to trick users into connecting to the fake network and steal their credentials or data. This is different from a rogue access point, which does not necessarily impersonate a legitimate network, but rather creates a new one².

ARP spoofing is a technique that allows an attacker to intercept or modify network traffic by sending fake ARP messages that associate their MAC address with an IP address of another host or device. It is used to perform man-in-the-middle attacks, denial-of-service attacks, or session hijacking. This is different from a rogue access point, which does not involve ARP messages or MAC address spoofing².

VLAN hopping is a technique that allows an attacker to access or send traffic to a VLAN that they are not authorized to. It can be done by exploiting misconfigured switches, trunk ports, or tagging protocols. This is different from a rogue access point, which does not involve VLANs or switches².

Reference:

1: Rogue Access Points and Evil Twins - Baeldung

2: What's the difference between an evil twin and a rogue access point? - Information Security Stack Exchange

3: What is a Hidden SSID? - How-To Geek

4: How to Find Hidden & Saved Passwords in Windows - Lifewire

5: What is a Wireless Bridge? - Linksys

6: How to Set Up a Wireless Bridge - PCMag

7: What is an Evil Twin Attack? - Norton

8: Which attack is more dangerous: Evil Twin or ARP spoofing? - Information Security Stack Exchange

9: What is ARP Spoofing? - Palo Alto Networks

10: How to Prevent ARP Spoofing - Cloudflare

11: What is VLAN Hopping? - Cisco

12: How to Prevent VLAN Hopping Attacks - Pluralsight

STION 398 A network security engineer locates an unapproved wireless bridge

NEW QUESTION: 604

A network technician is troubleshooting an area where the wireless connection to devices is poor. The technician theorizes that the signal-to-noise ratio in the area is causing the issue. Which of the following should the technician do NEXT?

- A. Move the access point to a different location.
- B. Remove any electronics that might be causing interference.
- C. Run diagnostics on the relevant devices.
- D. Escalate the issue to the vendor's support team.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 605

An IT administrator received an assignment with the following objectives

- * Conduct a total scan within the company's network for 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. netstat
- D. tcpdump

Answer: A ([LEAVE A REPLY](#))

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: 606

Which of the following should be implemented to allow remote users to access network resources while only redirecting necessary traffic?

- A. Split-tunnel VPN
- B. Geofencing
- C. Client-to-site VPN
- D. Remote desktop gateway

Answer: A ([LEAVE A REPLY](#))

Explanation

A split-tunnel VPN is a VPN feature that allows remote users to access network resources while only redirecting necessary traffic through the VPN tunnel. A split-tunnel VPN enables users to choose which applications or websites to secure with the VPN and which to connect normally through the internet. This can improve

performance, conserve bandwidth, and avoid compatibility issues with some services that depend on the user's location. A split-tunnel VPN can also allow users to access local devices or resources that are not accessible through the VPN.

NEW QUESTION: 607

Which of the following DNS records maps an alias to a true name?

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

Answer: D ([LEAVE A REPLY](#))

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

NEW QUESTION: 608

Which of the following attacks encrypts user data and requires a proper backup implementation to recover?

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

Answer: C ([LEAVE A REPLY](#))

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

NEW QUESTION: 609

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 of 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 ([LEAVE A REPLY](#))

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: 610

A network technician is deploying multiple switches for a new office. The switches are separately managed and need to be cabled in to support dual firewalls in a HA setup. Which of the following should the technician enable to support proper stability of the network switches?

- A. NTP
- B. STP
- C. CDMA
- D. 802.1Q
- E. LACP

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 611

A network technician receives a report from the server team that a server's network connection is not working correctly. The server team confirms the server is operating correctly except for the network connection. The technician checks the switchport connected to the server and reviews the following data;

Metric	Value
Bytes input	441,164,698
Bytes output	2,625,115,257
Runts	0
CRCs	5,489
Collisions	1
MDIX	On
Speed	1,000
Duplex	Full

Which of the following should the network technician perform to correct the issue?

- A. Replace the Cat 5 patch cable with a Cat 6 cable
- B. Install a crossover cable between the server and the switch
- C. Reset the switchport configuration.
- D. Use NetFlow data from the switch to isolate the issue.
- E. Disable MDIX on the switchport and reboot the server.

Answer: A ([LEAVE A REPLY](#))

Explanation

"Bad cables, incorrect pinouts, or bent pins: Faulty cables (with electrical characteristics preventing successful transmission) or faulty connectors (which do not properly make connections) can prevent successful data transmission at Layer 1. A bad cable could simply be an incorrect category of cable being used for a specific

purpose. For example, using a Cat 5 cable (instead of a Cat 6 or higher cable) to connect two 1000BASE-TX devices would result in data corruption. Bent pins in a connector or incorrect pinouts could also cause data to become corrupted."

NEW QUESTION: 612

A technician is troubleshooting a user's connectivity issues and finds that the computer's IP address was changed to 169.254.0.1.

Which of the following is the most likely reason?

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

Answer: B ([LEAVE A REPLY](#))

Explanation

IP addresses beginning with 169.254. are called link-local addresses or APIPA (Automatic Private IP Addressing)¹. They are assigned by the computer itself when it cannot reach a DHCP server to obtain a valid IP address from the network². This can happen for several reasons, such as a faulty router, a misconfigured network, or a disconnected cable³.

To troubleshoot this issue, the technician should check the network settings, the router configuration, and the physical connection of the computer. The technician should also try to renew the IP address by using the command `ipconfig /renew` in Windows or `dhclient` in Linux. If the problem persists, the technician may need to contact the network administrator or the ISP for further assistance.

NEW QUESTION: 613

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 ([LEAVE A REPLY](#))

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: 614

The power company notifies a network administrator that it will be turning off the power to the building over the weekend. Which of the following is the BEST solution to prevent the servers from going down?

- A. Redundant power supplies
- B. Uninterruptible power supply
- C. Generator
- D. Power distribution unit

Answer: B (LEAVE A REPLY)

A power outage is a loss of electrical power to a network device or system, which can cause data loss, downtime, or damage¹².

A network administrator should implement power protection measures to prevent or mitigate the impact of power outages on the network¹².

One of the power protection measures is an uninterruptible power supply (UPS), which is a device that provides backup power to a network device or system in case of a power outage¹².

A UPS works by using a battery or other energy source to supply power to the connected device or system when the main power source fails or drops below a certain level¹².

A UPS can also provide power conditioning, which is the process of filtering and regulating the quality of the power supply to prevent fluctuations, spikes, or surges that can damage or disrupt the network device or system¹².

A UPS is the BEST solution to prevent the servers from going down in this scenario, because it can provide continuous and stable power to the servers during the power outage, allowing them to operate normally or shut down gracefully¹².

The other options are not the best solution to prevent the servers from going down, because they have different limitations or disadvantages:

A Redundant power supplies are devices that provide an alternative power source to a network device or system in case of a power failure or malfunction of the primary power source¹². They are not the best solution to prevent the servers from going down, because they still depend on the availability of the main power supply or another power source, such as a generator or a UPS¹². They also do not provide power conditioning, which can protect the servers from power fluctuations¹².

C . A generator is a device that converts mechanical energy into electrical energy, which can be used to power a network device or system in case of a power outage¹². It is not the best solution to prevent the servers from going down, because it can take some time to start up and switch over to the generator power, which can cause a brief interruption or data loss¹². It also requires fuel, maintenance, and ventilation, which can add to the cost and complexity of the power protection system¹².

D . A power distribution unit (PDU) is a device that distributes power from a single source to multiple outlets, which can be used to connect and manage multiple network devices or systems¹². It is not a solution to prevent the servers from going down, because it does not provide backup power or power conditioning, but only distributes the existing power supply¹². It can also introduce a single point of failure, if the PDU itself fails or malfunctions¹².

Reference:

1: Power Protection - N10-008 CompTIA Network+ : 5.5

2: CompTIA Network+ N10-008 Full Course for Beginners - Power Protection (5.5)

NEW QUESTION: 615

A security administrator is trying to prevent incorrect IP addresses from being assigned to clients on the network. Which of the following would MOST likely prevent this and allow the network to continue to operate?

- A. Configuring DHCP snooping on the switch
- B. Preventing broadcast messages leaving the client network
- C. Blocking ports 67/68 on the client network
- D. Enabling port security on access ports

Answer: A (LEAVE A REPLY)

Explanation

To prevent incorrect IP addresses from being assigned to clients on the network and allow the network to continue to operate, the security administrator should consider configuring DHCP (Dynamic Host Configuration Protocol) snooping on the switch. DHCP snooping is a security feature that is used to prevent unauthorized DHCP servers from operating on a network. It works by allowing the switch to monitor and validate DHCP traffic on the network, ensuring that only legitimate DHCP messages are forwarded to clients.

This can help to prevent incorrect IP addresses from being assigned to clients, as it ensures that only authorized DHCP servers are able to provide IP addresses to clients on the network.

NEW QUESTION: 616

A network administrator walks into a data center and notices an unknown person is following closely. The administrator stops and directs the person to the security desk. Which of the following attacks did the network administrator prevent?

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

Answer: B (LEAVE A REPLY)

Tailgating is a type of physical security attack in which an unauthorized person follows an authorized person into a restricted area, such as a data center, without proper identification or authentication. Tailgating can allow attackers to access sensitive data, equipment, or network resources, or to plant malicious devices or software. The network administrator prevented tailgating by stopping and directing the unknown person to the security desk, where they would have to verify their identity and purpose.

References: Digital Threats and Cyberattacks at the Network Level Network attacks and how to prevent them.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com

N10-008 dumps with Test Engine here: <https://www.braindumps.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 617

Which of the following IP packet header fields is the mechanism for ending loops at Layer 3?

- A. Checksum
- B. Type
- C. Time-to-live
- D. Protocol

Answer: ([SHOW ANSWER](#))

Explanation

The time-to-live (TTL) field is the mechanism for ending loops at Layer 3, which is the network layer of the OSI model. The TTL field is an 8-bit field that indicates the maximum time or number of hops that an IP packet can travel before it is discarded. Every time an IP packet passes through a router, the router decrements the TTL value by one. If the TTL value reaches zero, the router drops the packet and sends an ICMP message back to the source, informing that the packet has expired. This way, the TTL field prevents an IP packet from looping endlessly in a network with routing errors or cycles¹²³.

The other options are not mechanisms for ending loops at Layer 3. The checksum field is a 16-bit field that is used to verify the integrity of the IP header. The checksum field is calculated by adding all the 16-bit words in the header and taking the one's complement of the result. If the checksum field does not match the calculated value, the IP packet is considered corrupted and discarded¹². The type field, also known as the type of service (TOS) or differentiated services code point (DSCP) field, is an 8-bit field that is used to specify the quality of service (QoS) or priority of the IP packet. The type field can indicate how the packet should be handled in terms of delay, throughput, reliability, or cost¹². The protocol field is an 8-bit field that is used to identify the transport layer protocol that is encapsulated in the IP packet. The protocol field can indicate whether the payload is a TCP segment, a UDP datagram, an ICMP message, or another protocol¹².

NEW QUESTION: 618

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 619

A network administrator replaced a faulty NIC in a printer, but the printer is still not reachable. The printer is configured with the correct IP address, mask, and gateway, and a link light is lit on the switch port that the printer is attached to. Which of the following is the best command for the administrator to run first on the switch?

- A. show vlan
- B. show route

C. show arp

D. show config

Answer: A (LEAVE A REPLY)

The best command for the administrator to run first on the switch is show vlan, which displays the VLAN configuration information on the switch, such as the VLAN IDs, names, and ports. The show vlan command can help the administrator to verify if the printer is assigned to the correct VLAN, and if there is any mismatch or misconfiguration that prevents the printer from being reachable. The show route command displays the routing table on the switch, which is not relevant for the printer connectivity, as the printer is configured with the correct gateway. The show arp command displays the ARP cache on the switch, which maps the IP addresses to the MAC addresses of the devices. The show arp command can help the administrator to check if the switch has learned the MAC address of the printer, but it is not the best command to run first, as the ARP cache can be cleared or updated frequently. The show config command displays the running configuration on the switch, which includes the VLAN configuration, but it also includes other information that is not related to the printer issue, such as the hostname, the interface settings, the security settings, and so on. The show config command can be overwhelming and time-consuming to analyze, so it is not the best command to run first.

Reference

1: VLANs and Trunking - N10-008 CompTIA Network+ : 2.3

2: N10-008 CompTIA Network+ : 5.5

3: Interface Configurations - N10-008 CompTIA Network+ : 2.3

4: Configuring VLANs - CompTIA Network+ N10-006 - 2.6

NEW QUESTION: 620

Due to concerns around single points of failure, a company decided to add an additional WAN to the network. The company added a second MPLS vendor to the current MPLS WAN and deployed an additional WAN router at each site. Both MPLS providers use OSPF on the WAN network, and EIGRP is run internally. The first site to go live with the new WAN is successful, but when the second site is activated significant network issues occur. Which of the following is the MOST likely cause for the WAN instability?

A. A routing loop

B. Asymmetrical routing

C. A switching loop

D. An incorrect IP address

Answer: B (LEAVE A REPLY)

Explanation

Asymmetrical routing is the most likely cause for the WAN instability. When two different routing protocols are used, like OSPF and EIGRP, it can cause asymmetrical routing, which results in traffic being routed differently in each direction. This can lead to instability in the WAN. A CDP neighbor change, a switching loop, or an incorrect IP address are not likely causes for WAN instability.

NEW QUESTION: 621

Which of the following DNS records maps an alias to a true name?

A. AAAA

- B. NS
- C. TXT
- D. CNAME

Answer: D ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 622

A network administrator receives a call about a network printer that is not working for a workstation. The network administrator verifies the printer is turned on. Given the following information:

Router's gateway IP: 10.0.0.1/25

Device: Printer

IP address	10.1.0.60
Subnet mask	255.255.255.128

Device: Workstation

IP address	10.0.0.126
Subnet mask	255.255.255.192

Which of the following should the administrator change to remediate this issue? (Choose two.)

- A. The subnet on the router
- B. The IP address on the printer
- C. The subnet on the printer
- D. The IP address on the router
- E. The subnet on the workstation
- F. The IP address on the workstation

Answer: ([SHOW ANSWER](#))

The printer's IP address and subnet place it in a different network segment than the workstation. The workstation and router are on the 10.0.0.0/26 network, while the printer is on the 10.1.0.0/25 network. Changing the printer's IP address to match the workstation's subnet or modifying the workstation's subnet to match the printer's network can resolve the issue.

NEW QUESTION: 623

A network administrator received complaints of intermittent network connectivity issues. The administrator investigates and finds that the network design contains potential loop scenarios. Which of the following should the administrator do?

- A. Enable spanning tree.

- B. Configure port security.
- C. Change switch port speed limits.
- D. Enforce 802.1Q tagging.

Answer: A ([LEAVE A REPLY](#))

Spanning tree is a protocol that prevents network loops by dynamically disabling or enabling switch ports based on the network topology. Network loops can cause intermittent connectivity issues, such as broadcast storms, MAC address table instability, and multiple frame transmission. By enabling spanning tree, the network administrator can ensure that there is only one active path between any two network devices at any given time.

Reference:

CompTIA Network+ N10-008 Certification Exam Objectives, page 91

CompTIA Network+ Cert Guide: Switching and Virtual LANs, page 172

NEW QUESTION: 624

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 625

A network administrator is investigating a network event that is causing all communication to stop. The network administrator is unable to use SSH to connect to the switch but is able to gain access using the serial console port. While monitoring port statistics, the administrator sees the following:

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

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

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 626

A network device is configured to send critical events to a syslog server; however, the following alerts are not being received:

Severity 5 LINK-UPDOWN: Interface 1/1, changed state to down

Severity 5 LINK-UPDOWN: Interface 1/3, changed state to down

Which of the following describes the reason why the events are not being received?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 627

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

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

Answer: A ([LEAVE A REPLY](#))

The valid alternative to maintain a deployed proxy technology while saving physical space in the data center by moving the network service to the virtualization infrastructure is NFV (Network Function Virtualization).

NFV is a technique that allows network functions, such as proxies, firewalls, routers, or load balancers, to be implemented as software applications running on virtual machines or containers. NFV reduces the need for dedicated hardware devices and improves scalability and flexibility of network services. References: CompTIA Network+ N10-008 Certification Study Guide, page 440; The Official CompTIA Network+ Student Guide (Exam N10-008), page 16-11.

NFV can be used to virtualize a wide variety of network functions, including proxy servers. By virtualizing proxy servers, organizations can save physical space in the data center and improve the scalability and efficiency of their networks.

To virtualize a proxy server using NFV, an organization would need to deploy a virtualization platform, such as VMware ESXi or Microsoft Hyper-V. The organization would then need to install a virtual proxy server appliance on the virtualization platform.

Once the virtual proxy server appliance is installed, it can be configured and used just like a physical proxy server.

NFV is a relatively new technology, but it is quickly gaining popularity as organizations look for ways to improve the efficiency and scalability of their networks.

NEW QUESTION: 628

A network administrator needs to provide remote clients with access to an internal web application. Which of the following methods provides the highest flexibility and compatibility while encrypting only the connection to the web application?

- A. Clientless VPN
- B. Virtual desktop
- C. Virtual network computing
- D. mGRE tunnel

Answer: A ([LEAVE A REPLY](#))

Explanation

A clientless VPN is a method of providing remote clients with access to an internal web application without installing any additional software or dedicated VPN client on their devices. Instead, users access the VPN through a web browser, utilizing a web portal or gateway provided by the VPN service. This method provides the highest flexibility and compatibility, as it supports various operating systems and devices, and encrypts only the connection to the web application, not the entire traffic of the device.

NEW QUESTION: 629

A technician is trying to configure a previously owned WAP. The technician successfully logs into the administrative console and attempts to input the IP address on the WAP. However, the WAP is not accepting the command. Which of the following is causing the problem?

- A. The WAP antenna is damaged
- B. The LWAPP image is installed on the WAP
- C. The terminal emulation software is misconfigured
- D. The WAP transmitter light is dim

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 630

A network administrator is installing a new server in the data center. The administrator is concerned the amount of traffic generated will exceed 1GB. and higher-throughput NiCs are not available for installation. Which of the following is the BEST solution for this issue?

- A. Install an additional NIC and configure LACP.
- B. Remove some of the applications from the server.
- C. Configure the NIC to use full duplex
- D. Configure port mirroring to send traffic to another server.
- E. Install a SSD to decrease data processing time.

Answer: ([SHOW ANSWER](#))

A NIC is a network interface card that enables a device to connect to a network using a wired or wireless medium. A NIC has a specific speed and bandwidth capacity that determines how much data it can transmit and receive per second. A higher-throughput NIC can handle more traffic than a lower-throughput NIC.

LACP is a link aggregation protocol that allows multiple physical links to be combined into a single logical link. LACP can increase the bandwidth, reliability, and load balancing of a network connection by distributing traffic across multiple links. LACP is also known as IEEE 802.3ad or port channeling.

A network administrator can install an additional NIC on a server and configure LACP to combine the two NICs into one logical link. This can effectively double the throughput of the server's network connection and allow it to handle more traffic without exceeding 1GB. This is the best solution for this issue because it improves the performance and availability of the server without affecting its functionality or requiring additional hardware.

The other options are not the best solutions for this issue because they either do not increase the throughput of the server's network connection, or they have negative impacts on the server's functionality or performance.

Removing some of the applications from the server may reduce the traffic generated, but it may also affect the

server's role and service delivery. Configuring the NIC to use full duplex may improve the efficiency of the network communication, but it does not increase the bandwidth capacity of the NIC. Configuring port mirroring to send traffic to another server may help with monitoring or troubleshooting, but it does not reduce the traffic load on the original server. Installing a SSD may decrease the data processing time of the server, but it does not affect the network throughput of the server. Reference:

CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Devices and Technologies, Section 2.2: Network Device Functions and Features, Subsection: Network Interface Cards, pp. 72-74.

CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Devices and Technologies, Section 2.3: Network Cabling and Connectors, Subsection: Link Aggregation, pp. 87-88.

Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 2.2: Network Devices, Subsection: Network Interface Cards, p. 28.

Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 2.3: Network Cabling and Connectors, Subsection: Link Aggregation, p. 31.

NEW QUESTION: 631

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

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

Answer: D (LEAVE A REPLY)

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 632

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 633

A network technician is working to deploy a new subnet to support 500 hosts. The technician needs to limit the number of unused IP addresses. Which of the following subnets should the technician choose?

- A. 255.255.224.0
- B. 255.255.248.0
- C. 255.255.252.0
- D. 255.255.254.0

Answer: ([SHOW ANSWER](#))

To get 500 hosts you need 9 host bits, that gives us a mask of 255.255.254.0 /23. This gives us 510 hosts, with 508 useable addresses. They did not mention expandability, so we should not read that into the answer, they did however, asked to have the fewest unused addresses.

NEW QUESTION: 634

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: ([SHOW ANSWER](#))

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: 635

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

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

Answer: A ([LEAVE A REPLY](#))

Coaxial cable is a type of cable that consists of a central copper conductor surrounded by an insulating layer and a braided metal shield. Coaxial cable is commonly used to connect a cable modem to an ISP by transmitting data over cable television networks. Coaxial cable can support high bandwidth and long distances with minimal interference or attenuation. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\),](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0),)

NEW QUESTION: 636

Ann, a new user, is unable to communicate on the network from her computer. A technician has verified that the cables are functioning properly. Based on the information below, which action should the technician take to correct Ann's problem?

Computer_A Switch_A

IP: 10.0.0.60 Int VLAN10

SM: 255.255.255.0 IP address 10.0.0.1/28

GW: 10.0.0.1 Speed 100 Duplex Full

- A. Change the IP address of the computer to 10.0.0.12
- B. Change the duplex on the switch interface to half
- C. Change the subnet mask of the computer to 255.255.255.240
- D. Change the speed on the switch interface to 10Mbps

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 637

While working in a coffee shop, an attacker watches a user log in to a corporate system and writes down the user's log-in credentials. Which of the following social engineering attacks is this an example of?

- A. Shoulder surfing
- B. Dumpster diving
- C. Phishing
- D. Tailgating

Answer: A ([LEAVE A REPLY](#))

Shoulder surfing is the social engineering attack where an attacker watches a user log in to a corporate system and writes down the user's log-in credentials. Social engineering is a type of attack that exploits human psychology and behavior to manipulate or trick people into revealing sensitive information or performing malicious actions. Shoulder surfing is a form of social engineering that involves observing or eavesdropping on someone's screen, keyboard, or paper documents to obtain confidential information such as passwords, PINs, or credit card numbers. Shoulder surfing can be done in person or remotely using cameras or other devices. Shoulder surfing can be prevented by using privacy filters, locking screens, shielding keyboards, or being aware of one's surroundings. References: [CompTIA Network+ Certification Exam Objectives], What Is Shoulder Surfing? | Definition & Examples | Forcepoint

NEW QUESTION: 638

A security engineer is trying to connect cameras to a 12-port PoE switch, but only eight cameras turn on. Which of the following should the engineer check first?

- A. Ethernet cable type
- B. Voltage
- C. Transceiver compatibility
- D. DHCP addressing

Answer: (SHOW ANSWER)

The most likely reason why only eight cameras turn on is that the PoE switch does not have enough power budget to supply all 12 cameras. The engineer should check the voltage and wattage ratings of the PoE switch and the cameras, and make sure they are compatible and sufficient. The Ethernet cable type, transceiver compatibility, and DHCP addressing are less likely to cause this problem, as they would affect the data transmission rather than the power delivery.

Reference:

CompTIA Network+ N10-008 Certification Study Guide, page 181

CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 352

PoE Troubleshooting: The Common PoE Errors and Solutions³

NEW QUESTION: 639

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

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

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

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

Answer: C (LEAVE A REPLY)

Explanation

The IP address configured on the router interface is 196.26.4.1/26, which belongs to the IP range assigned by the ISP (196.26.4.0/26). However, this IP address is not valid for this interface because it is the network address of the subnet, which cannot be assigned to any host device. The network address is the first address of a subnet that identifies the subnet itself. The valid IP addresses for this subnet are from 196.26.4.1 to 196.26.4.62, excluding the network address (196.26.4.0) and the broadcast address (196.26.4.63). The router interface should be configured with a valid IP address within this range to restore Internet connectivity for all users. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

<https://www.techopedia.com/definition/24136/network-address>

NEW QUESTION: 640

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

- A. A Layer 3 switch

- B. A proxy server
- C. A NGFW
- D. A WLAN controller

Answer: (SHOW ANSWER)

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

NEW QUESTION: 641

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

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

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

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

Answer: C (LEAVE A REPLY)

Explanation

CRC stands for Cyclic Redundancy Check, and it is a type of error-detecting code used to detect accidental changes to raw data. If the CRC count is increasing on a particular interface, it indicates that there might be an issue with the cabling, which is causing data corruption. References:

Network+ N10-008 Objectives: 2.1 Given a scenario, troubleshoot common physical connectivity issues.

NEW QUESTION: 642

Which of the following systems would MOST likely be found in a screened subnet?

- A. LDAP
- B. RADIUS
- C. FTP
- D. SQL

Answer: (SHOW ANSWER)

NEW QUESTION: 643

You are tasked with verifying the following requirements are met in order to ensure network security.

Requirements:

Datacenter

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic Building A

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide devices to support 5 additional different office users Add an additional mobile user Replace the Telnet

server with a more secure solution Screened subnet Ensure network is subnetted to allow all devices to

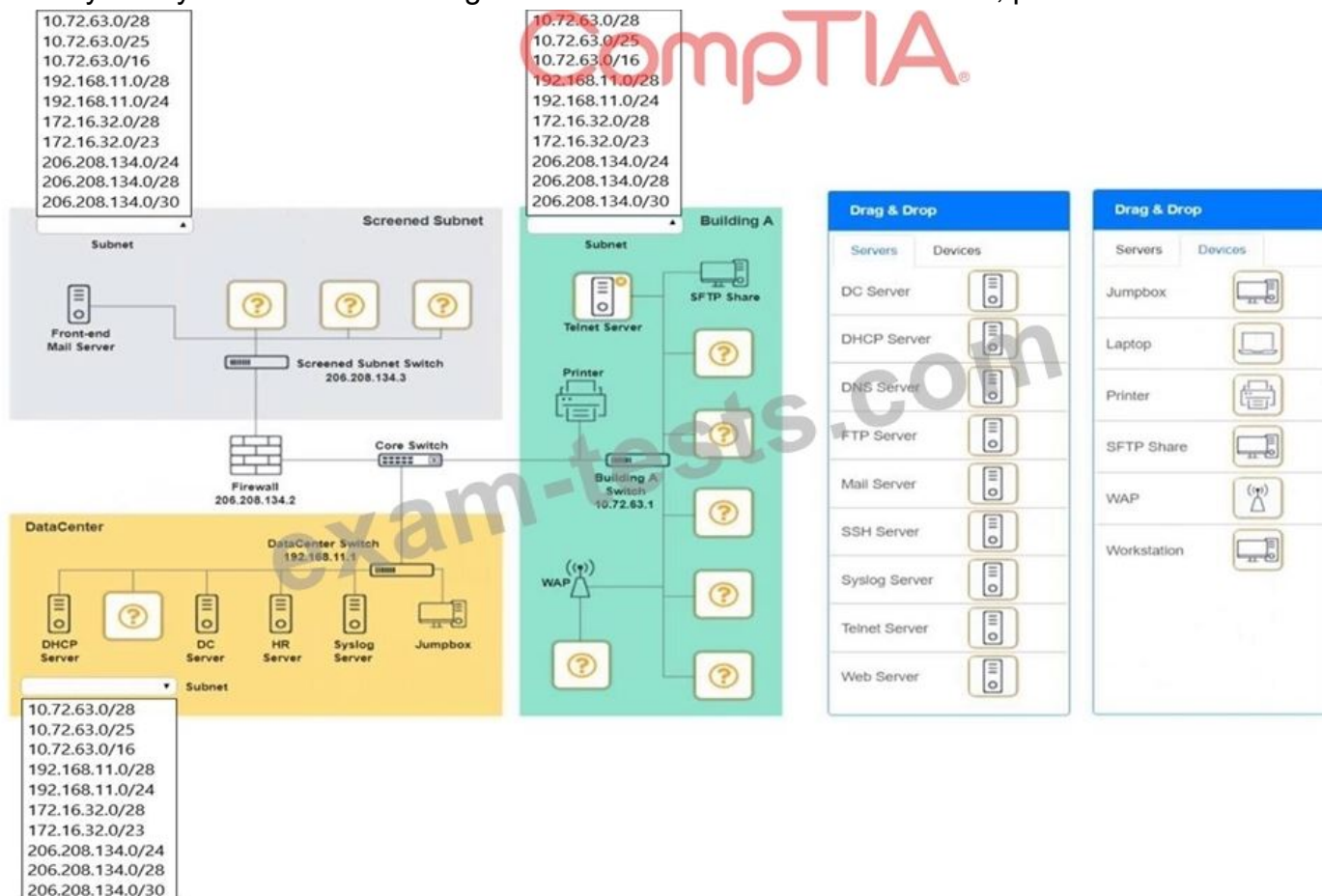
communicate properly while minimizing address space usage Provide a server to handle external 80/443 traffic

Provide a server to handle port 20/21 traffic INSTRUCTIONS Drag and drop objects onto the appropriate

locations. Objects can be used multiple times and not all placeholders need to be filled.

Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



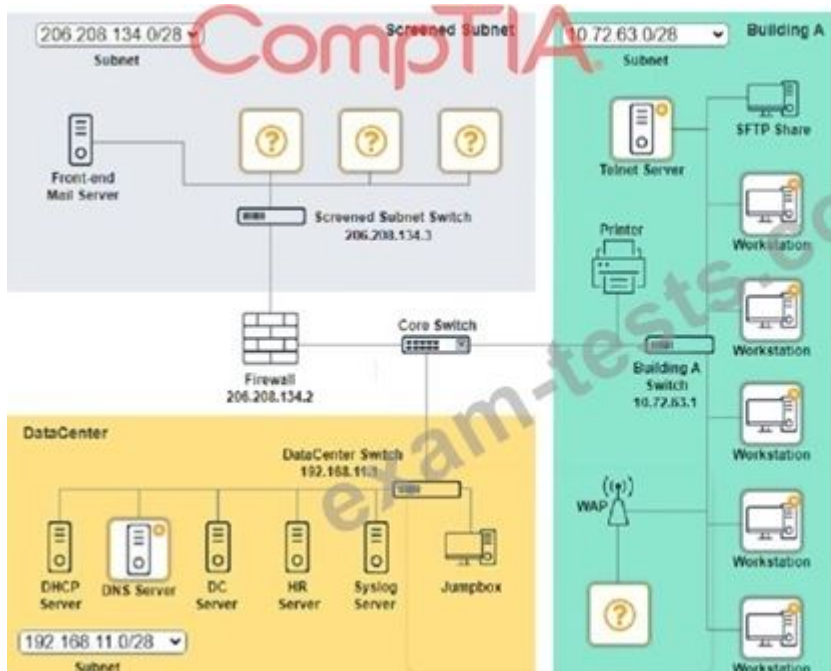
Answer:

See explanation below

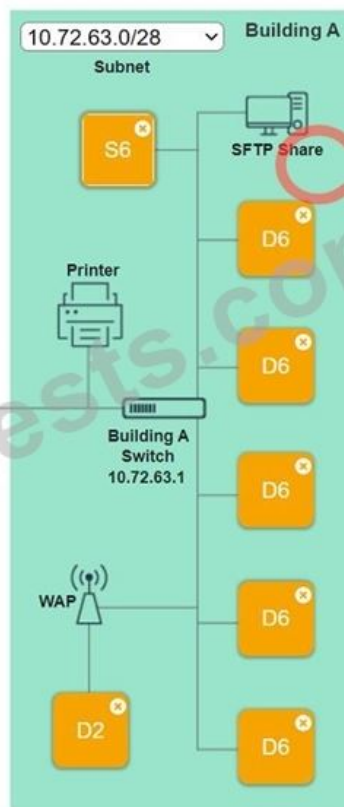
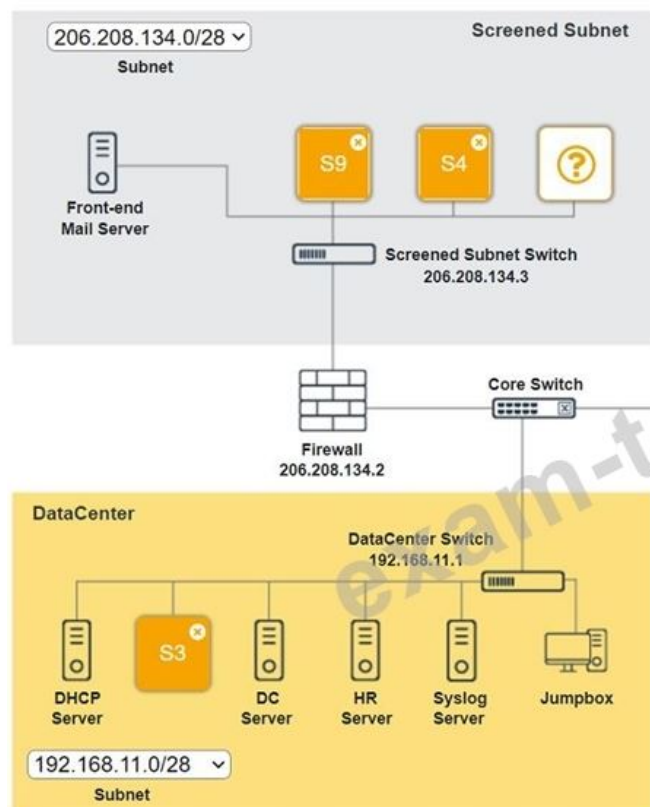
Explanation:

Screened Subnet devices - Web server, FTP server

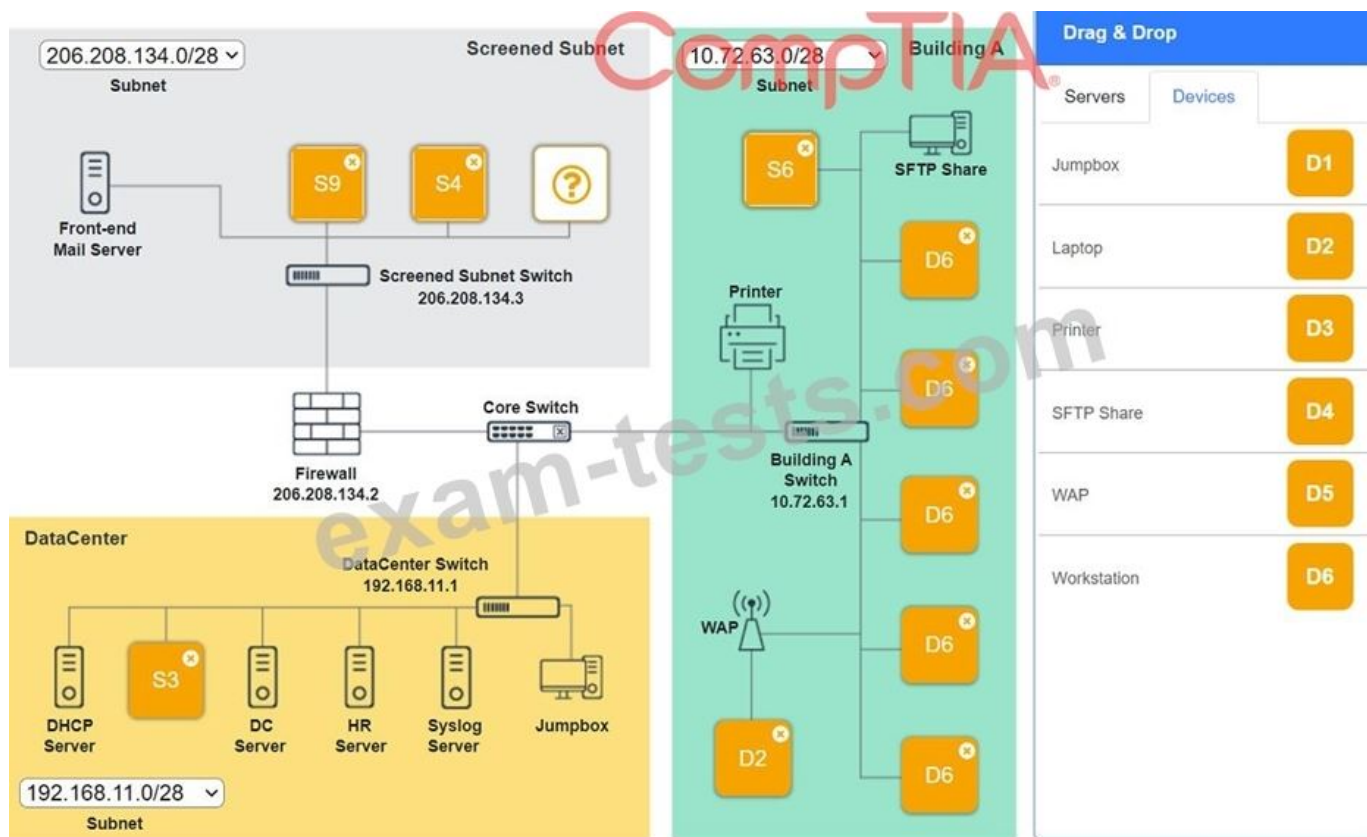
Building A devices - SSH server top left, workstations on all 5 on the right, laptop on bottom left DataCenter devices - DNS server.



Drag & Drop	
Servers	Devices
DC Server	
DHCP Server	
DNS Server	
FTP Server	
Mail Server	
SSH Server	
Syslog Server	
Telnet Server	
Web Server	



Drag & Drop	
Servers	Devices
DC Server	S1
DHCP Server	S2
DNS Server	S3
FTP Server	S4
Mail Server	S5
SSH Server	S6
Syslog Server	S7
Telnet Server	S8
Web Server	S9



NEW QUESTION: 644

A network administrator needs to query the NSs for a remote application. Which of the following commands would BEST help the administrator accomplish this task?

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

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 645

Which of the following can be used to centrally manage credentials for various types of administrative privileges on configured network devices?

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

Answer: (SHOW ANSWER)

NEW QUESTION: 646

A company is moving to a new building designed with a guest waiting area that has existing network ports. Which of the following practices would BEST secure the network?

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

Answer: (SHOW ANSWER)

One of the best practices to secure the network would be to disable unneeded switchports in the guest waiting area. This will prevent unauthorized users from connecting to the network through these ports. It's important to identify which switchports are not in use and disable them, as this will prevent unauthorized access to the network.

Other practices such as ensuring all guests sign an NDA, lowering the radio strength to reduce Wi-Fi coverage in the waiting area and enabling MAC filtering to block unknown hardware addresses are not as effective in securing the network as disabling unneeded switchports. Enforcing an NDA with guests may not stop a malicious user from attempting to access the network, reducing the radio strength only limits the Wi-Fi coverage, and MAC filtering can be easily bypassed by hackers.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 647

A network technician is installing an analog desk phone for a new receptionist. After running a new phone line, the technician now needs to crimp on a new connector. Which of the following connectors would MOST likely be used in this case?

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

Answer: B (LEAVE A REPLY)

Explanation

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

<https://www.comptia.org/blog/what-is-rj11>

NEW QUESTION: 648

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 ([LEAVE A REPLY](#))

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: 649

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: B ([LEAVE A REPLY](#))

The security principle of least privilege states that users or processes should only have the minimum level of access or permissions required to perform their tasks. This reduces the risk of unauthorized or malicious actions, as well as the impact of potential breaches. In this scenario, the systems operator is granted access to only the applications that are relevant to their role, and denied access to the applications that are not. This is an example of applying the least privilege principle. References:

* CompTIA Network+ N10-008 Certification Study Guide, Chapter 7: Network Security Concepts and Tools, Section 7.1: Common Security Concepts, Subsection: Least Privilege¹

* Professor Messer's CompTIA N10-008 Network+ Course, Section 7.1: Common Security Concepts, Video: Least Privilege²

NEW QUESTION: 650

A network administrator is installing a wireless network at a client's office. Which of the following IEEE 802.11 standards would be BEST to use for multiple simultaneous client access?

- A. CDMA
- B. CSMA/CD
- C. CSMA/CA

D. GSM

Answer: C (LEAVE A REPLY)

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is an IEEE 802.11 standard that would be best to use for multiple simultaneous client access on a wireless network. CSMA/CA is a media access control method that allows multiple devices to share the same wireless channel without causing collisions or interference. It works by having each device sense the channel before transmitting data and waiting for an acknowledgment from the receiver after each transmission. If the channel is busy or no acknowledgment is received, the device will back off and retry later with a random delay. References:

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-csma-ca.html>

NEW QUESTION: 651

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 (LEAVE A REPLY)

The OSI model is a conceptual framework that describes how data is transmitted and processed across a network. It consists of seven layers, each with a specific function and responsibility.

The application layer (layer 7) is the highest layer of the OSI model and interacts with the user applications and services. It provides the interface and functionality for the end-user communication.

The presentation layer (layer 6) is the layer below the application layer and receives data from it. It is responsible for converting the data into a common syntax and format that is readable by other devices on the network. It also handles encryption, compression, and translation of data.

The network layer (layer 3) is the layer that handles the routing and addressing of data packets across different networks. It uses logical addresses, such as IP addresses, to identify the source and destination of the data.

The physical layer (layer 1) is the lowest layer of the OSI model and deals with the transmission and reception of raw bits over the physical medium. It defines the electrical, mechanical, and procedural characteristics of the network devices and cables.

Therefore, the correct answer is C. Layer 6, as it is the layer that receives data from the application layer and converts it into syntax that is readable by other devices on the network. Reference:

[CompTIA Network+ N10-008 Study Guide], Chapter 1: Network Concepts, Section 1.1: Explain the OSI Reference Model, p. 13-18

[Professor Messer's CompTIA N10-008 Network+ Course Notes], Section 1.1: The OSI Model, p. 2-3 Free CompTIA N10-008 Exam Questions - Study4Exam, Question 420

NEW QUESTION: 652

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

- A. UDP
- B. ARP
- C. ICMP
- D. TCP

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 653

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: ([SHOW ANSWER](#))

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: 654

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: ([SHOW ANSWER](#))

Change management is the process of planning, implementing, and documenting changes to the network infrastructure, software, hardware, or configuration. It involves the following steps:

Requesting a change: A change request is a formal document that describes the proposed change, the reason for it, the expected benefits, the potential risks, and the estimated costs and resources.

Reviewing and approving a change: A change review board (CRB) or a change advisory board (CAB) is a group of stakeholders who evaluate the change request and decide whether to approve, reject, or modify it. The CRB or CAB may also prioritize the change request based on its urgency, impact, and feasibility.

Scheduling and implementing a change: A change schedule is a calendar that shows when the approved changes will be executed. A change window is a specific time slot allocated for performing the change, usually during off-peak hours or maintenance periods. A change rollback plan is a contingency plan that outlines how to restore the network to its previous state in case of failure or unexpected results.

Testing and validating a change: A change test plan is a set of procedures and criteria that verify the functionality, performance, and security of the network after the change. A change validation plan is a set of metrics and feedback mechanisms that measure the effectiveness and satisfaction of the change.

Documenting and communicating a change: A change log is a record of all the changes made to the network, including the date, time, description, status, and outcome of each change. A change notification is a message that informs the affected users, customers, and vendors about the change, its purpose, its impact, and its duration.

Change management is used to enforce and schedule critical updates with supervisory approval and include backup plans in case of failure because it ensures that the updates are aligned with the business objectives, comply with the security policies, minimize the disruption and downtime, and improve the network performance and reliability.

Reference:

[CompTIA Network+ N10-008 Certification Study Guide], Chapter 5: Network Operations, Section 5.2: Change Management, pp. 269-271

[Professor Messer's CompTIA N10-008 Network+ Course Notes], Section 5.2: Change Management, p. 68

[Professor Messer's CompTIA N10-008 Network+ Training Course], Video 5.2: Change Management, 12:31 minutes

NEW QUESTION: 655

An application is not working. When the log files are reviewed, the application continuously tries to reach the following destination:

Destination
::1/128

Which of the following is most likely associated with this IP address?

- A. APIPA
- B. Default gateway
- C. Link local
- D. Loopback

Answer: (SHOW ANSWER)

The IP address ::1/128 is the loopback address of the local host in IPv6, which is the equivalent of the 127.0.0.1 in IPv4. The loopback address is a virtual interface that loops all traffic back to itself, the local host. The loopback address is used for testing and troubleshooting purposes, such as checking the connectivity and configuration of the network stack. If an application tries to reach the loopback address, it means that it is not communicating with any external network or server, but only with itself.

The other options are not correct because they are not associated with the IP address ::1/128. They are:

- * APIPA. APIPA stands for Automatic Private IP Addressing, which is a feature that allows a device to assign itself a private IPv4 address in the range of 169.254.0.0/16 when no DHCP server is available.

APIPA does not apply to IPv6 addresses, and it is not related to the loopback address.

- * Default gateway. The default gateway is the IP address of the router or device that connects a local network to other networks. The default gateway is usually the first or last usable IP address in a subnet, and it is not the same as the loopback address.

- * Link local. Link local addresses are IPv6 addresses that are used for communication within a single network segment or link. Link local addresses have the prefix fe80::/10, and they are not routable or reachable from other networks. Link local addresses are not the same as the loopback address.

References1: Loopback Address - ::1/128 - ipUpTime.net2: Network+ (Plus) Certification | CompTIA IT

Certifications3: Reserved IP addresses - Wikipedia

NEW QUESTION: 656

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

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

Answer: (SHOW ANSWER)

Explanation

Stratum 1 devices are the most accurate ntp time sources accessible via a network connection. A Stratum 1 device would normally be synchronised via a Stratum 0 reference clock.

Reference: <https://endruntechnologies.com/products/ntp-time-servers/stratum1>

NEW QUESTION: 657

Which of the following would be BEST suited for a long cable run with a 40Gbps bandwidth?

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

Answer: (SHOW ANSWER)

Cat 7 is a type of twisted-pair copper cable that supports up to 40 Gbps bandwidth and up to 100 meters cable length. Cat 7 is suitable for long cable runs that require high-speed data transmission. Cat 7 has better shielding and crosstalk prevention than lower categories of cables.

References: Network+ Study Guide Objective 1.5: Compare and contrast network cabling types, features and their purposes.

NEW QUESTION: 658

Which of the following is the first step to troubleshoot a network issue?

- A. Establish a theory of probable cause.
- B. Document the findings.
- C. Identify the problem.
- D. Test the theory to determine the cause.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 659

A help desk technician discovers the following note while reviewing tickets in a customer's account:

`Was able to confirm customer's problem with the system. Will upgrade system to latest version and monitor for further connectivity problems per developer's instructions.`

Which of the following describes what the technician was documenting with this note?

- A. The technician was approaching multiple problems individually.
- B. The technician was establishing a plan of action and identifying potential effects.
- C. The technician was testing a theory to determine the cause.
- D. The technician was identifying the problem by gathering information.

Answer: D ([LEAVE A REPLY](#))

The technician was identifying the problem by gathering information with this note. This is the first step of the troubleshooting methodology, which is a systematic process of finding and resolving issues in a network or system. By gathering information, the technician can understand the symptoms, scope, and impact of the problem, as well as collect relevant data from various sources, such as users, logs, tools, or documentation.

The note shows that the technician was asking questions to the user, checking the network status and configuration, and reviewing previous tickets to gather information about the problem. References: [CompTIA Network+ Certification Exam Objectives], Troubleshooting Methodology - CompTIA Network+ N10-007 -

1.4 | Professor Messer IT Certification Training Courses

NEW QUESTION: 660

After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect take to troubleshoot the issue?

- A. Check to see if the end connections were wrapped in copper tape before terminating.
- B. Use passthrough modular crimping plugs instead of traditional crimping plugs.
- C. Connect the RX/TX wires to different pins.
- D. Run a speed test on a device that can only achieve 100Mbps speeds.

Answer: A ([LEAVE A REPLY](#))

Cat 8 keystones are shielded to prevent interference from external sources, but they also require proper grounding to avoid interference from within the cable. Wrapping the end connections with copper tape before terminating them is one way to ensure a good ground connection and reduce interference. Using passthrough modular crimping plugs, connecting the RX/TX wires to different pins, or running a speed test on a slow device are not relevant or effective steps to troubleshoot the issue.

Reference:

CompTIA Network+ N10-008 Certification Study Guide, page 191

CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 362

CAT8 RJ45 Keystone Problem : r/HomeNetworking2

How to Terminate Cat8 Shielded Keystone Jacks3

NEW QUESTION: 661

A network administrator is talking to different vendors about acquiring technology to support a new project for a large company. Which of the following documents will MOST likely need to be signed before information about the project is shared?

A. BYOD policy

B. NDA

C. SLA

D. MOU

Answer: B (LEAVE A REPLY)

Explanation

NDA stands for Non-Disclosure Agreement, which is a legal contract between two or more parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to by others. A network administrator may need to sign an NDA before sharing information about a new project with different vendors, as the project may involve sensitive or proprietary data that the company wants to protect from competitors or unauthorized use. References:

<https://www.adobe.com/sign/esignature-resources/sign-nda.html>

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 662

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

A. Packet shaping

B. Quality of service

- C. Port mirroring
- D. Load balancing

Answer: B ([LEAVE A REPLY](#))

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

NEW QUESTION: 663

Which of the following is used to ensure traffic flows efficiently on multiple T-1 circuits?

- A. DNS server
- B. Proxy server
- C. Content filter
- D. Load balancer

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 664

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 665

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. Audit log
- C. Trap
- D. Syslog

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 666

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

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 667

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

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

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

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

Answer: C ([LEAVE A REPLY](#))

Explanation

The IP address configured on the router interface is 196.26.4.1/26, which belongs to the IP range assigned by the ISP (196.26.4.0/26). However, this IP address is not valid for this interface because it is the network address of the subnet, which cannot be assigned to any host device. The network address is the first address of a subnet that identifies the subnet itself. The valid IP addresses for this subnet are from 196.26.4.1 to 196.26.4.62, excluding the network address (196.26.4.0) and the broadcast address (196.26.4.63). The router interface should be configured with a valid IP address within this range to restore Internet connectivity for all users. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

<https://www.techopedia.com/definition/24136/network-address>

NEW QUESTION: 668

A company's web server is hosted at a local ISP. This is an example of:

- A. colocation.
- B. an on-premises data center.

- C. a branch office.
- D. a cloud provider.

Answer: ([SHOW ANSWER](#))

Co-location refers to the way IT equipment and resources are located or installed. This usually refers to the networking hardware resources owned by an organization, such as Web or database servers, which are located outside the vicinity of the organization's premises and "co-located" with another organization's hardware, usually an ISP or a service provider. This is usually done because the ISP might be the best candidate for maintaining the Web server hardware for the organization and it would be better to keep the hardware in a more suitable place since ISPs have specially built places for networking hardware.

NEW QUESTION: 669

A network engineer installed a new fiber uplink for an office and wants to make sure that the link meets throughput requirements. Which of the following tools should the engineer use to verify that the new link is sufficient?

- A. tcpdump
- B. netstat
- C. ping
- D. iperf

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 670

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: ([SHOW ANSWER](#))

OSPF (Open Shortest Path First) is a link-state routing protocol that is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links¹². OSPF uses the Dijkstra algorithm to calculate the shortest path to each destination based on link cost, which can be influenced by bandwidth, delay, reliability, and load¹². OSPF also supports hierarchical routing, which divides the network into areas and reduces the amount of routing information exchanged and processed¹².

RIPv2 (Routing Information Protocol version 2) is a distance-vector routing protocol that is mainly used in small to medium-sized networks with simple topologies and low bandwidth requirements¹². RIPv2 uses hop count as the metric to determine the best path to each destination, and has a maximum hop count of 15, which limits its scalability¹². RIPv2 also suffers from slow convergence, routing loops, and high bandwidth consumption due to periodic updates¹².

QoS (Quality of Service) is not a routing protocol, but a set of techniques and mechanisms that prioritize and manage network traffic according to different parameters, such as bandwidth, delay, jitter, packet loss, and application type¹³. QoS can enhance the performance and reliability of network services, especially for real-time

and interactive applications, such as voice and video¹³. QoS can be implemented at different layers of the network, such as the application, transport, network, and data link layers¹³.

STP (Spanning Tree Protocol) is not a routing protocol, but a network protocol that prevents loops and ensures redundancy in switched networks by creating a logical tree topology and blocking or enabling links based on their role and state¹. STP can also dynamically adjust to network changes, such as link failures or additions, by recalculating the tree and switching the link states accordingly¹. STP operates at the data link layer and uses bridge protocol data units (BPDUs) to exchange information among switches¹.

Reference:

1: CompTIA Network+ N10-008 Study Guide, Chapter 3: Routing and Switching

2: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 32: Routing Protocols

3: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 36: Quality of Service

4: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 38: Spanning Tree Protocol

NEW QUESTION: 671

A company cell phone was stolen from a technician's vehicle. The cell phone has a passcode, but it contains sensitive information about clients and vendors. Which of the following should also be enabled?

- A. Two-factor authentication
- B. Factory reset
- C. Autolock
- D. Encryption

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 672

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 673

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: ([SHOW ANSWER](#))

- * Jumbo frames are Ethernet frames that have a payload size larger than the standard 1500 bytes. They can range from 1501 to 9000 bytes, depending on the network device and configuration.
- * Jumbo frames can reduce the overhead of file transfers by decreasing the number of frames that need to be sent and received, as well as the number of headers and checksums that need to be processed.
- * Jumbo frames can also improve the throughput and efficiency of the network, as they reduce the fragmentation and reassembly of packets, and the CPU utilization of the network devices.
- * However, jumbo frames also have some drawbacks, such as increased latency, higher memory requirements, and compatibility issues with some network devices and applications. Therefore, they should be used with caution and only when the network supports them.
- * To enable jumbo frames, both the sender and the receiver, as well as all the intermediate devices (such as switches and routers) along the path, must support and be configured with the same maximum transmission unit (MTU) size. Otherwise, the frames will be dropped or fragmented, resulting in poor performance or errors.
- * The other options are not relevant to reducing the overhead of file transfers:
- * Link aggregation is a technique of combining multiple physical links into a logical link, to increase the bandwidth and redundancy of the network. It does not affect the frame size or the overhead of file transfers.
- * Port security is a feature that restricts the access to a switch port based on the MAC address of the device connected to it. It prevents unauthorized devices from accessing the network, but it does not reduce the overhead of file transfers.
- * Flow control is a mechanism that regulates the rate of data transmission between two devices, to avoid congestion and data loss. It can be implemented at the data link layer (using pause frames) or the transport layer (using TCP windowing). It does not reduce the overhead of file transfers, but rather adapts to the network conditions.
- * Lower FTP port is not a valid configuration change, as FTP uses well-defined ports for its operation. FTP uses port 21 for control connections and port 20 for data connections, or a random port above 1024 for passive mode. Changing the FTP port would not reduce the overhead of file transfers, but rather cause connection problems or security risks. References:
- * CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Devices and Technologies, Section 2.3: Configure Switches, p. 97-98
- * Professor Messer's Network+ N10-008 Course Notes, Section 2.3: Switch Configuration, p. 22
- * Professor Messer's Network+ N10-008 Video Training Course, 2.3 Switch Configuration - Part 2

NEW QUESTION: 674

Which of the following is associated with the session layer of the OSI model?

- A. Data representation
- B. Packets
- C. Sockets
- D. Frames

Answer: (SHOW ANSWER)

The session layer of the OSI model, which is Layer 5, is responsible for establishing, managing, and terminating connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogs between the applications at each end. It handles sessions using service points, which are

called "sockets." Therefore, sockets are closely associated with the session layer as they provide the endpoint for communication sessions between client-server applications. Other options such as data representation, packets, and frames are associated with other OSI layers (presentation, network, and data link, respectively).

NEW QUESTION: 675

A company upgrades its network and PCs to gigabit speeds. After the upgrade, users are not getting the expected performance.

Technicians discover that the speeds of the endpoint NICs are inconsistent. Which of the following should be checked first to troubleshoot the issue?

- A.** Speed mismatches
- B.** Load balancer settings
- C.** Devices' duplex settings
- D.** Office wiring category

Answer: C ([LEAVE A REPLY](#))

Explanation

Duplex settings determine how data is transmitted and received over a network. If the devices have inconsistent duplex settings, such as half-duplex and full-duplex, they may experience performance issues, collisions, and errors. To troubleshoot the issue, the technicians should check the devices' duplex settings and make sure they match the network's configuration.

References:

Gigabit Ethernet does not work - Microsoft Community¹

Network Tests: Are We Getting Gigabit Performance? - Tom's Hardware²

CompTIA Network+ N10-008 Exam Objectives

<https://www.comptia.org/certifications/network#examdetails>

NEW QUESTION: 676

Which of the following is used to provide disaster recovery capabilities to spin up an critical devices using internet resources?

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

Answer: ([SHOW ANSWER](#)**)**

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com

N10-008 dumps with Test Engine here: <https://www.braindumps.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 677

A new company recently moved into an empty office space. Within days, users in the new office began noticing increased latency and packet drops with their Wi-Fi-connected devices. Which of the following is the MOST likely reason for this issue?

- A. Channel overlap
- B. Distance from the AP
- C. Bandwidth latency
- D. RF attenuation
- E. Network congestion

Answer: A (LEAVE A REPLY)

* Channel overlap occurs when two or more wireless access points (APs) use the same or adjacent frequency channels within the same area¹². This can cause interference and degradation of the wireless signal quality, resulting in increased latency and packet drops for the Wi-Fi-connected devices¹².

* Channel overlap is one of the most common causes of Wi-Fi performance issues, especially in densely populated areas where there are many wireless networks operating in the same spectrum¹². The 2.4 GHz band, which is widely used by Wi-Fi devices, has only three non-overlapping channels (1, 6, and 11) in most regions, making it more prone to channel overlap than the 5 GHz band, which has more non-overlapping channels available¹².

* To fix channel overlap, network administrators should perform a site survey to identify the existing wireless networks and their channel usage, and then configure their APs to use the least congested or non-overlapping channels¹². Alternatively, they can use APs that support automatic channel selection, which can dynamically adjust the channel based on the network conditions¹².

* The other options are not the most likely reasons for the issue. Distance from the AP can affect the signal strength and quality, but it does not explain why the issue occurred only after the new company moved in³. Bandwidth latency is a measure of the delay in data transmission, which can be affected by various factors such as network congestion, routing, or quality of service, but it is not a cause of the issue itself⁴. RF attenuation is the loss of signal power due to distance, obstacles, or interference, which can also affect the Wi-Fi performance, but it is not specific to the scenario described in the question⁵. Network congestion is the state of high demand and low availability of network resources, which can cause latency and packet loss, but it is not necessarily related to channel overlap⁶. References:

* 1: CompTIA Network+ N10-008 Certification Study Guide, Chapter 4: Wireless Networks, Section 4.4: Wireless Network Troubleshooting⁷

* 2: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 25: Wireless Troubleshooting⁸

* 3: CompTIA Network+ N10-008 Certification Study Guide, Chapter 4: Wireless Networks, Section 4.2: Wireless Network Implementations⁷

* 4: CompTIA Network+ N10-008 Certification Study Guide, Chapter 2: Network Protocols and Services, Section 2.5: Bandwidth and Latency⁷

* 5: CompTIA Network+ N10-008 Certification Study Guide, Chapter 4: Wireless Networks, Section 4.1:

Wireless Network Fundamentals7

* 6: CompTIA Network+ N10-008 Certification Study Guide, Chapter 3: Routing, Section 3.5: Network Congestion7

* 7: CompTIA Network+ N10-008 Certification Study Guide2

* 8: Professor Messer's CompTIA Network+ N10-008 Training Course5

NEW QUESTION: 678

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 (LEAVE A REPLY)

* A warm site is a backup data center that has some network equipment and connectivity, but not enough to handle the full load of the primary site. It requires some time and effort to activate and configure in the event of a disaster12.

* An active-active site is a backup data center that is fully operational and synchronized with the primary site, and can take over the load immediately if the primary site fails. It is the most expensive and complex option12.

* A cold site is a backup data center that has no network equipment or connectivity, and only provides physical space and power. It requires a lot of time and resources to set up and activate in the event of a disaster. It is the cheapest and simplest option12.

* A cloud site is a backup data center that is hosted by a third-party provider, and can offer various levels of availability and scalability depending on the service level agreement. It can be a cost-effective and flexible option, but also introduces some challenges such as security, compliance, and vendor lock-in13.

References:

* 1: CompTIA Network+ N10-008 Study Guide, Chapter 6: Network Resiliency and Availability, Section: Disaster Recovery

* 2: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 54: Disaster Recovery Sites

* 3: Backup Strategy: Ultimate Guide for Data Backup

NEW QUESTION: 679

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 (LEAVE A REPLY)

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: 680

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

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

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 681

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 (LEAVE A REPLY)

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: 682

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: [\(SHOW ANSWER\)](#)

The end user can access local network shares and intranet pages, which means that the IP address and the subnet mask are configured correctly and the network interface is working properly.

However, the end user is unable to access the internet or remote resources, which means that there is a problem with the name resolution or the routing of the traffic.

The gateway address is responsible for routing the traffic to the destination network, which could be on the internet or another subnet. If the gateway address is incorrect, the end user would not be able to reach any network outside the local subnet.

The DNS servers are responsible for resolving the domain names to the IP addresses, which are needed to communicate with the internet or remote resources. If the DNS servers are incorrect, the end user would not be able to resolve the names of the websites or servers they want to access.

Therefore, the most likely cause of the connectivity issue is that the DNS servers need to be reconfigured with the correct addresses. Reference:

CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Protocols and Services, Section 2.2: TCP/IP Suite, p. 76-77 Network+ N10-008 Practice Test, Question 359 CompTIA Network+ (N10-008) Performance-based Questions (PBQs), Part 1, 1:36

NEW QUESTION: 683

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 \(LEAVE A REPLY\)](#)

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: 684

Which of the following ports is commonly used by VoIP phones?

- A. 20

- B. 143
- C. 445
- D. 5060

Answer: D (LEAVE A REPLY)

TCP/UDP port 5060 is commonly used by VoIP phones. It is the default port for SIP (Session Initiation Protocol), which is a signaling protocol that establishes, modifies, and terminates multimedia sessions over IP networks. SIP is widely used for VoIP applications such as voice and video calls. Reference: <https://www.voip-info.org/session-initiation-protocol/>

NEW QUESTION: 685

At which of the following OSI model layers does routing occur?

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

Answer: D (LEAVE A REPLY)

Routing is the process of forwarding packets from one network to another, based on the destination IP address¹. Routing occurs at the network layer of the OSI model, which is the third layer from the bottom².

The network layer is responsible for logical addressing, path selection, and packet delivery across multiple networks².

Routers are the devices that operate at the network layer and perform routing functions, using protocols such as RIP, OSPF, EIGRP, or BGP³.

The other layers of the OSI model have different roles in the network communication process, such as:

The data link layer is the second layer from the bottom, and it is responsible for framing, addressing, and error detection of data packets over a single network, using protocols such as Ethernet, Wi-Fi, or PPP².

The transport layer is the fourth layer from the bottom, and it is responsible for ensuring reliable, error-free, and ordered data transfer between devices, using protocols such as TCP or UDP².

The physical layer is the bottom layer, and it is responsible for transmitting and receiving bits over a physical medium, such as a cable, a fiber, or a wireless signal². Reference:

1: CompTIA Network+ N10-008 Cert Guide, 1st Edition, Chapter 5: Routing, p. 179

2: CompTIA Network+ N10-008 Cert Guide, 1st Edition, Chapter 1: Introduction to Networks, pp. 22-29

3: CompTIA Network+ N10-008 Cert Guide, 1st Edition, Chapter 5: Routing, pp. 180-191

NEW QUESTION: 686

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

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 687

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

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

Answer: C (LEAVE A REPLY)

Explanation

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

<https://www.comptia.org/blog/what-is-port-tagging>

NEW QUESTION: 688

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 (LEAVE A REPLY)

The structure of the management data of a device subsystem using a hierarchical namespace containing object identifiers

NEW QUESTION: 689

A network technician is performing tests on a potentially faulty network card that is installed in a server. Which of the following addresses will MOST likely be used during traffic diagnostic tests?

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

Answer: B (LEAVE A REPLY)

127.0.0.1 is the loopback address, it is used to test the functionality of a network card by sending traffic to the card and then verifying that it is received properly. This address is used because it is guaranteed to always point

to the local host, regardless of the network configuration. The IP address range for loopback addresses is 127.0.0.0/8.

NEW QUESTION: 690

While waking from the parking lot to 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. Piggybacking
- C. Shoulder surfing
- D. Phishing

Answer: A (LEAVE A REPLY)

The difference between piggybacking and tailgating 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: 691

A technician is troubleshooting intermittent connectivity between devices and viewing the following syslog entries from a switch:

```
21 Feb 2022 16:02:0231 NOTIFICATION %LINK-I-DOWN: G1/10
21 Feb 2022 16:02:0262 NOTIFICATION %LINK-I-UP: G1/10
21 Feb 2022 16:03:5321 NOTIFICATION %LINK-I-DOWN: G1/10
21 Feb 2022 16:03:7873 NOTIFICATION %LINK-I-UP: G1/10
```

Which of the following are these entries indicative of?

- A. DDoS attack
- B. Jitter
- C. Latency
- D. Link flapping

Answer: ([SHOW ANSWER](#))

The syslog entries are indicative of link flapping, which is when a switch port rapidly transitions between the up and down states. This can cause intermittent connectivity issues, network instability, and increased CPU utilization on the switch. Link flapping can be caused by various factors, such as faulty cables, misconfigured interfaces, duplex mismatches, or network attacks. To troubleshoot link flapping, the technician should check the physical layer, verify the interface settings, and monitor the network traffic for anomalies.

References:

- * What is Link Flapping? - CompTIA1
- * Troubleshooting Switch Port and Interface Problems - Cisco2
- * Network Troubleshooting - N10-008 CompTIA Network+ : 4.1 - YouTube3

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 692

Which of the following does OSPF use to communicate routing updates?

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 693

Which of the following would MOST likely utilize PoE?

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

Answer: A ([LEAVE A REPLY](#))

A camera is most likely to utilize PoE (Power over Ethernet). PoE is a technology that allows electrical power to be delivered over Ethernet cables. It is used to power a variety of devices, such as cameras, phones, access points, and other networking equipment. Cameras are particularly well-suited for PoE because they are often

installed in locations where it is difficult or impossible to run electrical power. By using PoE, cameras can be powered directly over the Ethernet cable, eliminating the need for separate power cables and outlets. Other devices, such as printers, hubs, and modems, are less likely to utilize PoE because they typically do not need to be powered over Ethernet. These devices are usually powered by AC (alternating current) power and are typically connected to a power outlet rather than an Ethernet cable.

NEW QUESTION: 694

An organization with one core and five distribution switches is transitioning from a star to a full-mesh topology. Which of the following is the number of additional network connections needed?

- A. 5
- B. 7
- C. 10
- D. 15

Answer: (SHOW ANSWER)

10 additional network connections are needed to transition from a star to a full-mesh topology. A star topology is a network topology where each device is connected to a central device, such as a switch or a hub. A full-mesh topology is a network topology where each device is directly connected to every other device. The number of connections needed for a full-mesh topology can be calculated by the formula $n(n-1)/2$, where n is the number of devices. In this case, there are six devices (one core and five distribution switches), so the number of connections needed for a full-mesh topology is $6(6-1)/2 = 15$. Since there are already five connections in the star topology (one from each distribution switch to the core switch), the number of additional connections needed is $15 - 5 = 10$.

References:

<https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION: 695

A network security engineer locates an unapproved wireless bridge connected to the corporate LAN that is broadcasting a hidden SSID, providing unauthenticated access to internal resources. Which of the following types of attacks BEST describes this finding?

- A. Rogue access point Most Voted
- B. Evil twin
- C. ARP spoofing
- D. VLAN hopping

Answer: A (LEAVE A REPLY)

Explanation

A rogue access point is an illegitimate access point plugged into a network to create a bypass from outside into the legitimate network. By contrast, an evil twin is a copy of a legitimate access point.

NEW QUESTION: 696

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: ([SHOW ANSWER](#))

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: 697

A customer is having issues accessing local resources on the network. A technician questions the user and discovers that a small switch had been taken out of storage and installed so that additional devices could be connected in the room. The technician runs the ping command from the PC to the network server and does not find any issues. However, data transfers to the server are slow, and the transfer appears to be locked up at times. Which of the following is the most likely cause of the issue?

- A. Cable crosstalk
- B. Duplexing mismatch
- C. Reversed TX/RX pinouts
- D. Failed transceiver

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 698

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

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

Answer: ([SHOW ANSWER](#))

Bandwidth management is the process of measuring and controlling the communications (traffic, packets) on a network link, to avoid filling the link to capacity or overfilling the link, which would result in network congestion and poor performance of the network.

NEW QUESTION: 699

An engineer is using a tool to run an ICMP sweep of a network to find devices that are online.

When reviewing the results, the engineer notices a number of workstations that are currently verified as being online are not listed in the report.

The tool was configured to scan using the following information:

- Network address: 172.28.16.0
- CIDR: /22

The engineer collected the following information from the client workstation:

- IP address: 172.28.17.206
- Subnet mask: 255.255.252.0

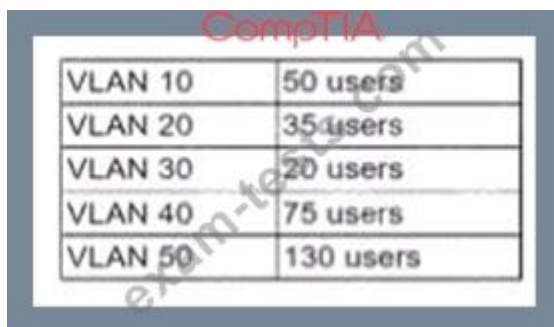
Which of the following MOST likely explains why the tool is failing to detect some workstations?

- A. The scanned network range is incorrect.
- B. The tool is unable to scan remote networks.
- C. The workstation has a firewall enabled.
- D. The subnet mask on the client is misconfigured.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 700

A network engineer needs to create a subnet that has the capacity for five VLANs. with the following number of clients to be allowed on each:



VLAN 10	50 users
VLAN 20	35 users
VLAN 30	20 users
VLAN 40	75 users
VLAN 50	130 users

Which of the following is the SMALLEST subnet capable of this setup that also has the capacity to double the number of clients in the future?

- A. 10.0.0.0/21
- B. 10.0.0.0/22
- C. 10.0.0.0/23
- D. 10.0.0.0/24

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 701

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

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

Answer: A ([LEAVE A REPLY](#))

Explanation

The valid alternative to maintain a deployed proxy technology while saving physical space in the data center by moving the network service to the virtualization infrastructure is NFV (Network Function Virtualization).

NFV is a technique that allows network functions, such as proxies, firewalls, routers, or load balancers, to be implemented as software applications running on virtual machines or containers. NFV reduces the need for dedicated hardware devices and improves scalability and flexibility of network services. References: CompTIA

Network+ N10-008 Certification Study Guide, page 440; The Official CompTIA Network+ Student Guide (Exam N10-008), page 16-11.

NFV can be used to virtualize a wide variety of network functions, including proxy servers. By virtualizing proxy servers, organizations can save physical space in the data center and improve the scalability and efficiency of their networks.

To virtualize a proxy server using NFV, an organization would need to deploy a virtualization platform, such as VMware ESXi or Microsoft Hyper-V. The organization would then need to install a virtual proxy server appliance on the virtualization platform.

Once the virtual proxy server appliance is installed, it can be configured and used just like a physical proxy server.

NFV is a relatively new technology, but it is quickly gaining popularity as organizations look for ways to improve the efficiency and scalability of their networks.

NEW QUESTION: 702

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 703

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

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 704

A business is using the local cable company to provide Internet access. Which of the following types of cabling will the cable company MOST likely use from the demarcation point back to the central office?

- A. 100BASE-T
- B. Multimode
- C. RG-6
- D. Cat 6
- E. Cat 5e

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 705

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

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

Answer: ([SHOW ANSWER](#)**)**

GDPR stands for General Data Protection Regulation, which is a European Union regulation on information privacy and security. It applies to any organization that collects or processes personal data of individuals in the EU, and it sets out rules and requirements for data protection, consent, breach notification, and enforcement¹

Reference

1: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

NEW QUESTION: 706

Which of the following needs to be tested to achieve a Cat 6a certification for a company's data cabling?

- A. Patch panel
- B. LC ports
- C. F-type connector
- D. RJ11

Answer: ([SHOW ANSWER](#)**)**

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 707

Which of the following is the best way to remotely monitor who is accessing a secure data center?

- A. Access control vestibule
- B. Cameras
- C. Employee training

D. Biometrics

Answer: B (LEAVE A REPLY)

Cameras are the best tool for remotely monitoring who is accessing a secure data center. They provide real-time visual verification of individuals entering and exiting the facility and can be monitored remotely to ensure security protocols are followed. Access control vestibules, employee training, and biometrics are also important for security but do not offer the same continuous, visual monitoring capability that cameras do. Cameras also serve as a deterrent to unauthorized access and can provide forensic evidence in the event of a security breach.

NEW QUESTION: 708

Which of the following would be used to adjust resources dynamically for a virtual web server under variable loads?

- A. Elastic computing**
- B. Scalable networking**
- C. Hybrid deployment**
- D. Multitenant hosting**

Answer: B (LEAVE A REPLY)

Explanation

A technique used to adjust resources dynamically for a virtual web server under variable loads is called auto-scaling. Auto-scaling automatically increases or decreases the number of instances of a virtual web server in response to changes in demand, ensuring that the right amount of resources are available to handle incoming traffic. This can help to improve the availability and performance of a web application, as well as reduce costs by avoiding the need to provision and maintain excess capacity.

NEW QUESTION: 709

Which of the following common agreements would a company most likely have an employee sign as a condition of employment?

- A. NDA**
- B. ISP**
- C. SLA**
- D. MOU**

Answer: A (LEAVE A REPLY)

Explanation

An NDA, or non-disclosure agreement, is a legal contract that binds an employee to keep certain information confidential and not share it with unauthorized parties. This information may include trade secrets, intellectual property, business strategies, customer data, or other sensitive or proprietary information that gives the company a competitive advantage. An NDA protects the company's interests and prevents the employee from disclosing or using the information for personal gain or malicious purposes¹.

References¹ - 10 Types of Employment Contracts | Indeed.com

NEW QUESTION: 710

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

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

Answer: A (LEAVE A REPLY)

A VLAN (Virtual Local Area Network) is a logical grouping of devices that share the same broadcast domain, regardless of their physical location or connection. VLANs can improve network performance, security, and management by separating different types of traffic, such as data, voice, and video¹.

A VoIP (Voice over Internet Protocol) phone is a device that uses the Internet to transmit voice calls, instead of the traditional phone lines. VoIP phones require a network connection, an IP address, and a gateway to communicate with other VoIP devices or phone systems².

A DHCP (Dynamic Host Configuration Protocol) server is a device that automatically assigns IP addresses and other network configuration parameters to devices that request them. DHCP simplifies network administration and avoids IP conflicts³.

A switchport is a physical interface on a switch that connects to a network device, such as a VoIP phone, a computer, or another switch. A switchport can be configured to belong to a specific VLAN or to carry traffic from multiple VLANs⁴.

A gateway is a device that connects different networks and enables communication between them. A gateway can also perform protocol conversion, such as translating between VoIP and analog signals⁵.

A route is a path that a packet takes to reach its destination. A route consists of a destination network, a next-hop device, and a metric. A router is a device that forwards packets based on their destination IP addresses and the routing table.

In order to allow a newly installed VoIP phone to operate correctly, the network administrator needs to assign the phone's switchport to the correct VLAN. This will ensure that the phone can communicate with the DHCP server and obtain an IP address that belongs to the same network as the phone system. This will also isolate the voice traffic from the data traffic and improve the quality of service.

Statically assigning the phone's gateway address is not enough to allow the phone to operate correctly, as the phone still needs an IP address and a subnet mask to communicate with other devices on the network. Moreover, statically assigning network parameters can be tedious and prone to errors, especially for a large number of devices.

Configuring a route on the VoIP network router is not necessary to allow the phone to operate correctly, as the phone and the phone system are on the same network and do not need to cross any routers. Configuring a route would only be needed if the phone and the phone system were on different networks and needed to communicate through a router.

Implementing a VoIP gateway is not required to allow the phone to operate correctly, as the phone and the phone system are both VoIP devices and use the same protocol. Implementing a VoIP gateway would only be needed if the phone or the phone system needed to communicate with a non-VoIP device or system, such as a traditional phone line or a public switched telephone network (PSTN).

Reference:

1: VLAN

2: VoIP Phone

- 3: DHCP
- 4: Switchport
- 5: Gateway
- 6: [Route]
- 7: [VoIP VLAN Configuration]
- 8: [Static vs Dynamic IP Addressing]
- 9: [Routing Basics]
- 10: [VoIP Gateway]

NEW QUESTION: 711

Which of the following OSI model layers contains IP headers?

- A. Presentation
- B. Data link
- C. Transport
- D. Application
- E. Network

Answer: E ([LEAVE A REPLY](#))

NEW QUESTION: 712

A network administrator is setting up several IoT 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 ([LEAVE A REPLY](#))

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 IoT 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. Reference: <https://www.comptia.org/blog/what-is-dhcp>

NEW QUESTION: 713

A network technician is investigating a trouble ticket for a user who does not have network connectivity. All patch cables between the wall jacks and computers in the building were upgraded over the weekend from Cat 5 to Cat 6. The newly installed cable is crimped with a TIA/EIA 568A on one end and a TIA/EIA 568B on the other end.

Which of the following should the technician do to MOST likely fix the issue?

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

Answer: B (LEAVE A REPLY)

Explanation

A straight-through cable is a type of twisted pair cable that has the same wiring standard (TIA/EIA 568A or 568B) on both ends. This is the most common type of cable used for connecting devices of different types, such as a computer and a switch. A cable that has different wiring standards on each end (TIA/EIA 568A on one end and 568B on the other) is called a crossover cable, which is used for connecting devices of the same type, such as two computers or two switches. Therefore, the technician should crimp the cable as a straight-through cable to fix the issue.

NEW QUESTION: 714

A network field technician is installing and configuring a secure wireless network. The technician performs a site survey. Which of the following documents would MOST likely be created as a result of the site survey?

- A. Physical diagram
- B. Heat map
- C. Asset list
- D. Device map

Answer: B (LEAVE A REPLY)

A heat map would most likely be created as a result of the site survey. A heat map is a graphical representation of the wireless signal strength and coverage in a given area. It can show the location of APs, antennas, walls, obstacles, interference sources, and dead zones. It can help with planning, optimizing, and troubleshooting wireless networks. References: <https://www.netspotapp.com/what-is-a-wifi-heatmap.html>

NEW QUESTION: 715

Which of the following is a valid and cost-effective solution to connect a fiber cable into a network switch without available SFP ports?

- A. Change the type of connector from SC to F-type
- B. Use a media converter and a UTP cable
- C. Install an additional transceiver module and use GBICs
- D. Use a loopback adapter to make the connection

Answer: B (LEAVE A REPLY)

NEW QUESTION: 716

Which of the following policies is MOST commonly used for guest captive portals?

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

Answer: (SHOW ANSWER)

Explanation

AUP stands for Acceptable Use Policy, which is a policy that defines the rules and guidelines for using a network or service. A guest captive portal is a web page that requires users to agree to the AUP before accessing the Internet or other network resources. This is a common way to enforce security and legal compliance for guest users. References:

https://www.arubanetworks.com/techdocs/Instant_87_WebHelp/Content/instant-ug/captive-portal/captive-portal

NEW QUESTION: 717

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

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

Answer: (SHOW ANSWER)

Reference:

<https://www.namecheap.com/support/knowledgebase/article.aspx/9604/2237/types-of-domain-redirects-301-302>

NEW QUESTION: 718

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

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

Answer: D (LEAVE A REPLY)

Traceroute is a network diagnostic tool that allows you to trace the path that network packets take from one device to another. By running traceroute to the file server, the technician can see the sequence of devices and networks that the packets pass through on their way to the file server.

This can help the technician to determine if there is a problem with the network connection between the user's computer and the file server, or if the issue is with the file server itself.

NEW QUESTION: 719

Which of the following cable types is MOST commonly used with POTS?

- A. Coaxial
- B. Multimode
- C. CAT6
- D. CAT3

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 720

An IT administrator is creating an alias to the primary customer's domain. Which of the following DNS record types does this represent?

- A. CNAME
- B. MX
- C. A
- D. PTR

Answer: A ([LEAVE A REPLY](#))

A CNAME record is a type of DNS record that maps an alias name to a canonical name, or the primary domain name. A CNAME record is used to create subdomains or alternative names for the same website, without having to specify the IP address for each alias. For example, a CNAME record can map [www.example.com](#) to [example.com](#), or [mail.example.com](#) to [example.com](#). References: CompTIA Network+ N10-008 Cert Guide, Chapter 2, Section 2.4

NEW QUESTION: 721

Which of the following should be used to associate an IPv6 address with a domain name?

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

Answer: ([SHOW ANSWER](#))

Explanation

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

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 722

A user is unable to reach any resources on the internet. A technician goes to the site and obtains the following output from the workstation:

Network Destination	Netmask	Gateway	Interface	Metric
10.10.51.0	255.255.255.0	On-Link	10.10.51.147	291
10.10.51.147	255.255.255.255	On-Link	10.10.51.147	291
10.10.51.255	255.255.255.255	On-Link	10.10.51.147	297
127.0.0.0	255.0.0.0	On-Link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-Link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-Link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-Link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-Link	10.10.51.147	291
255.255.255.255	255.255.255.255	On-Link	127.0.0.1	331
255.255.255.255	255.255.255.255	On-Link	10.10.51.147	291

Which of the following commands should the technician use to correct the issue?

- A. route ADD 0.0.0.0 MASK 0.0.0.0 10.10.51.10 metric 35
- B. route CHANGE 10.10.51.0 MASK 255.255.255.255 10.10.52.1 metric 5
- C. route DELETE 127.255.255.255
- D. route CHANGE 10.10.51.255 MASK 255.0.0.0 On-Link metric 1

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 723

After a company installed a new IPS, the network is experiencing speed degradation. A network administrator is troubleshooting the issue and runs a speed test. The results from the different network locations are as follows:

Which of the following is the most likely issue?

- A. Packet loss
- B. Bottlenecking
- C. Channel overlap
- D. Network congestion

Answer: (SHOW ANSWER)

The most likely issue is bottlenecking. Bottlenecking occurs when a component or device limits the performance or capacity of the network. In this case, the IPS (intrusion prevention system) may be causing a bottleneck by inspecting and filtering the incoming and outgoing traffic, which reduces the speed and bandwidth available for the network devices¹² To confirm this issue, the network administrator can compare the speed test results before and after installing the IPS, and check the IPS configuration and logs for any errors or warnings. The network administrator can also try to bypass the IPS temporarily and run the speed test again to see if there is any improvement³ If the IPS is indeed the cause of the bottleneck, the network administrator can try to optimize the IPS settings, such as adjusting the inspection rules, thresholds, and priorities, to reduce the processing overhead and latency. Alternatively, the network administrator can upgrade the IPS hardware or software, or add more IPS devices to balance the load and increase the throughput⁴⁵

1: What is Network Congestion? Common Causes and How to Fix Them? - GeeksforGeeks 2: Network congestion - Wikipedia 3: How to Fix Packet Loss - Lifewire 4: How to Optimize Your IPS Performance - Cisco 5: How to Avoid Network Bottlenecks - TechRepublic

NEW QUESTION: 724

A customer connects a firewall to an ISP router that translates traffic destined for the internet. The customer can connect to the internet but not to the remote site. Which of the following will verify the status of NAT?

- A. tcpdump
- B. nmap
- C. ipconfig
- D. tracert

Answer: A ([LEAVE A REPLY](#))

tcpdump is a command-line tool that can capture and analyze network traffic on a given interface. tcpdump can verify the status of NAT by showing the source and destination IP addresses of the packets before and after they pass through the ISP router that translates traffic destined for the internet. tcpdump can also show the NAT protocol and port numbers used by the router. nmap, ipconfig, and tracert are not suitable tools for verifying the status of NAT, as they do not show the IP address translation process.

References

- * 1: Network Address Translation - N10-008 CompTIA Network+ : 1.4
- * 2: CompTIA Network+ N10-008 Certification Study Guide, page 95-96
- * 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 16
- * 4: CompTIA Network+ N10-008 Certification Practice Test, question 7

NEW QUESTION: 725

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

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

Answer: C ([LEAVE A REPLY](#))

Explanation

Updating the firewalls with current firmware and software is an important step to ensure all the firewalls are hardened successfully, as it can fix any known vulnerabilities or bugs and provide new features or enhancements. Enabling an implicit permit rule is not a good practice for firewall hardening, as it can allow unwanted traffic to pass through the firewall. Configuring the log settings on the firewalls to the central syslog server is a good practice for monitoring and auditing purposes, but it does not harden the firewalls themselves.

Using the same complex passwords on all firewalls is not a good practice for password security, as it can increase the risk of compromise if one firewall is breached. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 3.0 Network Security, Objective 3.3 Given a scenario, implement network hardening techniques.

NEW QUESTION: 726

Which of the following issues are present with RIPv2? (Select TWO).

- A. Scalability
- B. Time to converge
- C. Route poisoning
- D. Adjacent neighbors
- E. Maximum transmission unit
- F. Unicast

Answer: C,D ([LEAVE A REPLY](#))

NEW QUESTION: 727

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: ([SHOW ANSWER](#))

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: 728

A customer has an attached USB printer that needs to be shared with other users. The desktop team set up printer sharing. Now, the network technician needs to obtain the necessary information about the PC and share it with other users so they can connect to the printer. Which of the following commands should the technician use to get the required information? (Select TWO).

- A. arp
- B. route
- C. netstat
- D. tcpdump
- E. hostname
- F. ipconfig

Answer: E,F ([LEAVE A REPLY](#))

The hostname and ipconfig commands should be used to get the required information about the PC and share it with other users so they can connect to the printer. The hostname command displays the name of the computer on a network. The ipconfig command displays the IP configuration of the computer, including its IP address, subnet mask, default gateway, and DNS servers. These information are necessary for other users to locate and connect to the shared printer on the network. For example, other users can use the UNC path

\\hostname\printername or \\ipaddress\printername to access the shared printer. References: [CompTIA Network + Certification Exam Objectives], How to Share a Printer in Windows 10

NEW QUESTION: 729

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 ([LEAVE A REPLY](#))

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: 730

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

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

Answer: A ([LEAVE A REPLY](#))

IPv6 networks use Stateless Address Auto Configuration (SLAAC) to assign IP addresses. With SLAAC, devices send the router a request for the network prefix, and the device then uses the prefix along with its own MAC address to create an IP address.

NEW QUESTION: 731

An organization has a guest network with a network IP range of 192.168.1.0/28 using a DHCP pool. One visitor reported difficulties connecting and configured a static IP address. Following this action, another visitor reported intermittent connection issues. Which of the following is the most likely reason?

- A. Address pool exhaustion
- B. Duplicate IP addresses
- C. Misconfigured default gateway
- D. Incorrect subnet mask

Answer: (SHOW ANSWER)

Explanation

A duplicate IP address occurs when two devices on the same network have the same IP address assigned to them. This can cause intermittent connection issues, as the network devices may not be able to distinguish between the two conflicting devices. A duplicate IP address can be caused by a visitor manually configuring a static IP address that is already in use by another device on the guest network. The network IP range of 192.168.1.0/28 has only 14 usable host addresses, so the chances of a duplicate IP address are higher than a larger network.

References

- 1: Troubleshooting IP Configurations - CompTIA Network+ N10-006 - 4.6
- 2: Troubleshooting Duplicate IP Addresses - CompTIA Network+ N10-005: 2.5
- 3: Network Address Translation - N10-008 CompTIA Network+ : 1.4

NEW QUESTION: 732

A technician monitors a switch interface and notices it is not forwarding frames on a trunked port. However, the cable and interfaces are in working order. Which of the following is MOST likely the cause of the issue?

- A. 802.1Q configuration
- B. STP policy
- C. Frame size
- D. Flow control

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 733

A technician needs to find the MAC address of a connecting router. Which of the following commands should the technician use?

- A. ping
- B. traceroute
- C. arp
- D. nslookup

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 734

At which of the following OSI model layers does an IMAP client run?

- A. Layer 6
- B. Layer 2
- C. Layer 4
- D. Layer 7

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 735

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

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

Answer: D (LEAVE A REPLY)

- a Display All connections and listening ports.
- e Display Ethernet statistics. (may be combined with -s)
- n Display addresses and port numbers in Numerical form.
- r Display the Routing table.
- o Display the Owning process ID associated with each connection.
- b Display the exe involved in creating each connection or listening port.*
- v Verbose - use in conjunction with -b, to display the sequence of components involved for all executables.
- p protocol

Show only connections for the protocol specified; can be any of: TCP, UDP, TCPv6 or UDPv6.

If used with the -s option then the following protocols can also be specified: IP, IPv6, ICMP, or ICMPv6.

-s Display per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; (The v6 protocols are not available under 2k and NT4) The -p option can be used to display just a subset of these.

NEW QUESTION: 736

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

Answer: (SHOW ANSWER)

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 737

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

- A. Throughput
- B. Latency

C. Bandwidth

D. Jitter

Answer: A ([LEAVE A REPLY](#))

Explanation

Throughput is the actual amount of data that can be transferred over a network in a given time. Throughput can be affected by various factors such as congestion, interference, errors, or hardware limitations. If the throughput is lower than the configured internet connection speed, it can cause a significant delay in data transmission. The ISP should check the throughput and identify the source of the problem.

References: Network+ Study Guide Objective 2.2: Explain the concepts and characteristics of routing and switching.

NEW QUESTION: 738

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

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

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

A. Migrate the network to IPv6.

B. Implement 802.1 X authentication

C. Set a private community string

D. Use SNMPv3.

E. Incorporate SSL encryption

F. Utilize IPsec tunneling.

Answer: C,D ([LEAVE A REPLY](#))

The packet shown in the image is an SNMP (Simple Network Management Protocol) packet, which is used to monitor and manage network devices. SNMP uses community strings to authenticate requests and responses between SNMP agents and managers. However, community strings are sent in clear text and can be easily intercepted by attackers. Therefore, one way to secure SNMP traffic is to set a private community string that is not the default or well-known value. Another way to secure SNMP traffic is to use SNMPv3, which is the latest version of the protocol that supports encryption and authentication of SNMP messages.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.5: Given a scenario, use remote access methods.

NEW QUESTION: 739

A network technician is observing the behavior of an unmanaged switch when a new device is added to the network and transmits data

a. Which of the following BEST describes how the switch processes this information?

A. The data is flooded out of every port, excluding the VLAN where it is located

B. The data is flooded out of every port, except the one on which it came in

C. The data is flooded out of every port but only in the VLAN where it is located.

D. The data is flooded out of every port, including the one on which it came in.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 740

A hacker used a packet sniffer on the network to capture the hardware address of the server. Which of the following types of attacks can the hacker perform now?

- A. Piggybacking
- B. VLAN hopping
- C. MAC spoofing
- D. Evil twin

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 741

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 [\(LEAVE A REPLY\)](#)

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: 742

A company is deploying a SAN at headquarters and a branch office 1,000mi (1,609km) away that will 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 [\(LEAVE A REPLY\)](#)

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: 743

During a risk assessment which of the following should be considered when planning to mitigate high CPU utilization of a firewall?

- A. Recovery time objective
- B. Uninterruptible power supply
- C. NIC teaming
- D. Load balancing

Answer: D ([LEAVE A REPLY](#))

The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs. This does nothing to help with CPU utilization. Load balancing does this.

NEW QUESTION: 744

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

Linux computer details:

Switch mirror port details:

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

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

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

Answer: A ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 745

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

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 746

A company's management team wants to implement NAC on the wired and wireless networks. Which of the following is an authentication component that must be used in this solution?

- A. IPSec
- B. 802.1X
- C. EAP
- D. TACACS+

Answer: B (LEAVE A REPLY)

802.1X is an authentication component that must be used in a network access control (NAC) solution. NAC is a method of enforcing security policies on devices that want to access a network, by verifying their identity, compliance, and authorization. 802.1X is a standard that defines how to provide authentication for devices trying to connect to a LAN or WLAN. It uses the Extensible Authentication Protocol (EAP) to exchange authentication information between the device (supplicant), the network access device (authenticator), and the authentication server (typically RADIUS or TACACS+). 802.1X can prevent unauthorized devices from accessing the network, and can also assign them to different VLANs or apply different policies based on their role or group.

IPSec is a protocol suite that provides encryption, authentication, and integrity for IP packets. It can be used to create secure VPN tunnels between networks or hosts. IPSec is not an authentication component for NAC, but rather a security component for protecting data in transit.

EAP is a framework that supports multiple authentication methods, such as passwords, certificates, tokens, or biometrics. EAP is used by 802.1X to provide authentication for network access, but it is not a component by itself. EAP requires a carrier protocol, such as 802.1X, to transport the authentication messages.

TACACS+ is a protocol that provides authentication, authorization, and accounting (AAA) services for network devices or users. It can be used as an authentication server for 802.1X, but it is not an authentication component for NAC by itself. TACACS+ requires a client-server protocol, such as 802.1X, to communicate with the network access device.

Reference What is 802.1X Network Access Control (NAC)? Compare TACACS + and RADIUS 802.1X: What EXACTLY is it regarding WPA and EAP? CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION: 747

A technician is assisting a user who cannot connect to a website. The technician attempts to ping the default gateway and DNS server of the workstation. According to troubleshooting methodology, this is an example of:

- A. a bottom-up approach.
- B. implementing a solution.
- C. a divide-and-conquer approach.
- D. a top-to-bottom approach.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 748

Which of the following topologies requires the MOST connections when designing a network?

- A. Star

- B. Ring
- C. Mesh
- D. Bus

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 749

A company is undergoing expansion but does not have sufficient rack space in its data center. Which of the following would be BEST to allow the company to host its new equipment without a major investment in facilities?

- A. Using a colocation service
- B. Using available rack space in branch offices
- C. Using a flat network topology
- D. Reorganizing the network rack and installing top-of-rack switching

Answer: A ([LEAVE A REPLY](#))

Explanation

A colocation service is a service that provides rack space, power, cooling, security, and connectivity for a company's network equipment in a data center. A colocation service can be used when a company does not have sufficient rack space in its own data center and does not want to invest in building or expanding its own facilities. By using a colocation service, a company can host its new equipment in a professional and reliable environment without a major investment in facilities. References:

<https://www.comptia.org/training/books/network-n10-008-study-guide> (page 414)

NEW QUESTION: 750

Which of the following devices and encapsulations are found at the data link layer? (Select TWO)

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 751

A technician is installing a new fiber connection to a network device in a datacenter. The connection from the device to the switch also traverses a patch panel connection. The chain of connections is in the following order:

Device

LC/LC patch cable
Patch panel
Cross-connect fiber cable
Patch panel
LC/LC patch cable
Switch

The connection is not working. The technician has changed both patch cables with known working patch cables. The device had been tested and was working properly before being installed. Which of the following is the MOST likely cause of the issue?

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

Answer: A (LEAVE A REPLY)

It is a fiber network and fiber has insane range thus it is unlikely to be attenuation. Bad device and bad cable are out because they are explicitly tested as described. Therefore TX/RX is the only reasonable option.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 752

An engineer is designing a network topology for a company that maintains a large on-premises private cloud. A design requirement mandates internet-facing hosts to be partitioned off from the internal LAN and internal server IP ranges. Which Of the following defense strategies helps meet this requirement?

- A. Implementing a screened subnet
- B. Deploying a honeypot
- C. Utilizing network access control
- D. Enforcing a Zero Trust model

Answer: A (LEAVE A REPLY)

Explanation

A screened subnet is a network segment that is isolated from both the internal LAN and the Internet by firewalls. A screened subnet can be used to host internet-facing hosts such as web servers, email servers, or DNS servers. A screened subnet provides an additional layer of security and prevents direct access to the internal network from the Internet.

References: Network+ Study Guide Objective 3.1: Explain the purposes and use cases for advanced networking devices.

NEW QUESTION: 753

A network technician is deploying multiple switches for a new office. The switches are separately managed and need to be cabled in to support dual firewalls in a HA setup. Which of the following should the technician enable to support proper stability of the network switches?

- A. NTP
- B. CDMA
- C. STP
- D. LACP
- E. 802.1Q

Answer: C ([LEAVE A REPLY](#))

STP stands for Spanning Tree Protocol, which is a network protocol that prevents loops in a switched network by blocking redundant links. STP allows only one active path between any two network devices, and dynamically reconfigures the network topology in case of link failures or changes. STP is essential for proper stability of the network switches, especially when they are cabled in a redundant or complex topology that involves multiple switches and firewalls. Without STP, loops can cause broadcast storms, MAC address table instability, and duplicate frames, which can degrade the network performance and availability. References: [CompTIA Network+ Certification Exam Objectives], Spanning Tree Protocol (STP) Explained | NetworkLessons.com

NEW QUESTION: 754

Which of the following is a major difference between a router and a Layer 3 switch?

- A. A router can perform PAT, but a Layer 3 switch cannot.
- B. A Layer 3 switch is more efficient than a router.
- C. A router uses higher speed interfaces than a Layer 3 switch.
- D. A Layer 3 switch can run more routing protocols than a router.

Answer: B ([LEAVE A REPLY](#))

A major difference between a router and a Layer 3 switch is that Layer 3 switches are generally more efficient than routers for performing routing tasks within a LAN. They are optimized for high-speed packet forwarding and are typically used in environments where high performance is required. Routers, on the other hand, are designed for more complex routing tasks and often operate at lower speeds compared to Layer 3 switches.

NEW QUESTION: 755

A company is reviewing ways to cut the overall cost of its IT budget. A network technician suggests removing various computer programs from the IT budget and only providing these programs on an as-needed basis. Which of the following models would meet this requirement?

- A. SaaS
- B. VPN
- C. IaaS

D. Multitenancy

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 756

A public, wireless ISP mounts its access points on top of traffic signal poles. Fiber-optic cables are installed from a fiber switch through the ground and up the pole to a fiber-copper media converter, and then connected to the AP. In one location, the switchport is showing sporadic link loss to the attached AP. A similar link loss is not seen at the AP interface. The fiber-optic cable is moved to another unused switchport with a similar result. Which of the following steps should the assigned technician complete NEXT?

- A. Disable and enable the switchport.
- B. Clean the fiber-optic cable ends.
- C. Replace the media converter.
- D. Replace the copper patch cord.

Answer: ([SHOW ANSWER](#))

Fiber-optic cables are cables that use light signals to transmit data over long distances at high speeds. Fiber-optic cables are sensitive to dirt, dust, moisture, or other contaminants that can interfere with the light signals and cause link loss or signal degradation. To troubleshoot link loss issues with fiber-optic cables, one of the steps that should be completed next is to clean the fiber-optic cable ends with a lint-free cloth or a specialized cleaning tool. Cleaning the fiber-optic cable ends can remove any dirt or debris that may be blocking or reflecting the light signals and restore the link quality.

NEW QUESTION: 757

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

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

Answer: B ([LEAVE A REPLY](#))

Explanation

Port mirroring is a feature that allows a switch to copy the traffic from one or more ports to another port, where a network analyzer or a monitoring device can capture and analyze the traffic. Port mirroring is useful for troubleshooting and security purposes, as it allows the network engineer to see the traffic that is passing through the switch without affecting the normal operation of the network.

References

- 1: Port Mirroring - CompTIA Network+ Certification (N10-008): The Total Course [Video]
- 2: CompTIA Network+ Certification Exam Objectives, page 5
- 3: CompTIA Network+ N10-005: 2.1 - Port Mirroring - Professor Messer IT Certification Training Courses
- 4: CompTIA Network+ N10-005: 1.4 - Port Mirroring

NEW QUESTION: 758

Which of the following is a major difference between a router and a Layer 3 switch?

- A. A router can perform PAT, but a Layer 3 switch cannot.
- B. A Layer 3 switch is more efficient than a router.
- C. A router uses higher speed interfaces than a Layer 3 switch.
- D. A Layer 3 switch can run more routing protocols than a router.

Answer: A ([LEAVE A REPLY](#))

PAT (Port Address Translation) is a type of Network Address Translation (NAT) that allows multiple devices to share a single public IP address by using different port numbers. PAT enables devices to access the internet without exposing their private IP addresses. A router is a device that can perform PAT by translating the source IP address and port number of outgoing packets and the destination IP address and port number of incoming packets. A Layer 3 switch is a device that can perform basic routing functions by using IP addresses, but it cannot perform PAT or other advanced routing features that a router can.

NEW QUESTION: 759

A customer called the help desk to report a network issue. The customer recently added a hub between the switch and the router in order to duplicate the traffic flow to a logging device. After adding the hub, all the Other network components that were connected to the switch slowed more than expected. Which Of the following is the MOST likely cause Of the issue?

- A. Duplex mismatch
- B. Flow control failure
- C. STP malfunction
- D. 802.1Q disabled

Answer: A ([LEAVE A REPLY](#))

A duplex mismatch is a situation where two devices on a network have different duplex settings, such as full-duplex or half-duplex. Full-duplex means that a device can send and receive data simultaneously, while half-duplex means that a device can only send or receive data at a time. A duplex mismatch can cause performance issues, such as collisions, errors, or slow throughput. In this scenario, the customer added a hub between the switch and the router. A hub is a device that operates at half-duplex and broadcasts all traffic to all ports. A switch and a router are devices that operate at full-duplex and forward traffic to specific ports. Therefore, adding a hub between the switch and the router can cause a duplex mismatch and slow down all the other network components that were connected to the switch.

NEW QUESTION: 760

An engineer was asked to update an MX record for an upcoming project. Which of the following server types is MOST likely to be in scope for the project?

- A. Email
- B. Web
- C. File
- D. Database

Answer: ([SHOW ANSWER](#))

An MX record is a type of DNS record that specifies the mail server responsible for accepting email messages on behalf of a domain name. Therefore, an engineer who needs to update an MX record is most likely working on an email server project

NEW QUESTION: 761

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



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

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

Answer: ([SHOW ANSWER](#))

Explanation

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

NEW QUESTION: 762

A network is secured and is only accessible via TLS and IPSec VPNs. Which of the following would need to be present to allow a user to access network resources on a laptop without logging in to the VPN application?

- A. Site-to-site
- B. Secure Shell
- C. In-band management
- D. Remote desktop connection

Answer: ([SHOW ANSWER](#))

Explanation

A site-to-site VPN is a type of VPN that connects two or more networks over the Internet using a secure tunnel. A site-to-site VPN allows users to access network resources on a laptop without logging in to the VPN application, as long as the laptop is connected to one of the networks in the VPN. A site-to-site VPN is transparent to the users and does not require any additional software or configuration on the client devices.

References: Network+ Study Guide Objective 3.4: Explain the purposes and use cases for VPNs.

NEW QUESTION: 763

A network engineer needs to enable device monitoring using authentication and encryption. Which of the following protocols offers this option?

- A. ESP
- B. SNMPv3
- C. NetFlow
- D. SSLv3

Answer: ([SHOW ANSWER](#))

Explanation

SNMPv3 is a protocol that offers device monitoring using authentication and encryption. SNMP stands for Simple Network Management Protocol, and it is a standard way of collecting and organizing information about network devices, such as routers, switches, servers, printers, and so on. SNMPv3 is the latest version of SNMP, and it provides enhanced security features, such as data integrity, data origin authentication, data confidentiality, and access control. SNMPv3 can use different algorithms to encrypt and authenticate the communication between the network management system and the network devices¹².

References:

Network Monitoring Tools - CompTIA Network+ N10-006 - 2.12

CompTIA Network+ N10-008 Certification Exam Objectives, page 93

NEW QUESTION: 764

A company joins a bank's financial network and establishes a connection to the clearinghouse servers in the range 192.168.124.0/27. An IT technician then realizes the range exists within the VM pool at the data center. Which of the following is the BEST way for the technician to connect to the bank's servers?

- A. CIDR
- B. NAT
- C. PAT
- D. SLAAC

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 765

A company that uses VoIP telephones is experiencing intermittent issues with one-way audio and dropped conversations. The manufacturer says the system will work if ping times are less than 50ms. The company has recorded the following ping times:

10ms	10ms	10ms	100ms	70ms	5ms	5ms	80ms	100ms	5ms	5ms

Which of the following is MOST likely causing the issue?

- A. VLAN mismatch
- B. Attenuation
- C. Jitter
- D. Latency

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 766

Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

- A. Scope options
- B. Reservation
- C. Dynamic assignment
- D. Exclusion
- E. Static assignment

Answer: ([SHOW ANSWER](#))

IP reservation assigns the same IP upon requesting IP renewal by a client.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 767

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

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

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 768

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

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 769

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

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

Answer: ([SHOW ANSWER](#))

Explanation

NIC teaming is a technology that allows multiple network interface cards (NICs) to work together as a single logical interface, providing redundancy and load balancing. This can prevent the loss of connection between a virtual server and network storage devices if one of the NICs fails or becomes disconnected. References:

[CompTIA Network+ Certification Exam Objectives], Domain 2.0 Networking Concepts, Objective 2.5:

Explain the purposes and use cases for advanced networking devices, Subobjective: NIC bonding/teaming

NEW QUESTION: 770

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

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

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 771

Which of the following would MOST likely utilize PoE?

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

Answer: A ([LEAVE A REPLY](#))

A camera would MOST likely utilize PoE (Power over Ethernet) because it allows the camera to be powered through the Ethernet cable, eliminating the need for a separate power source and making installation and maintenance easier.

NEW QUESTION: 772

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. LTE
- C. TKIP
- D. SSID

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 773

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

- A. Virtual network computing
- B. Secure Socket Shell
- C. In-band connection
- D. Site-to-site VPN

Answer: D ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 774

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 (LEAVE A REPLY)

A media converter is a device that allows you to interconnect different types of network media, such as copper, fiber, and coaxial cables.

A media converter can be used to connect newer network technologies, such as Gigabit Ethernet or ATM, to existing networks, such as 10BASE-T or 100BASE-T.

A media converter can also be used to extend the distance and improve the immunity of network signals by converting them from electrical to optical or vice versa.

A proxy server, an industrial control system, and a load balancer are not devices that can connect different physical characteristics of network media. They have different functions and purposes in a network.

A proxy server is a device that acts as an intermediary between a client and a server, providing security, caching, and filtering services.

An industrial control system is a system that monitors and controls industrial processes, such as manufacturing, power generation, and transportation.

A load balancer is a device that distributes network traffic across multiple servers, improving performance and availability. Reference:

Media Converters - CompTIA Network+ N10-006 - 1.5

Transceivers (Media Converters) | Network+ Exam Cram: Networking Devices in Modern Networks

NEW QUESTION: 775

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 (LEAVE A REPLY)

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 169.254.255.254. 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: 776

Users attending security training at work are advised not to use single words as passwords for corporate applications. Which of the following does this BEST protect against?

- A. An on-path attack**

- B. A brute-force attack
- C. A dictionary attack
- D. MAC spoofing
- E. Denial of service

Answer: C (LEAVE A REPLY)

A dictionary attack software matches the hash to those produced by ordinary words found in a dictionary.

NEW QUESTION: 777

Which of the following would be used to forward requests and replies between a DHCP server and client?

- A. Relay
- B. Lease
- C. Scope
- D. Range

Answer: A (LEAVE A REPLY)

The Dynamic Host Configuration Protocol (DHCP) is a protocol that automatically assigns IP addresses and other network configuration parameters to network devices¹². DHCP uses a client-server model, where a DHCP client requests an IP address from a DHCP server, and the DHCP server responds with an IP address and other information³⁴.

When a DHCP client and server are on the same physical network, the DHCP client broadcasts a DHCPDISCOVER message to find a DHCP server, and the DHCP server replies with a DHCPOFFER message containing an IP address offer³⁴. The DHCP client then broadcasts a DHCPREQUEST message to request the IP address, and the DHCP server replies with a DHCPACK message to acknowledge the IP address assignment³⁴.

When a DHCP client and server are not on the same physical network, a DHCP relay is used to forward the DHCP messages between them⁵⁶. A DHCP relay is a network device, such as a router or a switch, that listens for DHCP broadcast messages on one network interface and relays them to another network interface where the DHCP server is located⁵⁶. The DHCP relay also adds the IP address of the network interface where the DHCP client is located to the DHCP messages, so that the DHCP server can determine which pool of IP addresses to use for the DHCP client⁵⁶.

The other options are not related to forwarding requests and replies between a DHCP server and client. A DHCP lease is the duration of time that a DHCP server assigns an IP address to a DHCP client⁷⁸. A DHCP scope is a range of IP addresses that a DHCP server can assign to DHCP clients on a specific network segment⁷⁸. A DHCP range is a subset of a DHCP scope that defines the start and end IP addresses that a DHCP server can assign to DHCP clients .

Therefore, the best answer is A. Relay, which would be used to forward requests and replies between a DHCP server and client.

Reference:

1: CompTIA Network+ N10-008 Certification Study Guide, page 215

2: CompTIA Network+ Certification Exam Objectives, page 9

3: [What is Dynamic Host Configuration Protocol (DHCP)? - Definition from WhatIs.com]

4: [Dynamic Host Configuration Protocol (DHCP) | CompTIA IT Certifications]

- 5: CompTIA Network+ N10-008 Certification Study Guide, page 216
- 6: [What is DHCP Relay? - Definition from Techopedia]
- 7: CompTIA Network+ N10-008 Certification Study Guide, page 217
- 8: [What is DHCP Lease? - Definition from Techopedia]
- 9: [What is DHCP Range? - Definition from Techopedia]
- 10: [DHCP Range | CompTIA IT Certifications]

NEW QUESTION: 778

Which of the following combinations of single cables and transceivers will allow a server to have 40GB of network throughput? (Choose two.)

- A. Cat 5e
- B. SFP+
- C. Cat 6a
- D. Multimode
- E. SFP
- F. QSFP+

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 779

A company wants to implement a disaster recovery site for non-critical applications, which can tolerate a short period of downtime. Which of the following types of sites should the company implement to achieve this goal?

- A. Hot
- B. Cold
- C. warm
- D. Passive

Answer: C ([LEAVE A REPLY](#))

Explanation

The type of site that the company should implement for non-critical applications that can tolerate a short period of downtime is a warm site. A warm site is a disaster recovery site that has some pre-installed equipment and software, but not as much as a hot site, which is fully operational and ready to take over the primary site's functions in case of a disaster. A warm site requires some time and effort to activate and synchronize with the primary site, but not as much as a cold site, which has no equipment or software installed and requires a lot of configuration and testing. A passive site is not a common term for a disaster recovery site, but it could refer to a site that only receives backups from the primary site and does not actively participate in the network operations. References: CompTIA Network+ N10-008 Certification Study Guide, page 347; The Official CompTIA Network+ Student Guide (Exam N10-008), page 13-10.

NEW QUESTION: 780

Ann, a technician, installs a wireless router in a network closet in a large office. She then configures all workstations in various offices on that floor to use the wireless connection.

Maximum connection speed at each workstation is 54 Mbps. Some users complain that their network connection is very slow. Which of the following is MOST likely the problem?

- A. Wireless network SSID is incorrect.
- B. Workstations were configured with the wrong connection speed on the wireless adapter.
- C. Users with a slow connection are too far away from the wireless router.
- D. Users that cannot connect are configured on the wrong channel.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 781

Which of the following routing protocols is generally used by major ISPs for handling large-scale internet traffic?

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

Answer: D ([LEAVE A REPLY](#))

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 782

A user reports that a new VoIP phone works properly, but the computer that is connected to the phone cannot access any network resources. Which of the following MOST likely needs to be configured correctly to provide network connectivity to the computer?

- A. Port duplex settings
- B. Port aggregation
- C. ARP settings
- D. VLAN tags
- E. MDIX settings

Answer: D ([LEAVE A REPLY](#))

A VoIP phone is a device that uses voice over IP (VoIP) technology to transmit and receive voice calls over a network. A VoIP phone typically has a built-in switch that allows a computer to be connected to the same network port as the phone, sharing the same physical link and bandwidth.

A VLAN tag is a piece of information that is added to the header of a network frame to indicate which virtual LAN (VLAN) it belongs to. A VLAN is a logical grouping of network devices that share the same broadcast domain, regardless of their physical location or connection. VLANs can help to isolate traffic, improve security, and reduce congestion on a network.

A VLAN tag is required to provide network connectivity to the computer that is connected to the VoIP phone, because the phone and the computer may belong to different VLANs. For example, the phone may belong to a voice VLAN that is dedicated for VoIP traffic, while the computer may belong to a data VLAN that is used for general network access. Without a VLAN tag, the switch that connects to the VoIP phone would not be able to distinguish between the frames from the phone and the frames from the computer, and would not be able to forward them to the correct destination VLAN.

Therefore, option D is the most likely answer, as the VLAN tags need to be configured correctly to provide network connectivity to the computer. The switch port that connects to the VoIP phone needs to be configured as a trunk port, which can carry multiple VLANs, and the VoIP phone needs to be configured to add the appropriate VLAN tag to the frames from the computer.

Option A is not a likely answer, as the port duplex settings determine the mode of data transmission between the switch and the VoIP phone. The port duplex settings can be either half-duplex, which means that data can be transmitted in one direction at a time, or full-duplex, which means that data can be transmitted in both directions simultaneously. The port duplex settings do not affect the VLAN tags or the network connectivity to the computer.

Option B is also not a likely answer, as the port aggregation is a technique that combines multiple physical ports into a single logical port, increasing the bandwidth and redundancy of the link. The port aggregation does not affect the VLAN tags or the network connectivity to the computer.

Option C is also not a likely answer, as the ARP settings are related to the address resolution protocol (ARP), which is a protocol that maps a network layer address, such as an IP address, to a data link layer address, such as a MAC address. The ARP settings do not affect the VLAN tags or the network connectivity to the computer.

Option E is also not a likely answer, as the MDIX settings are related to the medium dependent interface crossover (MDIX), which is a feature that allows a switch to automatically detect the type of cable that is connected to a port, and adjust the pinout accordingly. The MDIX settings do not affect the VLAN tags or the network connectivity to the computer.

Reference:

CompTIA Network+ N10-008 Study Guide, Chapter 3: Network Architecture, Section 3.1: Network Topologies and Technologies, Page 1361 Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 3.1: Network Topologies and Technologies, Page 232 What is a VoIP Phone? | Definition and Examples3 What is a VLAN Tag? | Definition and Examples4 How to Configure VLANs on a VoIP Phone - Cisco5

NEW QUESTION: 783

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 784

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

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

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

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

Answer: (SHOW ANSWER)

CRC stands for Cyclic Redundancy Check, and it is a type of error-detecting code used to detect accidental changes to raw data. If the CRC count is increasing on a particular interface, it indicates that there might be an issue with the cabling, which is causing data corruption. Reference:

Network+ N10-008 Objectives: 2.1 Given a scenario, troubleshoot common physical connectivity issues.

NEW QUESTION: 785

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 786

A network security engineer is responding to a security incident. The engineer suspects that an attacker used an authorized administrator account to make configuration changes to the boundary firewall. Which of the following should the network security engineer review?

- A. Network traffic logs
- B. Audit logs

C. Syslogs

D. Event logs

Answer: B ([LEAVE A REPLY](#))

Audit logs are records of the actions performed by users or processes on a system or network device. They can provide information about who made what changes, when, and why. Audit logs are essential for detecting and investigating security incidents, as well as for ensuring compliance with policies and regulations. Audit logs can help the network security engineer to identify the source of the unauthorized configuration changes to the boundary firewall, as well as the scope and impact of the changes.

References1 - Changes to Cyber Essentials requirements - April 2021 update2 - 8 Firewall Best Practices for Securing the Network3 - How to secure your network boundaries with a firewall

NEW QUESTION: 787

A client moving into a new office wants the IP network set up to accommodate 412 network- connected devices that are all on the same subnet. The subnet needs to be as small as possible.

Which of the following subnet masks should be used to achieve the required result?

A. 255.255.0.0

B. 255.255.252.0

C. 255.255.254.0

D. 255.255.255.0

Answer: (SHOW ANSWER)

An class C give you at most 256 addresses including network ID and broadcast address. In this case, we need more than 256 addresses while being smallest thus we looking at class B of at least 2 host size.

NEW QUESTION: 788

Due to concerns around single points of failure, a company decided to add an additional WAN to the network. The company added a second MPLS vendor to the current MPLS WAN and deployed an additional WAN router at each site. Both MPLS providers use OSPF on the WAN network, and EIGRP is run internally. The first site to go live with the new WAN is successful, but when the second site is activated significant network issues occur.

Which of the following is the MOST likely cause for the WAN instability?

A. An incorrect IP address

B. Asymmetrical routing

C. A switching loop

D. A routing loop

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 789

Which of the following cloud deployment models involves servers that are hosted at a company's property and are only used by that company?

A. Public

B. Private

C. Hybrid

D. Community

Answer: (SHOW ANSWER)

Explanation

A private cloud deployment model involves servers that are hosted at a company's property and are only used by that company. A private cloud provides exclusive access and control over the cloud resources to the company, as well as higher security and privacy. However, a private cloud also requires more investment and maintenance from the company, compared to other cloud deployment models¹

NEW QUESTION: 790

A customer has an attached USB printer that needs to be shared with other users. The desktop team set up printer sharing. Now, the network technician needs to obtain the necessary information about the PC and share it with other users so they can connect to the printer. Which of the following commands should the technician use to get the required information? (Select TWO).

A. arp

B. route

C. netstat

D. tcpdump

E. hostname

F. ipconfig

Answer: E,F (LEAVE A REPLY)

Explanation

The hostname and ipconfig commands should be used to get the required information about the PC and share it with other users so they can connect to the printer. The hostname command displays the name of the computer on a network. The ipconfig command displays the IP configuration of the computer, including its IP address, subnet mask, default gateway, and DNS servers. These information are necessary for other users to locate and connect to the shared printer on the network. For example, other users can use the UNC path \\hostname\printrname or \\ipaddress\printrname to access the shared printer. References: [CompTIA Network + Certification Exam Objectives], How to Share a Printer in Windows 10

NEW QUESTION: 791

Which of the following attacks encrypts user data and requires a proper backup implementation to recover?

A. DDoS

B. Phishing

C. Ransomware

D. MAC spoofing

Answer: C (LEAVE A REPLY)

Ransome is a kind of attache that encrypts your data or OS and require payment in a give time.

NEW QUESTION: 792

A network engineer designed and implemented a new office space with the following characteristics:

Building construction type:	Brick
Layout:	10,764sq ft (1,000sq m) commercial office space
Users:	50
Servers:	2
Laptops:	50

One month after the office space was implemented, users began reporting dropped signals when entering another room and overall poor connections to the 5GHz network. 'which of the following should the engineer do to best resolve the issue?

- A. use non-overlapping channels
- B. Reconfigure the network to support 2.4GHz_
- C. Upgrade to WPA3.
- D. Change to directional antennas-

Answer: D (LEAVE A REPLY)

Explanation

The best solution to resolve the issue of dropped signals and poor connections to the 5GHz network is to change to directional antennas. Directional antennas are antennas that focus the wireless signal in a specific direction, increasing the range and strength of the signal. Directional antennas are suitable for environments where there are obstacles or interference that can weaken or block the wireless signal. In the image, the office space has several walls and doors that can reduce the signal quality of the 5GHz network, which has a shorter wavelength and higher frequency than the 2.4GHz network. By using directional antennas, the network engineer can aim the wireless signal towards the desired areas and avoid the signal loss caused by the walls and doors. References: CompTIA Network+ N10-008 Certification Study Guide, page 76; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-19.

NEW QUESTION: 793

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 794

A network administrator needs to add access points to the network because coverage in some areas is improper. Which of the following should the administrator do first?

- A. Interference analysis
- B. Wireless survey
- C. Traffic analysis

D. Packet capture

Answer: B (LEAVE A REPLY)

Explanation

A wireless survey is the first step that a network administrator should do before adding access points to the network. A wireless survey is a process of collecting data about the wireless environment, such as signal strength, channel usage, interference, and coverage. A wireless survey can help the network administrator to determine the optimal locations and configurations for the access points to provide the best possible coverage and performance for the wireless network. A wireless survey can also help to identify and troubleshoot any issues that may cause improper coverage in some areas.

<https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guide.html>

NEW QUESTION: 795

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

A. nslookup

B. show config

C. netstat

D. show interface

E. show counters

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 796

A technician was cleaning a storage closet and found a box of transceivers labeled 8Gbps. Which of the following protocols uses those transceivers?

A. Internet Small Computer Systems Interface

B. Gigabit interface converter

C. Fibre Channel

D. Coaxial over Ethernet

Answer: C (LEAVE A REPLY)

Explanation

The transceivers labeled 8Gbps are likely to be used with the Fibre Channel protocol. Fibre Channel is a high-speed networking technology that is primarily used to connect storage devices to servers in storage area networks (SANs). It is capable of transmitting data at speeds of up to 8 Gbps (gigabits per second), and uses specialized transceivers to transmit and receive data over fiber optic cables.

Coaxial over Ethernet (CoE) is a networking technology that uses coaxial cables to transmit data, and is not related to the transceivers in question. Internet Small Computer Systems Interface (iSCSI) is a protocol that allows devices to communicate over a network using the SCSI protocol, and does not typically use specialized

transceivers. Gigabit interface converter (GBIC) is a type of transceiver used to transmit and receive data over fiber optic cables, but it is not capable of transmitting data at 8 Gbps.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 797

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 (LEAVE A REPLY)

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: 798

A network administrator is notified that a user cannot access resources on the network. The network administrator checks the physical connections to the workstation labeled User 3 and sees the Ethernet is properly connected. However, the network interface's indicator lights are not blinking on either the computer or the switch. Which of the following is the most likely cause?

- A. The switch failed.
- B. The default gateway is wrong.
- C. The port is shut down.
- D. The VLAN assignment is incorrect.

Answer: (SHOW ANSWER)

If the port is shut down, it means that the switch has disabled the port and is not sending or receiving any traffic on it. This would explain why the network interface's indicator lights are not blinking on either the computer or the switch, and why the user cannot access resources on the network. The port could be shut down manually by the network administrator, or automatically by the switch due to security or error conditions.

Reference

Port shutdown is one of the common switch configuration options covered in Objective 2.3 of the CompTIA Network+ N10-008 certification exam1.

Port shutdown can cause the network interface's indicator lights to stop blinking2.

Port shutdown can prevent the user from accessing resources on the network3.

1: CompTIA Network+ Certification Exam Objectives, page 5 2: CompTIA Network+ N10-008: Switch not forwarding frames on trunked port3 3: Cable Management - N10-008 CompTIA Network+ : 1.3

NEW QUESTION: 799

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

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

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

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

Answer: A (LEAVE A REPLY)

Explanation

Based on the site survey table, we can see that AP 2, AP 3, and AP 4 are all broadcasting on the same channel, which can cause interference and affect performance. Therefore, the next step a wireless technician should take to troubleshoot this issue is to reconfigure the channels to reduce overlap. This will help to improve network performance and eliminate any interference.

References:

Network+ N10-007 Certification Exam Objectives, Objective 2.8: Given a scenario, troubleshoot common wireless problems and perform site surveys.

NEW QUESTION: 800

Switch 3 was recently added lo an existing stack to extend connectivity to various parts of the network. After the update, new employees were not able to print to the main networked copiers from then workstations.

Following are the port configurations for the switch stack in question:

Switch 1:

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

Switch 2:

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

Switch 3:

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

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

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

Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 801

A network administrator is trying to identify a device that is having issues connecting to a switchport. Which of the following would BEST help identify the issue?

- A. A rack diagram
- B. The security log
- C. A syslog server
- D. Change management records

Answer: C (LEAVE A REPLY)

NEW QUESTION: 802

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 803

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

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

Answer: B ([LEAVE A REPLY](#))

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

NEW QUESTION: 804

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 following is MOST likely the cause of the issue?

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

Answer: A ([LEAVE A REPLY](#))

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: 805

Which of the following OSI model layers are responsible for handling packets from the sources to the destination and checking for errors? (Select two).

- A. Physical
- B. Session
- C. Data link
- D. Network
- E. Presentation
- F. Application

Answer: (SHOW ANSWER)

The data link and network layers are responsible for handling packets from the source to the destination and checking for errors. The data link layer is the second layer of the OSI model, which is a conceptual framework that describes how different network functions are organized and interact. The data link layer is responsible for providing reliable and efficient data transmission between two adjacent nodes on a network. The data link layer uses frames as its unit of data, and adds a header and a trailer to each frame that contain information such as source and destination MAC addresses, frame type, and error detection code. The data link layer can check for errors by using techniques such as parity check, checksum, or cyclic redundancy check (CRC). The network layer is the third layer of the OSI model, which is responsible for providing logical addressing and routing of packets across different networks. The network layer uses packets as its unit of data, and adds a header to each packet that contains information such as source and destination IP addresses, protocol type, and hop count. The network layer can check for errors by using techniques such as Internet Control Message Protocol (ICMP), which can send and receive error messages or diagnostic information. Reference: [CompTIA Network+ Certification Exam Objectives], Data Link Layer - an overview | ScienceDirect Topics, Network Layer - an overview | ScienceDirect Topics

NEW QUESTION: 806

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: A,B (LEAVE A REPLY)

* A MAC address is a unique identifier assigned to a network interface card (NIC) that allows it to communicate on a physical network layer, such as Ethernet1. An IP address is a logical identifier assigned to a device that allows it to communicate on a network layer, such as IP2.

* A technician can use different methods to find the IP address of a device if they know its MAC address.

Two of the most common methods are looking at the ARP table and the DHCP leases.

* The ARP table is a data structure that stores the mappings between IP addresses and MAC addresses on a device. ARP stands for Address Resolution Protocol, which is a network protocol that enables devices to discover the MAC address of another device based on its IP address3. The ARP table is populated by sending ARP requests and receiving ARP replies, or by using static ARP entries that are manually configured4.

* A technician can look at the ARP table of their own device or a nearby device, such as a router or a switch, to find the IP address of a device with a known MAC address. For example, on a Windows device, the technician can use the command `arp -a` to display the ARP table, and look for the entry that matches the MAC address. On a Cisco device, the technician can use the command `show ip arp` to display the ARP table, and look for the entry that matches the MAC address.

* The DHCP leases are the records of the IP addresses that are assigned by a DHCP server to DHCP clients. DHCP stands for Dynamic Host Configuration Protocol, which is a network protocol that enables devices to obtain IP addresses and other network configuration parameters automatically from a DHCP server. The DHCP leases contain information such as the IP address, the MAC address, the lease duration, and the expiration time of each DHCP client.

* A technician can look at the DHCP leases of the DHCP server that serves the network segment where the device with the known MAC address is connected. For example, on a Windows DHCP server, the technician can use the DHCP console to view the DHCP leases, and look for the entry that matches the MAC address. On a Cisco DHCP server, the technician can use the command `show ip dhcp binding` to view the DHCP leases, and look for the entry that matches the MAC address.

* The other options are incorrect for the following reasons:

* C. IP route table is a data structure that stores the routes to different network destinations on a device. It does not store the MAC addresses of the devices on the network.

* D. DNS cache is a data structure that stores the mappings between domain names and IP addresses on a device. DNS stands for Domain Name System, which is a network service that translates human-readable domain names into IP addresses. It does not store the MAC addresses of the devices on the network.

* E. MAC address table is a data structure that stores the mappings between MAC addresses and switch ports on a switch. It does not store the IP addresses of the devices on the network.

* F. STP topology is a network design that uses the Spanning Tree Protocol (STP) to prevent loops and create a loop-free logical topology on a switched network. It does not store the IP addresses or the MAC addresses of the devices on the network. References:

* 1: MAC address - Wikipedia

* 2: IP address - Wikipedia

* 3: Address Resolution Protocol - Wikipedia

* 4: How ARP Works

* : How to Use the Arp Command in Windows

* : `show ip arp`

* : Dynamic Host Configuration Protocol - Wikipedia

* : DHCP Lease

* : View DHCP Leases

* : `show ip dhcp binding`

* : Routing table - Wikipedia

* : Domain Name System - Wikipedia

* : DNS cache - Wikipedia

* : MAC address table - Wikipedia

* : Spanning Tree Protocol - Wikipedia

NEW QUESTION: 807

A network administrator wants to improve the security of the management console on the company's switches and ensure configuration changes made can be correlated to the administrator who conformed them Which of the following should the network administrator implement?

- A. Port security
- B. Local authentication
- C. TACACS+
- D. Access control list

Answer: (SHOW ANSWER)

TACACS+ is a protocol that provides centralized authentication, authorization, and accounting (AAA) for network devices and users. TACACS+ can help improve the security of the management console on the company's switches by verifying the identity and credentials of the administrators, enforcing granular access policies and permissions, and logging the configuration changes made by each administrator. This way, the network administrator can ensure only authorized and authenticated users can access and modify the switch settings, and also track and correlate the changes made by each user. Reference: <https://www.comptia.org/blog/what-is-tacacs>

NEW QUESTION: 808

Which of the following ports is used for secure email?

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

Answer: D (LEAVE A REPLY)

Port 587 is typically used for secure email submission, specifically for sending emails securely using the SMTP (Simple Mail Transfer Protocol) with TLS (Transport Layer Security) or SSL (Secure Sockets Layer) encryption. It's commonly used as an alternative to port 25 for secure mail submission by mail clients or applications.

NEW QUESTION: 809

Which of the following describes a situation in which an employee knowingly allows someone access to a restricted area without verifying authentication?

- A. Piggybacking
- B. Tailgating
- C. Shoulder surfing
- D. Phishing

Answer: B (LEAVE A REPLY)

The situation in which an employee knowingly allows someone access to a restricted area without verifying authentication is called Tailgating. Here's why:

Piggybacking (Option A) refers to an unauthorized person following an authorized person into a secure area without their knowledge.

Shoulder surfing (Option C) involves someone observing sensitive information (such as passwords) by looking over another person's shoulder.

Phishing (Option D) is a form of social engineering where attackers deceive individuals into revealing confidential information.

Therefore, the correct answer is B. Tailgating

NEW QUESTION: 810

A network administrator is configuring a new switch and wants to connect two ports to the core switch to ensure redundancy. Which of the following configurations would meet this requirement?

- A. Full duplex
- B. 802.1Q tagging
- C. Native VLAN
- D. Link aggregation

Answer: (SHOW ANSWER)

Link aggregation is a technique that allows multiple physical ports to be combined into a single logical channel, which provides increased bandwidth, load balancing, and redundancy. Link aggregation can be configured using protocols such as Link Aggregation Control Protocol (LACP) or static methods.

References

- * Link aggregation is one of the common Ethernet switching features covered in Objective 2.3 of the
- * CompTIA Network+ N10-008 certification exam¹.
- * Link aggregation can be used to connect two ports to the core switch to ensure redundancy²³.
- * Link aggregation can be configured using LACP or static methods²³.

1: CompTIA Network+ Certification Exam Objectives, page 5 2: Interface Configurations - N10-008 CompTIA Network+ : 2.3 3: CompTIA Network+ N10-008 Cert Guide, Chapter 11, page 323

NEW QUESTION: 811

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: (SHOW ANSWER)

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>

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 812

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

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

Answer: B (LEAVE A REPLY)

A screened subnet is a network segment that is isolated from both the internal and external networks by firewalls or routers. It is used to host publicly accessible servers that need some protection from external attacks, but also need to be separated from the internal network for security reasons.

References

- * 1: Seven-Second Subnetting - N10-008 CompTIA Network+ : 1.4
- * 2: CompTIA Network+ Study Guide: Exam N10-008, 5th Edition, page 56
- * 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 22

NEW QUESTION: 813

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

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

Answer: (SHOW ANSWER)

Single-mode fiber is a type of optical fiber that has a small core diameter and allows only one mode of light to propagate. This reduces signal attenuation and increases transmission distance, making it suitable for long-distance communication networks. Single-mode fiber can carry data over thousands of kilometers without requiring repeaters or amplifiers. Single-mode fiber is also immune to electromagnetic interference and has a higher bandwidth than multimode fiber. Therefore, single-mode fiber is the best cable type for connecting sites on multiple continents. References: [CompTIA Network+ Certification Exam Objectives], [Single-mode optical fiber - Wikipedia]

Single-mode fiber optic cable uses a single ray of light to transmit data. This allows it to achieve very low attenuation and high bandwidth.

Multimode fiber optic cable uses multiple rays of light to transmit data. This results in higher attenuation and lower bandwidth than single-mode cable.

Twisted pair copper cable uses two insulated copper wires to transmit data. It is less expensive than fiber optic cable, but it has higher attenuation and lower bandwidth.

When choosing a cable type for a long-distance application, it is important to consider the following factors:

- * Attenuation: The amount of signal loss that occurs over the length of the cable.

- * Bandwidth: The amount of data that can be transmitted over the cable per second.

- * Cost: The cost of the cable and installation.

Single-mode fiber optic cable is the best choice for long-distance applications because it has the lowest attenuation and highest bandwidth of any cable type. However, it is also the most expensive cable type.

NEW QUESTION: 814

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

A. NIC teaming

B. Load balancer

C. RAID array

D. PDUs

Answer: [\(SHOW ANSWER\)](#)

NIC teaming, also known as network interface card teaming or link aggregation, allows multiple network interface cards to be grouped together to provide redundancy and increased throughput. In the event of a port failure on a switch, NIC teaming ensures that the file server remains connected to the LAN by automatically switching to another network interface card.

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

NEW QUESTION: 815

Which of the following is a hybrid routing protocol?

A. BGP

B. EIGRP

C. RIPv2

D. OSPF

Answer: **B** [\(LEAVE A REPLY\)](#)

NEW QUESTION: 816

The power company notifies a network administrator that it will be turning off the power to the building over the weekend. Which of the following is the BEST solution to prevent the servers from going down?

A. Generator

B. Redundant power supplies

C. Power distribution unit

D. Uninterruptible power supply

Answer: B (LEAVE A REPLY)

NEW QUESTION: 817

A network administrator is in the process of installing a new broadband circuit. The administrator assigns the new static IP address with a /30 prefix. However, the administrator is unable to connect to the internet. Given the following information:

IP address: 4.11.17.6

Subnet mask: 255.255.255.252

Default gateway: 4.11.17.1

DNS1: 1.1.1.1

DNS2: 8.8.8.8

Which of the following is the most likely cause?

A. Routing table

B. Subnet mask

C. DNS

D. Default gateway

Answer: D (LEAVE A REPLY)

The most likely cause of the administrator's inability to connect to the internet is the incorrect default gateway. The default gateway is the IP address of the router that connects the local network to the internet. The default gateway should be in the same subnet as the IP address of the device. However, in this case, the IP address of the device is 4.11.17.6 and the subnet mask is 255.255.255.252, which means the subnet has only four addresses: 4.11.17.4, 4.11.17.5, 4.11.17.6, and 4.11.17.7. The first and the last addresses are reserved for the network and the broadcast, respectively, so the only valid addresses for the device and the gateway are 4.11.17.5 and 4.11.17.6. Therefore, the default gateway should be 4.11.17.5, not 4.11.17.1, which is in a different subnet. The routing table, the subnet mask, and the DNS are not the causes of the problem, as they are either correct or irrelevant for the internet connectivity.

Reference

1: CompTIA Network+ N10-008 Certification Study Guide, page 83-84

2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 8

3: CompTIA Network+ N10-008 Certification Practice Test, question 3

NEW QUESTION: 818

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, the administrator sees the 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 3
- B. Rule 4
- C. Rule 1
- D. Rule 2

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 819

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

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

Answer: A ([LEAVE A REPLY](#))

Wireless Client Isolation is a security feature that prevents wireless clients from communicating with one another. This feature is useful for guest and BYOD SSIDs adding a level of security to limit attacks and threats between devices connected to the wireless networks.

NEW QUESTION: 820

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

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

Answer: C ([LEAVE A REPLY](#))

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

NEW QUESTION: 821

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

- A. TXT
- B. NS
- C. SOA

D. CNAME

Answer: D (LEAVE A REPLY)

NEW QUESTION: 822

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

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

Answer: B (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 823

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 (LEAVE A REPLY)

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: 824

A company that uses VoIP telephones is experiencing intermittent issues with one-way audio and dropped conversations. The manufacturer says the system will work if ping times are less than 50ms. The company has recorded the following ping times:

Which of the following is MOST likely causing the issue?

- A. Attenuation
- B. Latency
- C. VLAN mismatch
- D. Jitter

Answer: D (LEAVE A REPLY)

Jitter is most likely causing the issue of intermittent one-way audio and dropped conversations for the company that uses VoIP telephones. Jitter is a variation in delay of packets arriving at the destination. It can cause choppy or distorted audio quality for VoIP applications, especially over WAN links that have limited bandwidth and high latency. The recommended jitter for VoIP is less than 10ms¹. The company has recorded ping times that exceed 50ms, which indicates high jitter and latency on their network. Reference: <https://www.voip-info.org/voip-jitter/> 1

NEW QUESTION: 825

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

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

Answer: B (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 826

A firewall administrator observes log entries of traffic being allowed to a web server on port 80 and port 443. The policy for this server is to only allow traffic on port 443. The firewall administrator needs to investigate how this change occurred to prevent a recurrence. Which of the following should the firewall administrator do next?

- A. Consult the firewall audit logs.
- B. Change the policy to allow port 80.
- C. Remove the server object from the firewall policy.
- D. Check the network baseline.

Answer: A ([LEAVE A REPLY](#))

Firewall audit logs are records of the changes made to the firewall configuration, policies, and rules. They can help the firewall administrator to track who, when, and what changes were made to the firewall, and identify any unauthorized or erroneous modifications that could cause security issues or network outages. By consulting the firewall audit logs, the firewall administrator can investigate how the change that allowed traffic on port 80 to the web server occurred, and prevent it from happening again

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 827

Which of the following factors should be considered when evaluating a firewall to protect a datacenter's east-west traffic?

- A. Replication traffic between an on-premises server and a remote backup facility
- B. Traffic between VMs running on different hosts
- C. Concurrent connections generated by Internet DDoS attacks
- D. VPN traffic from remote offices to the datacenter's VMs

Answer: B ([LEAVE A REPLY](#))

Traffic flows within a datacenter typically occur within the framework of one of two models: East- West or North-South. The names may not be the most intuitive, but the East-West traffic model means that data is flowing among devices within a specific datacenter while North-South means that data is flowing into the datacenter (from a system physically outside the datacenter) or out of it (to a system physically outside the datacenter).

NEW QUESTION: 828

A network technician is installing an analog desk phone for a new receptionist After running a new phone line, the technician now needs to connect on a new connector. Which of the following connectors would MOST likely be used in this case?

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 829

A disaster recovery team needs a solution that would best meet the following requirements:

- The server infrastructure has been pre-installed

- The fail-over location offers basic life support.
- The fail-over location provides basic network connectivity.
- Minimizing cost is preferred over quicker business recovery times
- The expected time for services to be fully operational is days.

Which of the following sites would meet the requirements?

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

Answer: C ([LEAVE A REPLY](#))

A warm site is a scaled-down version of a hot site. The recovery site is often only configured with power, phone, and network jacks. It may have computers and other resources, but they are not configured and ready to go.

- You bring the hardware, software, data
- A second site in the event of a disaster
- Doesn't mirror all live data

NEW QUESTION: 830

A network engineer has added a new route on a border router and is trying to determine if traffic is using the new route. Which of the following commands should the engineer use?

- A. ping
- B. arp
- C. route
- D. trace

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 831

SIMULATION

You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

The SSIDs need to be configured as CorpNet with a key of S3cr3t!

The wireless signals should not interfere with each other

The subnet the Access Points and switch are on should only support 30 devices maximum

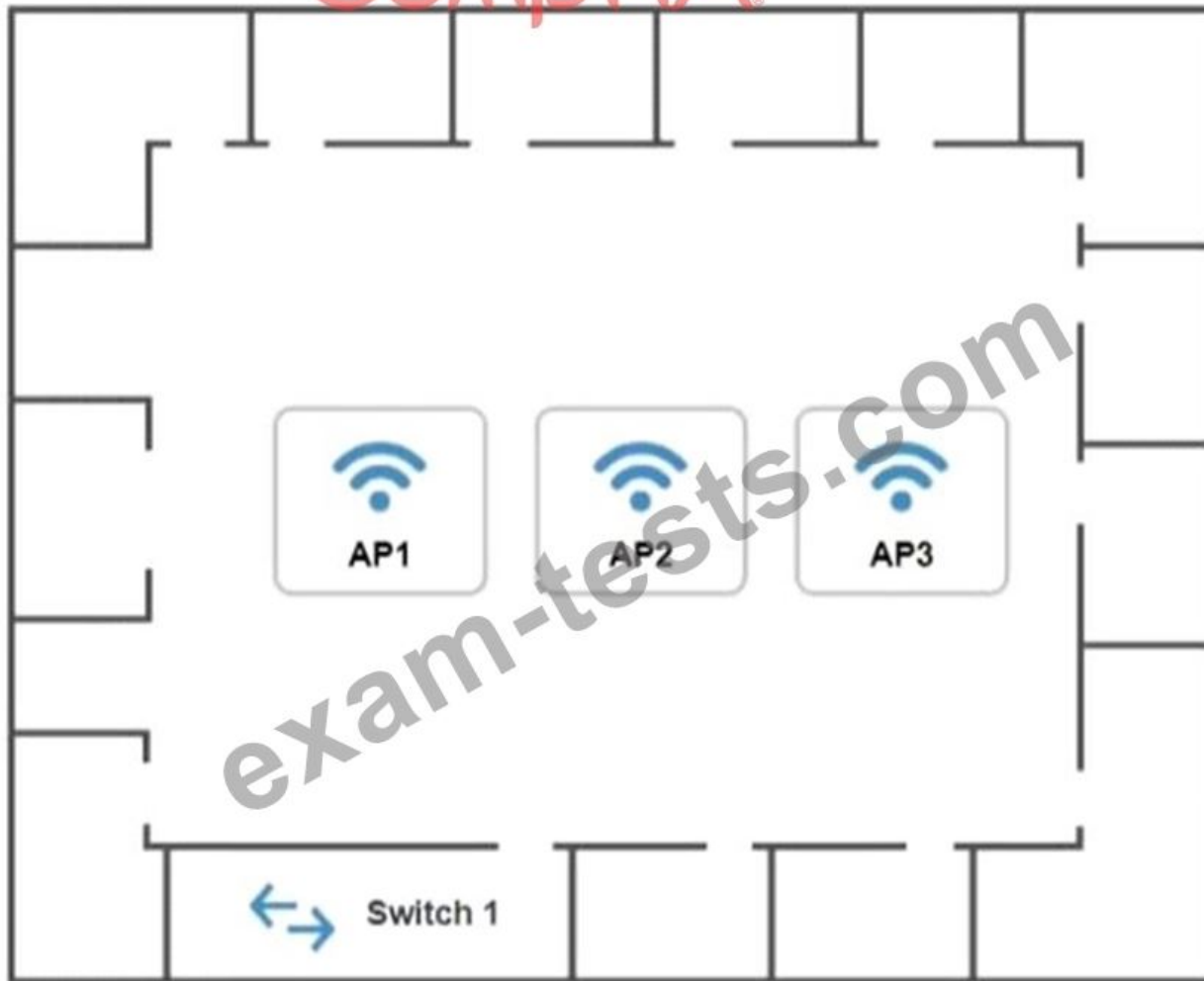
The Access Points should be configured to only support TKIP clients at a maximum speed

INSTRUCTIONS

Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

CompTIA



192.168.1.2
Speed: Auto
Duplex: Auto

AP1 Configuration

https://ap1.setup.do

Basic Configuration

Access Point Name

AP1

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes

☐ No

Wireless

Mode

B

G

Channel

Wired

Speed

☐ Auto

☒ 100

☐ 1000

Duplex

☐ Auto

☐ Half

☒ Full

Security Configuration

Security Settings

☒ None

☐ WEP

☐ WPA

☐ WPA2

☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

AP2 Configuration



https://ap2.setup.do

Basic Configuration

Access Point Name

AP2

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B
G

Channel

1
2
3
4
5
6
7
8
9
10
11

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name: AP3

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode:
 B
 G

Channel:
 1
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11

Wired

Speed: ☐ Auto ☒ 100 ☐ 1000

Duplex: ☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings: ☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase:

Answer:

On the first exhibit, the layout should be as follows

Access Point Name AP1

IP Address 192.168.1.3

Gateway 192.168.1.2

SSID corpnet

SSID Broadcast yes
Mode G
Channel 1
Speed Auto
Duplex Auto
WPA
Passphrase S3cr3t!
Exhibit 2 as follows
Access Point Name AP2
IP Address 192.168.1.4
Gateway 192.168.1.2
SSID corpnet
SSID Broadcast yes
Mode G
Channel 6
Speed Auto
Duplex Auto
WPA
Passphrase S3cr3t!
Exhibit 3 as follows
Access Point Name AP3
IP Address 192.168.1.5
Gateway 192.168.1.2
SSID corpnet
SSID Broadcast yes
Mode G
Channel 11
Speed Auto
Duplex Auto
WPA
Passphrase S3cr3t!

NEW QUESTION: 832

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

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 833

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

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

Answer: (SHOW ANSWER)

A default gateway is a device that routes traffic from one network to another network, such as the Internet. A default gateway is usually configured on each host device to specify the IP address of the router that connects the host's network to other networks. In this case, the user's device and the destination device are on different networks (192.168.1.0/24 and 192.168.2.0/24), so the user needs to configure a default gateway on their device to reach the destination device. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

<https://www.techopedia.com/definition/25761/default-gateway>

NEW QUESTION: 834

A network administrator is in the process of installing a new broadband circuit. The administrator assigns the new static IP address with a /30 prefix. However, the administrator is unable to connect to the internet. Given the following information:

IP address: 4.11.17.6

Subnet mask: 255.255.255.252

Default gateway: 4.11.17.1

DNS1: 1.1.1.1

DNS2: 8.8.8.8

Which of the following is the most likely cause?

- A. Routing table
- B. Subnet mask
- C. DNS
- D. Default gateway

Answer: (SHOW ANSWER)

The most likely cause of the administrator's inability to connect to the internet is the incorrect default gateway. The default gateway is the IP address of the router that connects the local network to the internet. The default gateway should be in the same subnet as the IP address of the device. However, in this case, the IP address of the device is 4.11.17.6 and the subnet mask is 255.255.255.252, which means the subnet has only four addresses: 4.11.17.4, 4.11.17.5, 4.11.17.6, and 4.11.17.7. The first and the last addresses are reserved for the network and the broadcast, respectively, so the only valid addresses for the device and the gateway are 4.11.17.5 and 4.11.17.6. Therefore, the default gateway should be 4.11.17.5, not 4.11.17.1, which is in a different subnet. The routing table, the subnet mask, and the DNS are not the causes of the problem, as they are either correct or irrelevant for the internet connectivity.

References

- * 1: CompTIA Network+ N10-008 Certification Study Guide, page 83-84
- * 2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 8
- * 3: CompTIA Network+ N10-008 Certification Practice Test, question 3

NEW QUESTION: 835

A technician is documenting an application that is installed on a server and needs to verify all existing web and database connections to the server. Which of the following tools should the technician use to accomplish this task?

- A. ipconfig
- B. tracert
- C. nslookup
- D. netstat

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 836

Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

- A. Scope options
- B. Reservation
- C. Dynamic assignment
- D. Exclusion
- E. Static assignment

Answer: (SHOW ANSWER)

A reservation should be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP. A reservation is a feature of DHCP that allows an administrator to assign a fixed 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, even if it is powered off or disconnected from the network for a long time. Reference: <https://docs.microsoft.com/en-us/windows-server/troubleshoot/configure-dhcp-reservations>

NEW QUESTION: 837

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 ([LEAVE A REPLY](#))

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:

NEW QUESTION: 838

Which of the following would be used to forward requests and replies between a DHCP server and client?

- A. Relay
- B. Lease
- C. Scope
- D. Range

Answer: A (LEAVE A REPLY)

As DHCP messages are broadcast, these broadcast messages are not forwarded out of subnet by router to other subnets (Assuming that you have more than one subnet). It means you need to have a DHCP server for each of your subnet, which is not practical. The DHCP relay agent receives DHCP Discover and Request messages broadcasted by the PC, and unicasts them directly to the DHCP server. With each of your subnets configured with a relay agent, one DHCP server can cater to all the clients in different subnets.

NEW QUESTION: 839

A wireless network technician is receiving reports from some users who are unable to see both of the corporate SSIDs on their mobile devices. A site survey was recently commissioned, and the results verified acceptable RSSI from both APs in all user areas. The APs support modern wireless standards and are all broadcasting their SSIDs. The following table shows some of the current AP settings:

Name	Power	Directionality	Wireless standard	Authentication standard	SSID
AP1	Medium	Omnidirectional	802.11b	WPA2 - PSK	CORP01
AP2	High	Directional	802.11a	WPA2 - PSK	CORP02

Which of the following changes would result in all of the user devices being capable of seeing both corporate SSIDs?

- A. Implementing the WPA2 Enterprise authentication standard
- B. Implementing omnidirectional antennas for both APs
- C. Configuring the highest power settings for both APs
- D. Configuring both APs to use the 802.11ac wireless standard

Answer: D (LEAVE A REPLY)

Explanation

The change that would result in all of the user devices being capable of seeing both corporate SSIDs is configuring both APs to use the 802.11ac wireless standard. 802.11ac is a wireless standard that operates in the 5 GHz frequency band and offers high data rates and performance. However, not all wireless devices support 802.11ac, especially older ones that only operate in the 2.4 GHz frequency band. In the table, AP1 uses 802.11b, which is an outdated wireless standard that operates in the 2.4 GHz frequency band and offers low data rates and performance. AP2 uses 802.11a, which is an older wireless standard that operates in the 5 GHz frequency band and offers moderate data rates and performance. Therefore, some user devices may not be able to see both SSIDs because they are incompatible with either 802.11b or 802.11a. By configuring both APs to use

802.11ac, which is backward compatible with previous wireless standards, all user devices should be able to see both SSIDs. References: CompTIA Network+ N10-008 Certification Study Guide, page 75; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-18.

NEW QUESTION: 840

Which of the following cloud deployment models involves servers that are hosted at a company's property and are only used by that company?

- A. Public
- B. Private
- C. Hybrid
- D. Community

Answer: B (LEAVE A REPLY)

A private cloud deployment model involves servers that are hosted at a company's property and are only used by that company. A private cloud provides exclusive access and control over the cloud resources to the company, as well as higher security and privacy. However, a private cloud also requires more investment and maintenance from the company, compared to other cloud deployment models¹

NEW QUESTION: 841

An attacker is attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt. Which of the following attack types BEST describes this action?

- A. Pass-the-hash attack
- B. Rainbow table attack
- C. Brute-force attack
- D. Dictionary attack

Answer: D (LEAVE A REPLY)

Explanation

The attacker attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt is using a dictionary attack. References: CompTIA Network+ Certification Study Guide, Chapter 6: Network Attacks and Mitigation.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 842

In which of the following components do routing protocols belong in a software-defined network?

- A. Infrastructure layer

- B. Control layer
- C. Application layer
- D. Management plane

Answer: B (LEAVE A REPLY)

A software-defined network (SDN) is a network architecture that decouples the control plane from the data plane and centralizes the network intelligence in a software controller. The control plane is the part of the network that makes decisions about how to route traffic, while the data plane is the part of the network that forwards traffic based on the control plane's instructions. The control layer is the layer in an SDN that contains the controller and the routing protocols that communicate with the network devices. The control layer is responsible for managing and configuring the network devices and providing them with the necessary information to forward traffic.

Reference: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 378)

NEW QUESTION: 843

Which of the following would enable a network technician to implement dynamic routing?

- A. A hub
- B. A Layer 3 switch
- C. A bridge
- D. An IPS

Answer: (SHOW ANSWER)

NEW QUESTION: 844

Which of the following types of data center architectures will MOST likely be used in a large SDN and can be extended beyond the data center?

- A. iSCSI
- B. FCoE
- C. Three-tiered network
- D. Spine and leaf
- E. Top-of-rack switching

Answer: D (LEAVE A REPLY)

The type of data center architecture that will most likely be used in a large SDN and can be extended beyond the data center is spine and leaf. Spine and leaf is a network topology that consists of two layers of switches: spine switches and leaf switches. Spine switches are interconnected to each other and form the core of the network, while leaf switches are connected to each spine switch and form the access layer of the network. Spine and leaf topology provides high scalability, performance, and flexibility for data center networks, especially for SDN (Software Defined Networking) environments that require dynamic traffic flows and virtualization. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 16; The Official CompTIA Network+ Student Guide (Exam N10-008), page 1-9.

NEW QUESTION: 845

Which of the following connector types would have the MOST flexibility?

- A. SFP

- B. BNC
- C. LC
- D. RJ45

Answer: A (LEAVE A REPLY)

SFP is a transceiver that allows for modular connection based on whatever is needed.

Example = Converting RJ45 to SC (copper to fiber), vice versa or some other combination needed.

NEW QUESTION: 846

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

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

Answer: D (LEAVE A REPLY)

NEW QUESTION: 847

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: (SHOW ANSWER)

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/13838-1>

NEW QUESTION: 848

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

- A. Link Aggregation Control Protocol
- B. Dynamic routing
- C. Quality of service
- D. Network load balancer

E. Static IP addresses

Answer: C (LEAVE A REPLY)

To improve performance for videoconferencing, the company should configure Quality of Service (QoS). This technology allows for the prioritization of network traffic, ensuring that videoconferencing traffic is given higher priority and therefore better performance. Link Aggregation Control Protocol (LACP), Dynamic routing, Network load balancer, and Static IP addresses are not directly related to improving performance for videoconferencing.

References:

* Network+ N10-007 Certification Exam Objectives, Objective 2.6: Given a scenario, implement and configure the appropriate wireless security and implement the appropriate QoS concepts.

NEW QUESTION: 849

A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the AP utilize?

- A. Omni
- B. Directional
- C. Yagi
- D. Parabolic

Answer: (SHOW ANSWER)

An omni antenna should be used by the AP to provide service in a radius surrounding a radio. An omni antenna is a type of antenna that has a 360-degree horizontal radiation pattern. It can provide wireless coverage in all directions from the antenna with varying degrees of vertical coverage. It is suitable for indoor environments where users are located around the AP¹. Reference: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html> 1

NEW QUESTION: 850

A network security engineer is investigating a potentially malicious insider on the network. The network security engineer would like to view all traffic coming from the user's PC to the switch without interrupting any traffic or having any downtime. Which of the following should the network security engineer do?

- A. Enable port mirroring.
- B. Implement dynamic ARP inspection.
- C. Configure 802.1Q.
- D. Turn on port security.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 851

A technician is troubleshooting a network switch that seems to stop responding to requests intermittently whenever the logging level is set for debugging. Which of the following metrics should the technician check to begin troubleshooting the issue?

- A. Audit logs
- B. CPU utilization
- C. CRC errors

D. Jitter

Answer: B ([LEAVE A REPLY](#))

CPU utilization is a metric that measures the percentage of time a CPU spends executing instructions. When the logging level is set for debugging, the router may generate a large amount of logging data, which can increase CPU utilization and cause the router to stop responding to requests intermittently. Reference:

Network+ N10-008 Objectives: 2.1 Given a scenario, troubleshoot common physical connectivity issues.

NEW QUESTION: 852

A technician replaces a customer's router, and is now unable to ping the ISP's gateway. Which of the following should the technician check?

- A.** The arp table of a network user.
- B.** The route table of the new customer's router.
- C.** The arp table of the new customer's router.
- D.** The route table of the next-hop router.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 853

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: ([SHOW ANSWER](#))

Explanation

802.11a/b/g/n/ac wireless networks operate in two frequency ranges: 2.4 GHz and 5 GHz. The 5 GHz frequency range supports more channels than the 2.4 GHz frequency range, making it a better choice for high-density wireless networks.

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

NEW QUESTION: 854

Which of the following should be implemented to allow remote users to access network resources while only redirecting necessary traffic?

- A.** Split-tunnel VPN
- B.** Geofencing
- C.** Client-to-site VPN
- D.** Remote desktop gateway

Answer: A ([LEAVE A REPLY](#))

A split-tunnel VPN is a VPN feature that allows remote users to access network resources while only redirecting necessary traffic through the VPN tunnel. A split-tunnel VPN enables users to choose which applications or

websites to secure with the VPN and which to connect normally through the internet. This can improve performance, conserve bandwidth, and avoid compatibility issues with some services that depend on the user's location. A split-tunnel VPN can also allow users to access local devices or resources that are not accessible through the VPN.

NEW QUESTION: 855

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.** Investigate for a client's disassociation caused by an evil twin AP
- D.** Confirm that a valid passphrase is being used during the web authentication

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 856

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: ([SHOW ANSWER](#)**)**

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

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com

N10-008 dumps with Test Engine here: <https://www.braindumps.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 857

A network administrator is checking to see if anything has changed. Which of the following steps of the troubleshooting methodology is involved?

- A. Identify the problem.
- B. Test the theory.
- C. Establish a theory.
- D. Document findings.

Answer: (SHOW ANSWER)

According to the CompTIA troubleshooting methodology¹, testing the theory is the step where the network administrator verifies if the problem is caused by a specific factor or change. This step involves checking the system logs, running diagnostic tools, or performing other tests to confirm or eliminate the possible cause.

Reference:

Troubleshooting Methodology | IT Support and Help Desk | CompTIA¹

NEW QUESTION: 858

Which of the following is the most cost-effective way for a network administrator to establish a persistent, secure connection between two facilities?

- A. Dedicated line
- B. Site-to-site VPN
- C. API gateway
- D. SSH tunnel

Answer: (SHOW ANSWER)

NEW QUESTION: 859

Which of the following is most closely associated with the management plane?

- A. Routing table
- B. Current configuration
- C. File operations
- D. Console port

Answer: B (LEAVE A REPLY)

The management plane is responsible for managing and controlling network devices. Let's evaluate the options:

Routing table: Part of the control plane, used for making forwarding decisions.

Current configuration: Part of the management plane. It includes settings, access control lists, and other configuration details.

File operations: Typically part of the management plane. It involves tasks like uploading/downloading configurations, firmware updates, and backups.

Console port: Also part of the management plane. It provides direct access to the device for configuration and troubleshooting.

Among the options, the one most closely associated with the management plane is the current configuration.

NEW QUESTION: 860

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

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

Answer: A ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 861

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

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

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

Answer: C ([LEAVE A REPLY](#))

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

NEW QUESTION: 862

Due to concerns around single points of failure, a company decided to add an additional WAN to the network. The company added a second MPLS vendor to the current MPLS WAN and deployed an additional WAN router

at each site. Both MPLS providers use OSPF on the WAN network, and EIGRP is run internally. The first site to go live with the new WAN is successful, but when the second site is activated significant network issues occur. Which of the following is the MOST likely cause for the WAN instability?

- A. A routing loop
- B. Asymmetrical routing
- C. A switching loop
- D. An incorrect IP address

Answer: ([SHOW ANSWER](#))

Asymmetrical routing is the most likely cause for the WAN instability. When two different routing protocols are used, like OSPF and EIGRP, it can cause asymmetrical routing, which results in traffic being routed differently in each direction. This can lead to instability in the WAN. A CDP neighbor change, a switching loop, or an incorrect IP address are not likely causes for WAN instability.

NEW QUESTION: 863

A user notifies a network administrator about losing access to a remote file server. The network administrator is able to ping the server and verifies the current firewall rules do not block access to the network fileshare.

Which of the following tools would help identify which ports are open on the remote file server?

- A. dig
- B. nmap
- C. tracer
- D. nslookup

Answer: ([SHOW ANSWER](#))

Explanation

nmap is the tool that would help identify which ports are open on the remote file server. nmap stands for Network Mapper, which is a free and open-source tool that can perform various network scanning and discovery tasks. nmap can help identify which ports are open on a remote device by sending probes or packets to different ports and analyzing the responses. nmap can also provide information about the operating system, services, versions, firewalls, or vulnerabilities of the remote device. nmap can be useful for network administrators, security professionals, or hackers to monitor, audit, or attack network devices. References:

[CompTIA Network+ Certification Exam Objectives], Nmap - Free Security Scanner For Network Exploration & Security Audits

NEW QUESTION: 864

Which of the following would be used to forward requests and replies between a DHCP server and client?

- A. Range
- B. Lease
- C. Scope
- D. Relay

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 865

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

- A. Polarization
- B. Channel utilization
- C. Channel bonding
- D. Antenna type
- E. MU-MIMO

Answer: D (LEAVE A REPLY)

The antenna type is the factor that would most likely facilitate the correct accessibility to the Wi-Fi network, as it determines the shape, direction, and range of the wireless signal¹². Different types of antennas have different characteristics, such as gain, beamwidth, and polarization, that affect how well they can cover a given area and overcome obstacles or interference¹². For example, an omnidirectional antenna can radiate the signal in all directions, while a directional antenna can focus the signal in a specific direction¹². By choosing the appropriate antenna type for the rented office space, the network administrator can ensure a sufficient signal and reduce exposure to the wireless network.

Polarization is the orientation of the electric field of the wireless signal, which can be either vertical, horizontal, or circular¹². Polarization affects the compatibility and performance of the wireless communication, as the transmitter and receiver antennas should have the same polarization to avoid signal loss¹². However, polarization alone would not facilitate the correct accessibility to the Wi-Fi network, as it depends on the antenna type and the environment¹².

Channel utilization is the measure of how much a wireless channel is occupied by data transmission, management frames, or control frames¹³. Channel utilization affects the efficiency and throughput of the wireless network, as a high channel utilization can indicate congestion, interference, or contention¹³. However, channel utilization alone would not facilitate the correct accessibility to the Wi-Fi network, as it depends on the network design, configuration, and demand¹³.

Channel bonding is the technique of combining two adjacent channels into one wider channel to increase the bandwidth and throughput of the wireless network¹. Channel bonding can improve the performance of the wireless network, especially for applications that require high data rates, such as video streaming¹. However, channel bonding alone would not facilitate the correct accessibility to the Wi-Fi network, as it also introduces some challenges, such as increased interference, reduced channel availability, and compatibility issues¹.

MU-MIMO (Multi-User Multiple Input Multiple Output) is a technology that allows a wireless access point to transmit data to multiple devices simultaneously using multiple antennas and spatial streams¹. MU-MIMO can enhance the capacity and efficiency of the wireless network, especially for high-density environments, such as offices, classrooms, or stadiums¹. However, MU-MIMO alone would not facilitate the correct accessibility to the Wi-Fi network, as it also requires some conditions, such as compatible devices, sufficient signal strength, and optimal antenna placement¹.

Reference:

1: CompTIA Network+ N10-008 Study Guide, Chapter 4: Wireless Technologies

2: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 42: Wireless Antennas

3: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 43: Wireless Troubleshooting

4: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 41: Wireless Channels

5: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 40: Wireless Technologies

NEW QUESTION: 866

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 (LEAVE A REPLY)

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. Reference: <https://www.securew2.com/blog/what-is-eap-tls> 1

NEW QUESTION: 867

Several employees have expressed concerns about the company monitoring their internet activity when they are working from home. The company wants to mitigate this issue and reassure employees that their private internet activity is not being monitored. Which of the following would satisfy company and employee needs?

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

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 868

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: ([SHOW ANSWER](#))

Link Aggregation Control Protocol (LACP) is implemented specifically to enable port aggregation (AKA NIC teaming).

NEW QUESTION: 869

An IT intern moved the location of a WAP from one conference room to another. The WAP was unable to boot following the move. Which of the following should be used to fix the issue?

- A.** Antenna
- B.** WLAN controller
- C.** Media converter
- D.** PoE injector

Answer: ([SHOW ANSWER](#))

A PoE injector is a device that provides power over Ethernet (PoE) to a WAP or other network device that does not have a built-in power supply. A PoE injector connects to a power outlet and an Ethernet cable, and sends both power and data to the WAP. If the WAP was moved to a location where there is no power outlet or PoE switch, it would need a PoE injector to boot up. References:

- * Part 3 of the current page talks about PoE and PoE injectors as a way to power WAPs.
- * [This article] explains how PoE injectors work and how to use them.

NEW QUESTION: 870

A technician is installing a new fiber connection to a network device in a datacenter. The connection from the device to the switch also traverses a patch panel connection. The chain of connections is in the following order:

- * Device
- * LC/LC patch cable
- * Patch panel
- * Cross-connect fiber cable
- * Patch panel
- * LC/LC patch cable
- * Switch

The connection is not working.

The technician has changed both patch cables with known working patch cables. The device had been tested and was working properly before being installed. Which of the following is the MOST likely cause of the issue?

- A.** TX/RX is reversed
- B.** An incorrect cable was used

- C. The device failed during installation
- D. Attenuation is occurring

Answer: A (LEAVE A REPLY)

It is a fiber network and fiber has insane range thus it is unlikely to be attenuation. Bad device and bad cable are out because they are explicitly tested as described. Therefore TX/RX is the only reasonable option.

NEW QUESTION: 871

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

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

Answer: A (LEAVE A REPLY)

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

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 872

A customer hired a network consultant to install a new wireless network with the following specifications:

2.4GHz

11Mbps

20MHz

Which of the following standards best fits these requirements?

- A. 802.11ac
- B. 802.11b
- C. 802.11g
- D. 802.11n

Answer: B (LEAVE A REPLY)

The 802.11b standard is a wireless networking protocol that operates in the 2.4GHz frequency band and supports a maximum data rate of 11Mbps. It uses a 20MHz channel width and a direct-sequence spread spectrum (DSSS) modulation technique². The 802.11b standard was released in 1999 and is backward compatible with the original 802.11 standard³. The other standards do not match the specifications given by the customer. 802.11ac operates in the 5GHz band and supports higher data rates up to 6.9Gbps. 802.11g also operates in the 2.4GHz band but supports data rates up to 54Mbps. 802.11n can operate in both 2.4GHz and 5GHz bands and supports data rates up to 600Mbps. It also uses a wider channel width of 40MHz and a multiple-input multiple-output (MIMO) technology³.

Reference

2 - 802.11 Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a - Lifewire

3 - Introduction to WLAN Frequency Bands | Engineering Education (EngEd ...

NEW QUESTION: 873

A network engineer is designing a secure communication link between two sites. The entire data stream needs to remain confidential. Which of the following will achieve this goal?

- A. GRE
- B. IKE
- C. ESP
- D. AH

Answer: C (LEAVE A REPLY)

ESP stands for Encapsulating Security Payload, and it is a protocol that provides confidentiality, integrity, and authentication for IP packets. ESP encrypts the payload of the IP packet, which contains the data stream, and adds a header and a trailer that contain security information. ESP can be used to create a secure communication link between two sites by using a VPN tunnel that protects the data stream from unauthorized access or modification. GRE stands for Generic Routing Encapsulation, and it is a protocol that encapsulates one network protocol inside another. GRE does not provide encryption or security by itself, but it can be combined with ESP or other protocols to create a secure VPN tunnel. IKE stands for Internet Key Exchange, and it is a protocol that negotiates and establishes security associations for IPsec, which is a suite of protocols that includes ESP and AH. IKE does not encrypt or protect the data stream, but it enables the secure exchange of keys and parameters for IPsec. AH stands for Authentication Header, and it is a protocol that provides integrity and authentication for IP packets. AH does not encrypt the payload of the IP packet, which means the data stream is not confidential. AH adds a header that contains security information and a checksum that verifies the integrity of the packet.

NEW QUESTION: 874

A company is opening a new building on the other side of its campus. The distance from the closest building to the new building is 1,804ft (550m). The company needs to connect the networking equipment in the new building to the other buildings on the campus without using a repeater. Which of the following transceivers should the company use?

- A. 10GBASE-SW
- B. 10GBASE-LR
- C. 10GBASE-LX4 over multimode fiber

D. 10GBASE-SR

Answer: B (LEAVE A REPLY)

Explanation

10GBASE-LR is a standard for 10 Gbps Ethernet over single-mode fiber optic cable. It can support a maximum distance of 6.2 miles (10 km), which is much longer than the distance between the buildings.

10GBASE-SW, 10GBASE-LX4, and 10GBASE-SR are all standards for 10 Gbps Ethernet over multimode fiber optic cable, which have shorter maximum distances ranging from 984ft (300m) to 1,312ft (400m).

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: 875

A network technician needs to use an RFC1918 IP space for a new office that only has a single public IP address. Which of the following subnets should the technician use for the LAN?

A. 10.10.10.0/24

B. 127.16.10.0/24

C. 174.16.10.0/24

D. 198.18.10.0/24

Answer: A (LEAVE A REPLY)

The RFC1918 IP space is a set of private IP addresses that are not routable on the public Internet and can be used for internal networks. The RFC1918 IP space consists of three ranges: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. Out of the four options, only A . 10.10.10.0/24 belongs to one of these ranges, specifically the 10.0.0.0/8 range. Therefore, the technician should use this subnet for the LAN.

Reference

1: https://en.wikipedia.org/wiki/Private_network

NEW QUESTION: 876

Which of the following functions is used to prioritize network traffic based on the type of traffic?

A. QoS

B. VPN

C. CDN

D. TTL

Answer: A (LEAVE A REPLY)

Explanation

QoS stands for Quality of Service, which is a feature that allows you to prioritize network traffic based on the type of traffic, such as voice, video, data, or gaming. QoS can help improve the performance and reliability of critical applications by allocating more bandwidth and lower latency to them, while reducing the impact of less important or non-essential traffic¹.

VPN stands for Virtual Private Network, which is a technology that creates a secure and encrypted connection between two or more devices over the Internet. VPN can help protect your privacy and data from hackers, ISPs, and government surveillance, as well as access geo-restricted content and services².

CDN stands for Content Delivery Network, which is a network of servers that deliver web content to users based on their geographic location, the origin of the content, and the performance of the network. CDN can help improve the speed and availability of web content, such as images, videos, and scripts, by caching them on servers closer to the users³.

TTL stands for Time To Live, which is a value that determines how long a packet can stay in a network before it is discarded or returned. TTL can help prevent network congestion and loops by limiting the lifespan of packets that are lost, corrupted, or delayed⁴.

NEW QUESTION: 877

A desktop support department has observed slow wireless speeds for a new line of laptops using the organization's standard image. No other devices have experienced the same issue. Which of the following should the network administrator recommend troubleshooting FIRST to resolve this issue?

- A.** Increasing wireless signal power
- B.** Installing a new WAP
- C.** Changing the protocol associated to the SSID
- D.** Updating the device wireless drivers

Answer: D ([LEAVE A REPLY](#))

Wireless drivers can affect the performance and compatibility of your wireless connection⁵. If only a new line of laptops using the organization's standard image has experienced slow wireless speeds, it could be that their wireless drivers are outdated or incompatible with the network. Updating the device wireless drivers could resolve this issue.

Wireless drivers play an important role in the performance of a wireless connection, as they control how the device interacts with the wireless network. If the laptops in question are using an outdated version of the wireless driver, it could be causing the slow speeds. The network administrator should recommend updating the device wireless drivers first to see if this resolves the issue.

NEW QUESTION: 878

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

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

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 879

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 ([LEAVE A REPLY](#))

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: 880

Which of the following diagnostic commands relies on proper forwarding of ICMP ECHO packets?

- A. nbstat
- B. ping
- C. ipconfig
- D. route

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 881

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 ([LEAVE A REPLY](#))

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: 882

An administrator is trying to retrieve management information from the network devices on their LAN. Which of the following monitoring resources provides the ability to collect this information encrypted over the network?

- A. IPSec
- B. VTP
- C. SNMPv3
- D. CDP

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 883

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

- A. Disabling unneeded switchports
- B. Securing SNMP
- C. MAC filtering
- D. Isolating the guest network

Answer: (SHOW ANSWER)

NEW QUESTION: 884

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 ([LEAVE A REPLY](#))

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://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

<https://cve.mitre.org/cve/>

NEW QUESTION: 885

Which of the following protocols can be routed?

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

Answer: C (LEAVE A REPLY)

iSCSI (Internet Small Computer System Interface) is a protocol that allows SCSI commands to be transported over IP networks1. iSCSI can be routed because it contains a network address and a device address, as required by a routable protocol2. iSCSI can be used to access block-level storage devices over a network, such as SAN (Storage Area Network).

FCoE (Fibre Channel over Ethernet) is a protocol that allows Fibre Channel frames to be encapsulated and transported over Ethernet networks1. FCoE cannot be routed because it does not contain a network address, only a device address. FCoE operates at the data link layer and requires special switches and adapters to support it. FCoE can also be used to access block-level storage devices over a network, such as SAN.

Fibre Channel is a protocol that provides high-speed and low-latency communication between servers and storage devices1. Fibre Channel cannot be routed because it does not use IP networks, but rather its own dedicated network infrastructure. Fibre Channel operates at the physical layer and the data link layer and requires special cables, switches, and adapters to support it. Fibre Channel can also be used to access block-level storage devices over a network, such as SAN.

NetBEUI (NetBIOS Extended User Interface) is an old protocol that provides session-level communication between devices on a local network1. NetBEUI cannot be routed because it does not contain a network address, only a device address. NetBEUI operates at the transport layer and relies on NetBIOS for name resolution. NetBEUI is obsolete and has been replaced by other protocols, such as TCP/IP.

NEW QUESTION: 886

A network engineer is installing hardware in a newly renovated data center. Major concerns that were addressed during the renovation included air circulation, building power redundancy, and the need for continuous monitoring. The network engineer IS creating alerts based on the following operation specifications:

AC input voltage	100 to 240VAC
AC maximum input current	<2.7A at 100V
Redundant power supply	Yes
Operating temperature	32–104°F (0–40°C)
Storage temperature	-4–149°F (-20–65°C)
Operating humidity	10–85%
Storage humidity	5–95%

Which of the following should the network engineer configure?

- A. Environmental monitoring alerts for humidity greater than 95%
- B. SIEM to parse syslog events for a failed power supply
- C. SNMP traps to report when the chassis temperature exceeds 95°F (3500)
- D. UPS monitoring to report when input voltage drops below 220VAC

Answer: C (LEAVE A REPLY)

Explanation

The alert that the network engineer should configure based on the operation specifications is SNMP traps to report when the chassis temperature exceeds 95°F (35°C). SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate their status and performance information to a central

management system, called an SNMP manager. SNMP traps are messages that are sent by network devices to notify the SNMP manager of an event or condition that requires attention, such as an error, a failure, or a threshold violation. In this case, the network engineer should configure SNMP traps on the network devices to send an alert when their chassis temperature exceeds 95°F (35°C), which is the maximum operating temperature specified in the table. This alert would help the network engineer monitor and troubleshoot any overheating issues that could affect the network performance or availability. References: CompTIA Network+ N10-008 Certification Study Guide, page 228; The Official CompTIA Network+ Student Guide (Exam N10-008), page 8-11.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 887

A Chief Information Officer (CIO) wants to improve the availability of a company's SQL database Which of the following technologies should be utilized to achieve maximum availability?

- A. Clustering
- B. Port aggregation
- C. NIC teaming
- D. Snapshots

Answer: A (LEAVE A REPLY)

Clustering is a technique that involves grouping multiple servers or instances together to provide high availability and fault tolerance for a database. Clustering can help improve the availability of a SQL database by allowing automatic failover and load balancing between the cluster nodes. If one node fails or becomes overloaded, another node can take over the database operations without disrupting the service. Reference: <https://www.educba.com/sql-cluster/>

NEW QUESTION: 888

A company hired a technician to find all the devices connected within a network. Which of the following software tools would BEST assist the technician in completing this task?

- A. IP scanner
- B. Terminal emulator
- C. NetFlow analyzer
- D. Port scanner

Answer: A (LEAVE A REPLY)

To find all devices connected within a network, a technician can use an IP scanner. An IP scanner sends a ping request to all IP addresses within a specified range and then identifies the active devices that respond to the request.

NEW QUESTION: 889

A technician, Joe, visits a site that has reported a network down emergency. He immediately reboots the switches and the router since the network is down. Which of the following network troubleshooting methodology steps should Joe have performed FIRST?

- A. Once a theory is confirmed determine the next step is to resolve the problem
- B. Determine if anything has changed
- C. Question the obvious
- D. Implement the solution or escalate as necessary

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 890

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: (SHOW ANSWER)

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: 891

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

- A. WLAN controller

- B. Cable modem
- C. Load balancer
- D. Switch
- E. Hub

Answer: D ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 892

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

Linux computer details:

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

Switch mirror port details:

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

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

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 893

An organization wants to perform maintenance on any of its web servers without affecting the service availability during a scheduled change window. Which of the following network devices would be required to provide this functionality?

- A. Router
- B. Forward proxy
- C. Load balancer
- D. Firewall

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 894

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 100MB speed
- D. Full duplex and 100MB speed

Answer: B (LEAVE A REPLY)

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: 895

According to troubleshooting methodology, which of the following should the technician do NEXT after determining the most likely probable cause of an issue?

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 896

A network technician is installing an analog desk phone for a new receptionist. After running a new phone line, the technician now needs to connect a new connector. Which of the following connectors would MOST likely be used in this case?

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

Answer: B ([LEAVE A REPLY](#))

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

<https://www.comptia.org/blog/what-is-rj11>

NEW QUESTION: 897

Which of the following WAN transmission mediums is the fastest and can travel the longest distance?

- A. Satellite
- B. Copper
- C. Wireless
- D. Fiber

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 898

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

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

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

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

Answer: D ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 899

An engineer is designing a network topology for a company that maintains a large on-premises private cloud. A design requirement mandates internet-facing hosts to be partitioned off from the internal LAN and internal server IP ranges. Which of the following defense strategies helps meet this requirement?

- A. Implementing a screened subnet
- B. Deploying a honeypot
- C. Utilizing network access control
- D. Enforcing a Zero Trust model

Answer: ([SHOW ANSWER](#))

Explanation

A screened subnet is a network topology that uses two firewalls to isolate a segment of the network from both the internal LAN and the internet. The screened subnet, also known as a demilitarized zone (DMZ), hosts the internet-facing servers that need to be accessible from outside the network, such as web servers, mail servers, or DNS servers. The first firewall, also known as the external firewall, filters the traffic between the internet and the DMZ, allowing only the necessary ports and protocols to pass through. The second firewall, also known as the internal firewall, filters the traffic between the DMZ and the internal LAN, allowing only authorized and secure connections to access the internal resources. This way, the screened subnet provides a layer of protection for both the internet-facing hosts and the internal LAN from potential attacks¹².

The other options are not defense strategies that help meet the design requirement of partitioning off the internet-facing hosts from the internal LAN and internal server IP ranges. Deploying a honeypot is a deception technique that lures attackers to a fake system or network that mimics the real one, in order to monitor their activities and collect information about their methods and motives. However, a honeypot does not isolate or protect the internet-facing hosts from the rest of the network³. Utilizing network access control is a security method that enforces policies on who or what can access the network resources, based on factors such as identity, role, device type, location, or time. However, network access control does not create a separate segment for the internet-facing hosts from the internal LAN. Enforcing a Zero Trust model is a security paradigm that assumes no trust for any entity inside or outside the network, and requires continuous verification and validation of every request and transaction. However, a Zero Trust model does not necessarily imply a specific network topology or architecture for separating the internet-facing hosts from the internal LAN.

NEW QUESTION: 900

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 for the VPN connection.

Which of the following will MOST likely point to the root cause of the issue?

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 901

An organization recently connected a new computer to the LAN. The user is unable to ping the default gateway.

Which of the following is the most likely cause?

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

Answer: A ([LEAVE A REPLY](#))

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

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!
BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 902

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

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

Answer: B,F (LEAVE A REPLY)

NEW QUESTION: 903

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 (LEAVE A REPLY)

The question describes a scenario where a student can connect to the campus Wi-Fi with a laptop, but not with a phone, even when they are close to each other.

This suggests that the problem is not related to the transmission speed, channel overlap, or antenna cable attenuation/signal loss, as these factors would affect both devices equally.

The most likely cause of this connection failure is that the student entered the incorrect passphrase on the phone, or the phone has a different security configuration than the laptop.

To verify this, the student should check the Wi-Fi settings on the phone and make sure they match the laptop's settings, such as the SSID, security type, and passphrase.

If the phone still cannot connect, the student should contact the network administrator or the Wi-Fi service provider for assistance. Reference:

CompTIA Network+ N10-008 Study Guide, Chapter 3, Section 3.1, Wireless Network Standards and Encryption, page 1251 Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 3.1, Wireless Network Standards and Encryption, page 192 Professor Messer's CompTIA N10-008 Network+ Training Course, Video 3.1 - Wireless Network Standards and Encryption, 12:00 - 13:003

NEW QUESTION: 904

An engineer needs to restrict the database servers that are in the same subnet from communicating with each other. The database servers will still need to communicate with the application servers in a different subnet. In some cases, the database servers will be clustered, and the servers will need to communicate with other cluster members. Which of the following technologies will be BEST to use to implement this filtering without creating rules?

- A. Private VLANs
- B. Access control lists
- C. Firewalls
- D. Control plane policing

Answer: A (LEAVE A REPLY)

Explanation

"Use private VLANs: Also known as port isolation, creating a private VLAN is a method of restricting switch ports (now called private ports) so that they can communicate only with a particular uplink. The private VLAN usually has numerous private ports and only one uplink, which is usually connected to a router, or firewall."

NEW QUESTION: 905

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

- A. Data link
- B. Network
- C. Transport

D. Session

Answer: A ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 906

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 ([LEAVE A REPLY](#))

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: 907

A network engineer is troubleshooting application connectivity issues between a server and a client. The network engineer needs to view the certificate exchange between the two hosts. Which of the following tools should the network engineer use?

- A.** dig
- B.** tcpdump
- C.** nmap
- D.** traceroute

Answer: ([SHOW ANSWER](#))

tcpdump is a tool that can capture and analyze network traffic, including the certificate exchange between two hosts. It can display the contents of packets, such as the SSL/TLS handshake, which involves the exchange of certificates. dig is a tool that can query DNS servers for domain name information. nmap is a tool that can scan ports and services on a network. traceroute is a tool that can show the path and hops between a source and a destination.

NEW QUESTION: 908

A user is tricked into providing log-in credentials to an attacker over the telephone. Which of the following attacks is this an example of?

- A. Shoulder surfing
- B. Tailgating
- C. Phishing
- D. Dumpster diving

Answer: C (LEAVE A REPLY)

Explanation

Phishing is a type of social engineering attack that uses email, phone, SMS, or other forms of personal communication to trick users into revealing sensitive information, such as log-in credentials, to an attacker. In this case, the user was deceived by a phone call that pretended to be from a legitimate source and asked for their log-in details.



Social engineering

NEW QUESTION: 909

A network administrator is preparing new switches that will be deployed to support a network extension project. The lead network engineer has already provided documentation to ensure the switches are set up properly Which of the following did the engineer most likely provide?

- A. Physical network diagram
- B. Site survey reports
- C. Baseline configurations
- D. Logical network diagram

Answer: C (LEAVE A REPLY)

Baseline configurations are the standard settings and parameters that are applied to network devices, such as switches, routers, firewalls, etc., to ensure consistent performance, security, and functionality across the network. Baseline configurations can include aspects such as IP addresses, VLANs, passwords, protocols, access lists, firmware versions, etc. Baseline configurations are usually documented and updated regularly to reflect any changes or modifications made to the network devices.

The lead network engineer most likely provided baseline configurations to the network administrator to ensure that the new switches are set up properly and in accordance with the network design and policies. Baseline configurations can help to simplify the deployment process, reduce errors and inconsistencies, and facilitate troubleshooting and maintenance.

The other options are not correct because they are not the most likely documentation that the lead network engineer provided to the network administrator. They are:

Physical network diagram. A physical network diagram is a graphical representation of the physical layout and connections of the network devices and components, such as cables, ports, switches, routers, servers, etc. A physical network diagram can help to visualize the network topology, identify the locations and distances of the devices, and plan for cabling and power requirements. However, a physical network diagram does not provide the specific settings and parameters that need to be configured on the network devices, such as the switches.

Site survey reports. A site survey report is a document that summarizes the findings and recommendations of a site survey, which is a process of assessing the suitability and readiness of a location for installing and operating network devices and components. A site survey report can include aspects such as environmental conditions, power and cooling availability, security and safety measures, interference and noise sources, signal coverage and quality, etc. A site survey report can help to identify and resolve any potential issues or challenges that may affect the network performance and reliability. However, a site survey report does not provide the specific settings and parameters that need to be configured on the network devices, such as the switches.

Logical network diagram. A logical network diagram is a graphical representation of the logical structure and functionality of the network devices and components, such as subnets, IP addresses, VLANs, protocols, routing, firewall rules, etc. A logical network diagram can help to understand the network design, architecture, and policies, as well as the data flow and communication paths between the devices. However, a logical network diagram does not provide the specific settings and parameters that need to be configured on the network devices, such as the switches.

Reference 1: Network+ (Plus) Certification | CompTIA IT Certifications 2: What is a Baseline Configuration? - Definition from Techopedia 3: What is a Physical Network Diagram? - Definition from Techopedia 4: What is a Site Survey? - Definition from Techopedia 5: [What is a Logical Network Diagram? - Definition from Techopedia]

NEW QUESTION: 910

An IP camera has a failed PoE NIC. This is the third time in months that a PoE NIC has failed on this device. The technician suspects a possible power issue. Which of the following should be used to test the theory?

- A. Loopback plug
- B. Multimeter
- C. Toner probe
- D. Protocol analyzer

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 911

A network technician crimped a length of RJ45 with TIA/EIA-568A on one end and TIA-EIA-568B on the other. Which of the following cable types did the technician create?

- A. Crossover cable
- B. Patch cable
- C. Twinaxial cable
- D. Rollover cable

Answer: ([SHOW ANSWER](#))

The cable type that the technician created is a crossover cable. A crossover cable is a type of twisted-pair cable that has the transmit and receive pairs reversed on one end. A crossover cable is used to connect two devices of

the same type, such as two switches or two computers, without using a hub or a switch. A crossover cable can be made by crimping one end of the cable with TIA/EIA-568A standard and the other end with TIA/EIA-568B standard, or vice versa. These standards define the color coding and pin assignments for RJ-45 connectors on twisted-pair cables. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 53; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-4.

NEW QUESTION: 912

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 (LEAVE A REPLY)

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/c>

NEW QUESTION: 913

A network technician needs to correlate security events to analyze a suspected intrusion. Which of the following should the technician use?

- A. SNMP
- B. SIEM
- C. Log review
- D. Vulnerability scanning

Answer: (SHOW ANSWER)

NEW QUESTION: 914

A network device is configured to send critical events to a syslog server; however, the following alerts are not being received:

Severity 5 LINK-UPDOWN: Interface 1/1, changed state to down

Severity 5 LINK-UPDOWN: Interface 1/3, changed state to down

Which of the following describes the reason why the events are not being received?

- A. The network device is not configured to log that level to the syslog server
- B. The network device was down and could not send the event

- C. The syslog server is not compatible with the network device
- D. The syslog server did not have the correct MIB loaded to receive the message

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 915

A systems administrator needs to improve WiFi performance in a densely populated office tower and use the latest standard. There is a mix of devices that use 2.4 GHz and 5 GHz. Which of the following should the systems administrator select to meet this requirement?

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

Answer: B (LEAVE A REPLY)

802.11ax is the latest WiFi standard that improves WiFi performance in densely populated environments and supports both 2.4 GHz and 5 GHz bands. 802.11ac is the previous standard that only supports 5 GHz band. 802.11g and 802.11n are older standards that support 2.4 GHz band only or both bands respectively. Reference: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.techtarget.com/searchnetworking/tip/Whats-the-difference-between-80211ax-vs-80211ac>

NEW QUESTION: 916

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: (SHOW ANSWER)

Change management is the process and organization of enacting change in an organization to ensure a safe, productive, cost saving, and smooth transition.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 917

A technician reviews a network performance report and finds a high level of collisions happening on the network. At which of the following layers of the OSI model would these collisions be found?

- A. Layer 1
- B. Layer 3
- C. Layer 4
- D. Layer 7

Answer: A (LEAVE A REPLY)

Collisions occur when two or more devices try to transmit signals on the same physical medium at the same time. This causes interference and data loss. Collisions can only happen at the physical layer of the OSI model, which is responsible for transmitting and receiving raw bits over a physical medium such as a cable or a wireless channel. The physical layer does not have any mechanism to prevent or resolve collisions. Therefore, higher layers of the OSI model, such as the data link layer, need to implement protocols to detect and recover from collisions, such as CSMA/CD for Ethernet networks.

References: Collision in computer networkingData Link Layer | Layer 2 | The OSI-Model

NEW QUESTION: 918

An organization has a security requirement that all network connections can be traced back to a user. A network administrator needs to identify a solution to implement on the wireless network. Which of the following is the best solution?

- A. Implementing enterprise authentication
- B. Requiring the use of PSKs
- C. Configuring a captive portal for users
- D. Enforcing wired equivalent protection

Answer: A (LEAVE A REPLY)

Enterprise authentication is a method of securing wireless networks that uses an external authentication server, such as RADIUS, to verify the identity of users and devices. Enterprise authentication can provide user traceability by logging the network connections and activities of each authenticated user. This can help the organization meet its security requirement and comply with any regulations or policies that mandate user accountability¹².

References:

* CompTIA Network+ N10-008 Certification Exam Objectives, page 83

* CompTIA Network+ Cert Guide: Wireless Networking, page 13

NEW QUESTION: 919

A Wi-Fi network was recently deployed in a new, multilevel building. Several issues are now being reported related to latency and drops in coverage. Which of the following is the FIRST step to troubleshoot the issues?

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

Answer: A (LEAVE A REPLY)

Incorrect antenna placement could cause or exacerbate attenuation and interference problems.

Use a site survey and heat map to determine the optimum position for APs and (if available) the direction in which to point adjustable antennas.

NEW QUESTION: 920

Which of the following would be used to adjust resources dynamically for a virtual web server under variable loads?

- A. Elastic computing
- B. Scalable networking
- C. Hybrid deployment
- D. Multitenant hosting

Answer: A (LEAVE A REPLY)

Elastic Computing. Elasticity refers to a systems ability to adjust dynamically to a changing workload.

NEW QUESTION: 921

A company is considering shifting its business to the cloud. The management team is concerned at the availability of the third-party cloud service. Which of the following should the management team consult to determine the promised availability of the cloud provider?

- A. Memorandum of understanding
- B. Business continuity plan
- C. Disaster recovery plan
- D. Service-level agreement

Answer: D (LEAVE A REPLY)

Explanation

A Service-level agreement (SLA) is a document that outlines the responsibilities of a cloud service provider and the customer. It typically includes the agreed-upon availability of the cloud service provider, the expected uptime for the service, and the cost of any downtime or other service interruptions. Consulting the SLA is the best way for the management team to determine the promised availability of the cloud provider. Reference:

CompTIA Cloud+ Study Guide, 6th Edition, page 28.

NEW QUESTION: 922

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. Duplex
- B. VLAN

C. Speed

D. Errors

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 923

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

A. Rogue DHCP server

B. Misconfigured HSRP

C. DNS poisoning

D. Exhausted IP scope

Answer: ([SHOW ANSWER](#))

Explanation

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

NEW QUESTION: 924

A network technician is troubleshooting a connectivity issue. All users within the network report that they are unable to navigate to websites on the internet; however, they can still access local network resources. The technician issues a command and receives the following results:

```
Pinging comptia.com [172.67.217.56] with 32 bytes of data:  
Reply from 172.67.217.56: TTL expired in transit.  
Reply from 172.67.217.56: TTL expired in transit.  
Reply from 172.67.217.56: TTL expired in transit.  
Reply from 172.67.217.56: TTL expired in transit.
```

Which of the following best explains the result of this command?

A. Incorrect VLAN settings

B. Upstream routing loop

C. Network collisions

D. DNS misconfiguration

Answer: D ([LEAVE A REPLY](#))

The users are unable to navigate to websites on the internet but can access local network resources, indicating a possible DNS issue. The ping command result showing "TTL expired in transit" suggests that packets are not reaching their destination due to a DNS misconfiguration that is not resolving website names into IP addresses correctly³. A possible solution is to check and correct the DNS server settings on the network devices⁴.

NEW QUESTION: 925

Which of the following most likely requires the use of subinterfaces?

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

Answer: A ([LEAVE A REPLY](#))

Subinterfaces are logical divisions of a physical interface that allow a router to communicate with multiple networks using a single LAN port. Subinterfaces can have different IP addresses, VLANs, and routing protocols. They are useful for reducing the number of physical interfaces and cables needed, as well as improving network performance and security.

References:

Subinterfaces - CompTIA Network+ N10-008 Domain 1.21 - YouTube1

CompTIA Network+ Certification Exam Objectives, page 92

NEW QUESTION: 926

A network engineer installed a new fiber uplink for an office and wants to make sure that the link meets throughput requirements. Which of the following tools should the engineer use to verify that the new link is sufficient?

- A. tcpdump
- B. ping
- C. iperf
- D. netstat

Answer: ([SHOW ANSWER](#))

Explanation

iperf is a tool that can measure the bandwidth and quality of a network link by generating and transferring TCP or UDP data streams. iperf can report the maximum achievable throughput, packet loss, jitter, and other statistics for a given link. iperf can be used to test both the uplink and downlink performance of a network link by running it on two endpoints and specifying the direction and duration of the test. iperf can help the engineer verify that the new fiber uplink meets the throughput requirements for the office network.

tcpdump is a tool that can capture and analyze network traffic by filtering and displaying packets based on various criteria. tcpdump can help the engineer troubleshoot network problems, monitor network activity, and inspect packet contents, but it cannot measure the throughput or quality of a network link.

ping is a tool that can test the reachability and latency of a network host by sending and receiving ICMP echo packets. ping can help the engineer check if the new fiber uplink is connected and responsive, and how long it takes for packets to travel between the endpoints, but it cannot measure the throughput or quality of a network link.

netstat is a tool that can display information about the network connections, routing tables, interfaces, and protocols on a network host. netstat can help the engineer view the status and details of the network connections using the new fiber uplink, but it cannot measure the throughput or quality of a network link.

References

iperf - The ultimate speed test tool for TCP, UDP and SCTP

How to use iperf to test local network LAN speed in Windows 10

How to Test Network Performance Between Two Linux Servers

What is tcpdump?

8 Common Network Utilities Explained

Monitoring Your Network: ping, netstat, tcpdump, and Ethereal

Netstat vs. Nmap vs. Netcat: Understanding the Differences

NEW QUESTION: 927

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

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

Answer: [\(SHOW ANSWER\)](#)

A broadcast storm Traffic that is recirculated and amplified by loops in a switching topology, causing network slowdowns and crashing switches.

NEW QUESTION: 928

A network administrator is setting up several IoT 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. Use DHCP exclusions to address each device
- B. Set up a reservation for each device
- C. Implement private VLANs for each device
- D. Configure a static IP on each device

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 929

Users report they cannot reach any websites on the internet. An on-site network engineer is able to duplicate the issue on a different PC. The network engineer then tries to ping a website and receives the following message:

Ping request could not find host www.google.com. Please check the name and try again.

Which of the following is the next step the engineer should take?

- A. Ping 127. 0. 0. 1 to test local hardware.
- B. Test the website from outside the company.
- C. Ping internal name server functionality.

D. Check internet firewall logs for blocked DNS traffic.

Answer: ([SHOW ANSWER](#))

The error message "Ping request could not find host www.google.com" indicates that the network engineer's PC cannot resolve the hostname www.google.com to its corresponding IP address. This means that there is a problem with the DNS (Domain Name System) service, which is responsible for translating hostnames to IP addresses and vice versa. The DNS service can be provided by internal or external name servers, depending on the network configuration.

The next step the engineer should take is to ping the internal name server functionality, which means to test if the PC can communicate with the name server that is configured in its network settings, and if the name server can resolve internal hostnames, such as those of the company's servers or devices. To do this, the engineer can use the following commands:

- * To find out the IP address of the name server, use `ipconfig /all` and look for the DNS Servers entry.
- * To ping the name server, use `ping <name server IP address>` and check if the packets are sent and received successfully.
- * To test the name resolution, use `nslookup <internal hostname>` and check if the name server returns the correct IP address.

If the ping or the nslookup commands fail, it means that the internal name server is not working properly, and the engineer should troubleshoot the name server configuration or connectivity. If the ping and the nslookup commands succeed, it means that the internal name server is working properly, but there is a problem with the external name resolution, and the engineer should check the internet firewall logs for blocked DNS traffic, or test the website from outside the company.

References Windows 10 can't resolve hostnames - ping with IP works but not with hostname
Ping request could not find host xyz.local.

Please check the name and try again
DNS problem, nslookup works, ping doesn't

NEW QUESTION: 930

Which of the following should be used to manage outside cables that need to be routed to various multimode uplinks?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 931

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

- A.** Reverse the fibers.
- B.** Reterminate the fibers.

C. Verify the fiber size.

D. Examine the cable runs for visual faults.

Answer: A (LEAVE A REPLY)

One of the most common causes of fiber connectivity issues is the reversal of the fibers. This means that the transmit (TX) and receive (RX) ports on one end of the fiber link are not matched with the corresponding ports on the other end. For example, if the TX port on one device is connected to the TX port on another device, and the same for the RX ports, then the devices will not be able to communicate with each other. This can result in no indicator light, no link, or no data transmission¹².

To troubleshoot this issue, the technician should first try to reverse the fibers. This can be done by swapping the connectors at one end of the fiber patch cable, or by using a crossover adapter or cable that reverses the polarity of the fibers. The technician should then check if the indicator light comes on and if the devices can communicate properly¹².

The other options are not the first steps to troubleshoot this issue. Reterminating the fibers is a time-consuming and costly process that should be done only if there is evidence of physical damage or poor quality of the termination. Verifying the fiber size is not relevant in this scenario, as multimode fiber is compatible with multimode fiber, and any mismatch in core diameter or bandwidth would result in high attenuation, not complete loss of signal. Examining the cable runs for visual faults is a useful technique, but it requires a special tool called a visual fault locator (VFL) that emits a visible red light through the fiber and shows any breaks or bends along the cable. However, a VFL cannot detect polarity issues or connector problems, so it is not sufficient to troubleshoot this issue

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 932

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

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

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 933

A technician is assisting a user who cannot connect to a website. The technician attempts to ping the default gateway and DNS server of the workstation. According to troubleshooting methodology, this is an example of:

- A. a divide-and-conquer approach.
- B. implementing a solution.
- C. a top-to-bottom approach.
- D. a bottom-up approach.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 934

Which of the following passwords would provide the best defense against a brute-force attack?

- A. ThisIsMyPasswordForWork
- B. Qwerty!@#\$
- C. Password!1
- D. T5!8j5

Answer: D ([LEAVE A REPLY](#))

Complexity: The password "T5!8j5" appears to be more complex, with a mix of uppercase letters, numbers, and special characters. This complexity increases the strength of the password and makes it more resistant to brute-force attacks.

Length: While longer passwords are generally more secure, in this case, the shorter password "T5!8j5" is still strong due to its complexity.

NEW QUESTION: 935

A technician needs to allow a device to maintain the same IP address lease based on the physical address of a network card. Which of the following should the technician use?

- A. MAC address reservation
- B. Static IP address
- C. Custom DNS server entry
- D. IP address exclusion

Answer: (SHOW ANSWER)

MAC address reservation is the technique that allows a device to maintain the same IP address lease based on the physical address of a network card. MAC address reservation is a feature of DHCP that allows network administrators to assign specific IP addresses to specific devices based on their MAC addresses. A MAC address is a unique identifier that is assigned to each network interface card (NIC) by its manufacturer. A MAC address reservation can ensure that a device always receives the same IP address from the DHCP server, regardless of its location or connection time. This can be useful for devices that need consistent network access or configuration, such as servers, printers, or cameras. Reference: [CompTIA Network+ Certification Exam Objectives], How to Reserve IP Addresses with DHCP Server

NEW QUESTION: 936

A lab environment hosts Internet-facing web servers and other experimental machines, which technicians use for various tasks. A technician installs software on one of the web servers to allow communication to the company's

file server, but it is unable to connect to it. Other machines in the building are able to retrieve files from the file server. Which of the following is the MOST likely reason the web server cannot retrieve the files, and what should be done to resolve the problem?

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 937

An engineer was asked to update an MX record for an upcoming project. Which of the following server types is MOST likely to be in scope for the project?

- A.** Email
- B.** Web
- C.** File
- D.** Database

Answer: ([SHOW ANSWER](#)**)**

Explanation

An MX record is a type of DNS record that specifies the mail server responsible for accepting email messages on behalf of a domain name. Therefore, an engineer who needs to update an MX record is most likely working on an email server project.

NEW QUESTION: 938

Which of the following would be used to indicate when unauthorized access to physical internal hardware has occurred?

- A.** Motion detectors
- B.** Radio frequency identification tags
- C.** Tamper evident seal
- D.** Locking racks

Answer: ([SHOW ANSWER](#)**)**

A tamper evident seal is a device or material that provides a visible indication of unauthorized access to physical internal hardware. Tamper evident seals can be stickers, labels, tapes, locks, or seals that are designed to break, tear, or change color when someone tries to open, remove, or tamper with them. Tamper evident seals can help deter and detect physical security breaches, such as theft, vandalism, or sabotage of hardware devices¹².

Tamper evident seals can also provide evidence for forensic analysis and legal action³.

References

1 - What Is Hardware Security? Definition, Threats, and Best Practices

2 - Device Physical Security Guideline | Information Security Office

3 - What is unauthorized physical access? - Heimduo

NEW QUESTION: 939

A network administrator received reports that a 40Gb connection is saturated. The only server the administrator can use for data collection in that location has a 10GB connection to the network.

Which of the following is the best method to use on the server to determine the source of the saturation?

- A. Port mirroring
- B. Log aggregation
- C. Flow data
- D. Packet capture

Answer: (SHOW ANSWER)

NEW QUESTION: 940

An IT officer is installing a new WAP. Which of the following must the officer change to conned users securely to the WAP?

- A. TKIP encryption protocol
- B. Dynamic selection of the frequency
- C. Channel to the highest frequency within the band
- D. AES encryption

Answer: D (LEAVE A REPLY)

NEW QUESTION: 941

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

Linux computer details:

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

Switch mirror port details:

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

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

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

Answer: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 942

Which of the following types of connections would need to be set up to provide access from the internal network to an external network so multiple satellite offices can communicate securely using various ports and protocols?

- A.** Client-to-site VPN
- B.** Clientless VPN
- C.** RDP
- D.** Site-to-site VPN
- E.** SSH

Answer: D (LEAVE A REPLY)

The question asks about the type of connection that would need to be set up to provide access from the internal network to an external network so multiple satellite offices can communicate securely using various ports and protocols.

A connection is a logical or physical link between two or more devices or networks that allows data transmission and exchange.

There are different types of connections that can be used for different purposes and scenarios, such as:

Client-to-site VPN: A connection that allows a remote client device to access a private network over a public network, such as the internet, using encryption and authentication. This type of connection is also known as a remote access VPN or a point-to-site VPN.

Clientless VPN: A connection that allows a remote client device to access a private network over a public network, such as the internet, using a web browser and a web-based portal, without requiring any additional software or configuration on the client device. This type of connection is also known as a web VPN or a SSL VPN.

RDP: A connection that allows a remote client device to access and control a remote host device over a network, using a graphical user interface and a protocol that transmits display, keyboard, mouse, and audio data. RDP stands for Remote Desktop Protocol and is a proprietary protocol developed by Microsoft.

Site-to-site VPN: A connection that allows two or more private networks to communicate securely over a public network, such as the internet, using encryption and authentication. This type of connection is also known as a router-to-router VPN or a network-to-network VPN.

SSH: A connection that allows a remote client device to access and execute commands on a remote host device over a network, using a text-based interface and a protocol that provides encryption, authentication, and integrity. SSH stands for Secure Shell and is an open standard protocol.

In this scenario, the best type of connection to use is a site-to-site VPN, because it can provide the following benefits:

It can connect multiple satellite offices to the main office, creating a virtual private network that spans across different geographic locations.

It can secure the communication between the offices, preventing unauthorized access, eavesdropping, or tampering by third parties on the public network.

Therefore, the answer is D, a site-to-site VPN, as it can provide access from the internal network to an external network so multiple satellite offices can communicate securely using various ports and protocols.

Reference:

CompTIA Network+ N10-008 Study Guide, Chapter 4: Network Security, Section 4.2: Secure Network Design,
Pages 204-207 Professor Messer's CompTIA N10-008 Network+ Course, Video 4.2: Secure Network Design,
Part 2 Network + N10-008 practice exam, Question 267, Answer D, Explanation

NEW QUESTION: 943

Hotspot Question

A network technician needs to resolve some issues with a customer's SOHO network. The customer reports that some of the PCs are not connecting to the network, while others appear to be working as intended.

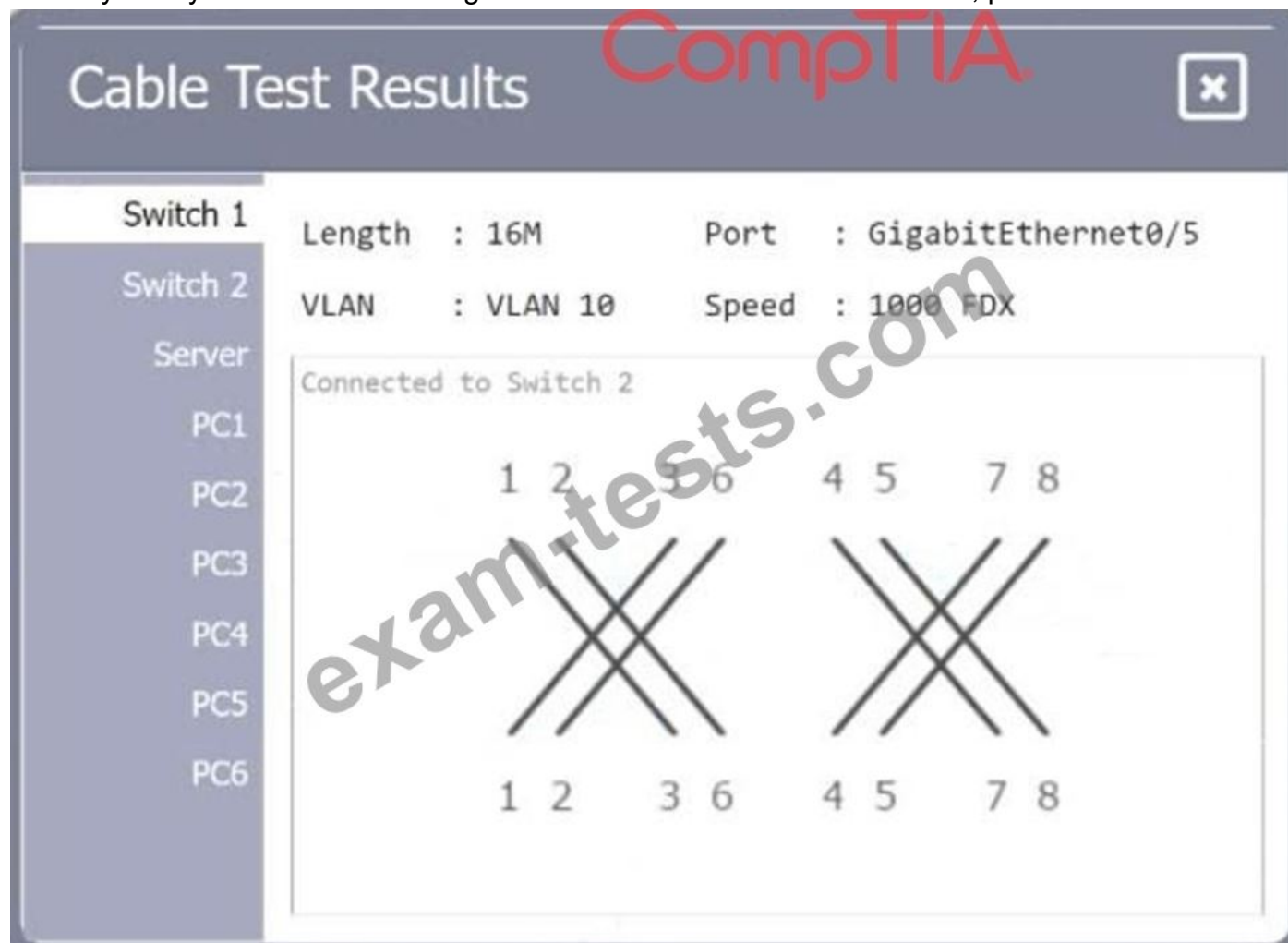
INSTRUCTIONS

Troubleshoot all the network components.

Review the cable test results first, then diagnose by clicking on the appropriate PC, server, and Layer 2 switch.

Identify any components with a problem and recommend a solution to correct each problem.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Cable Test Results

Switch 1

Switch 2

Server

PC1

PC2

PC3

PC4

PC5

PC6

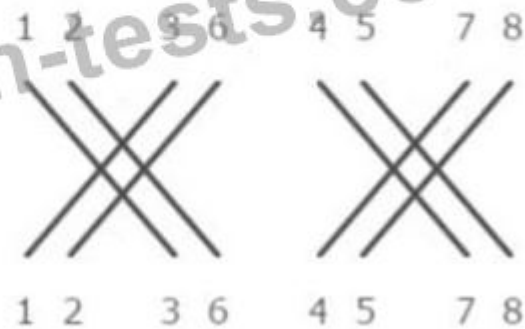
Length : 16M

Port : GigabitEthernet0/5

VLAN : VLAN 10

Speed : 1000 FDX

Connected to Switch 1



Cable Test Results

Switch 1

Switch 2

Server

PC1

PC2

PC3

PC4

PC5

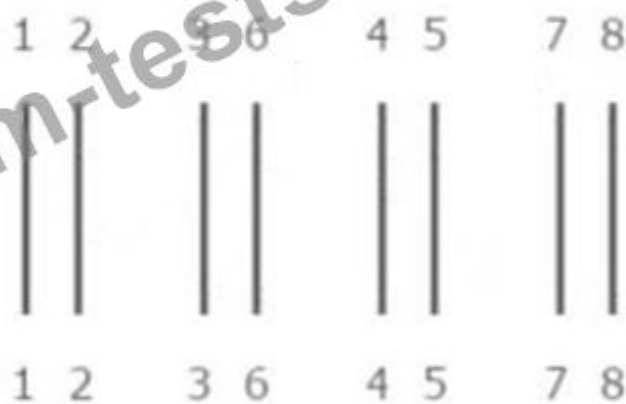
PC6

Length : 22M

Port : GigabitEthernet0/1

VLAN : VLAN 10

Speed : 1000 FDX



Cable Test Results



Switch 1

Length : 42M

Port : GigabitEthernet0/2

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

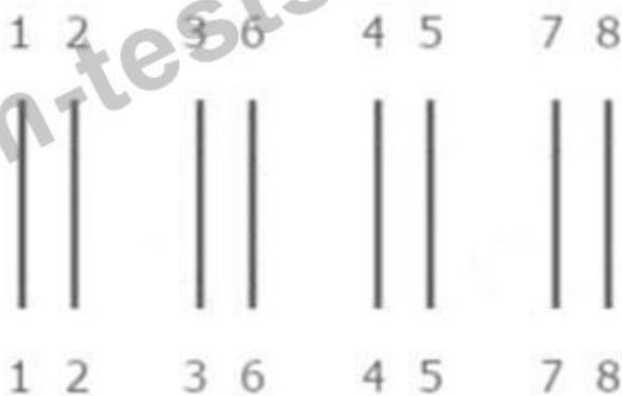
PC2

PC3

PC4

PC5

PC6



CompTIA

Cable Test Results



Switch 1

Length : 12M

Port : GigabitEthernet0/1

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

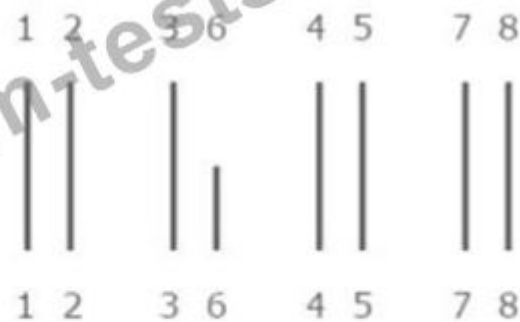
PC2

PC3

PC4

PC5

PC6



CompTIA

Cable Test Results



Switch 1

Length : 20M

Port : GigabitEthernet0/2

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

PC2

PC3

PC4

PC5

PC6

1 2 3 6 4 5 7 8

1 2 3 6 4 5 7 8

Cable Test Results



Switch 1

Length : 18M

Port : GigabitEthernet0/3

Switch 2

VLAN : VLAN 11

Speed : 1000 FDX

Server

PC1

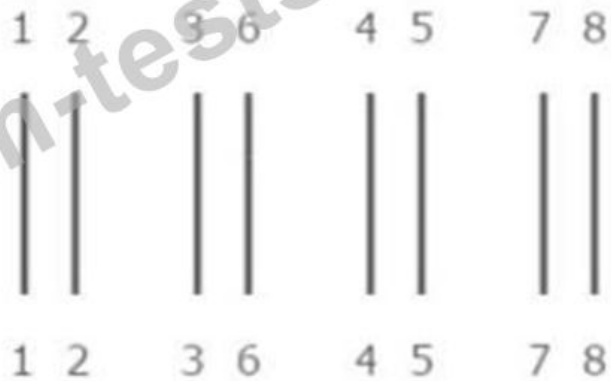
PC2

PC3

PC4

PC5

PC6



CompTIA

Cable Test Results



Switch 1

Length : 33M

Port : GigabitEthernet0/4

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

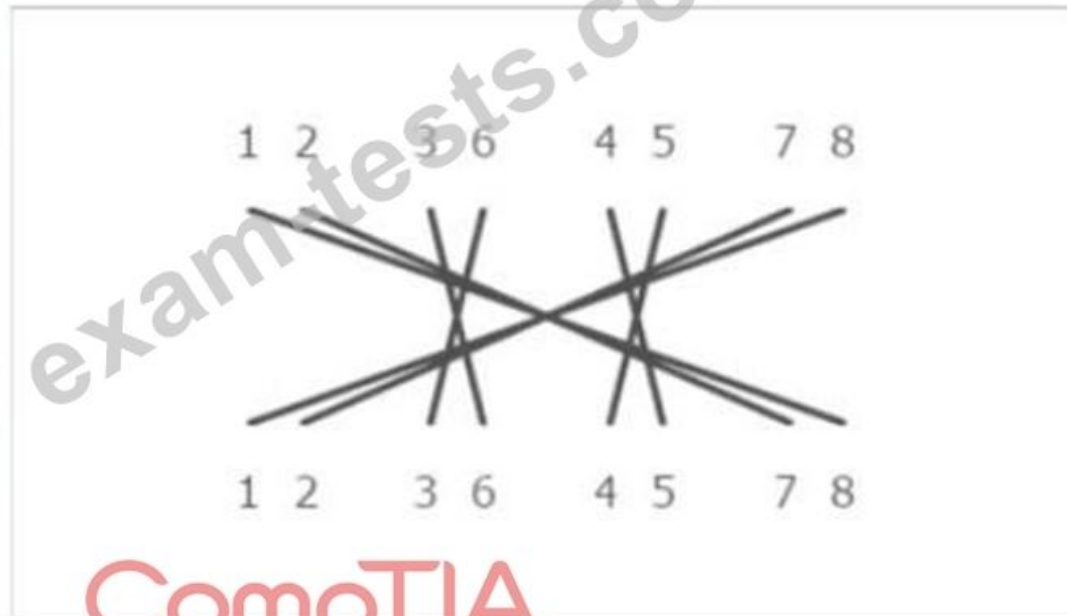
PC2

PC3

PC4

PC5

PC6



CompTIA

Cable Test Results



Switch 1

Length : 90M

Port : GigabitEthernet0/3

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

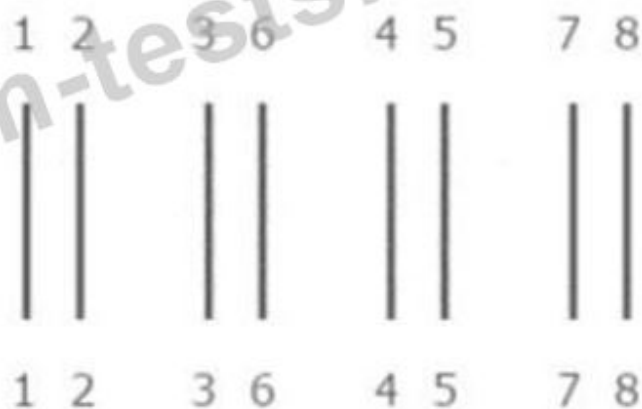
PC2

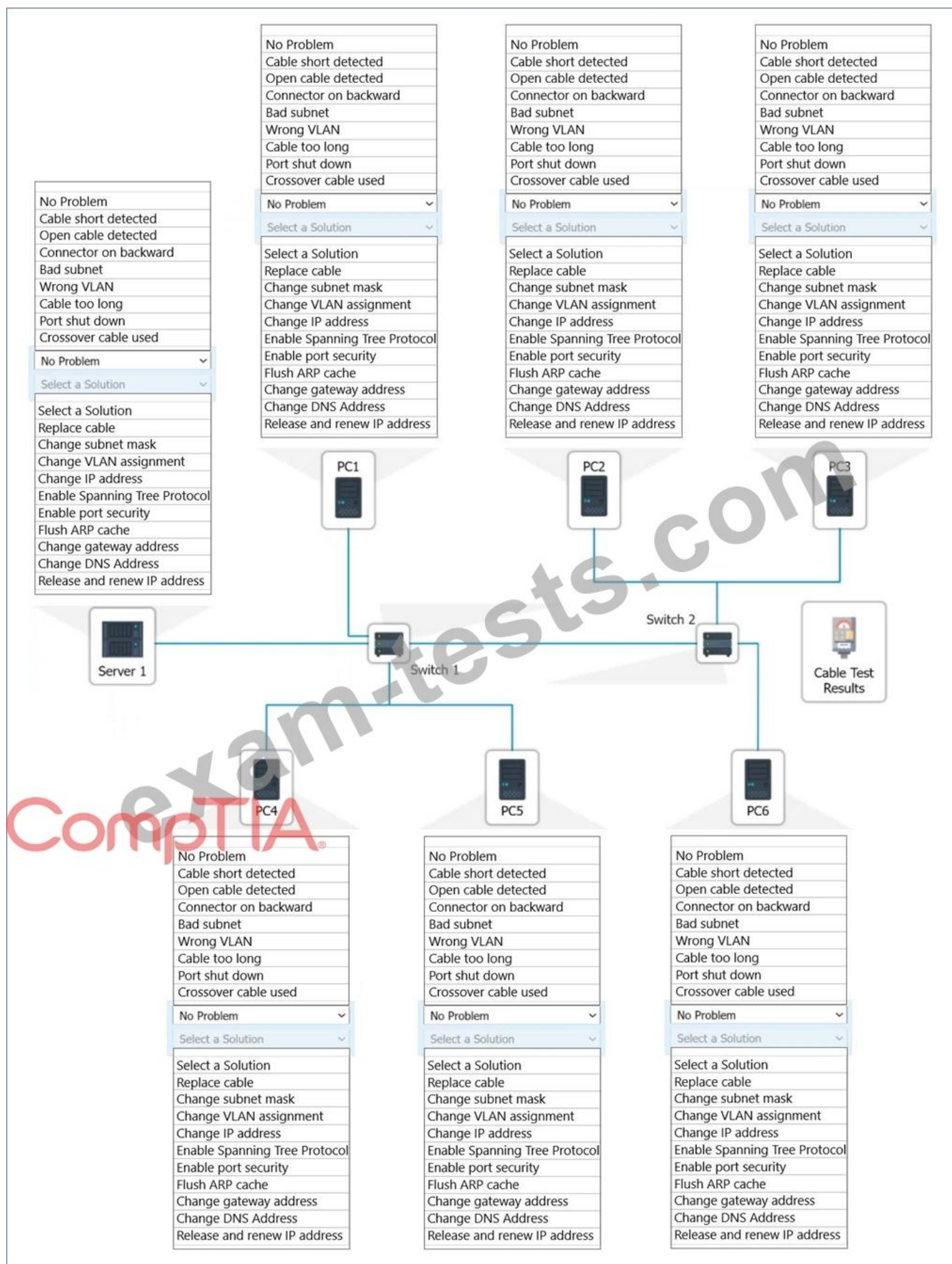
PC3

PC4

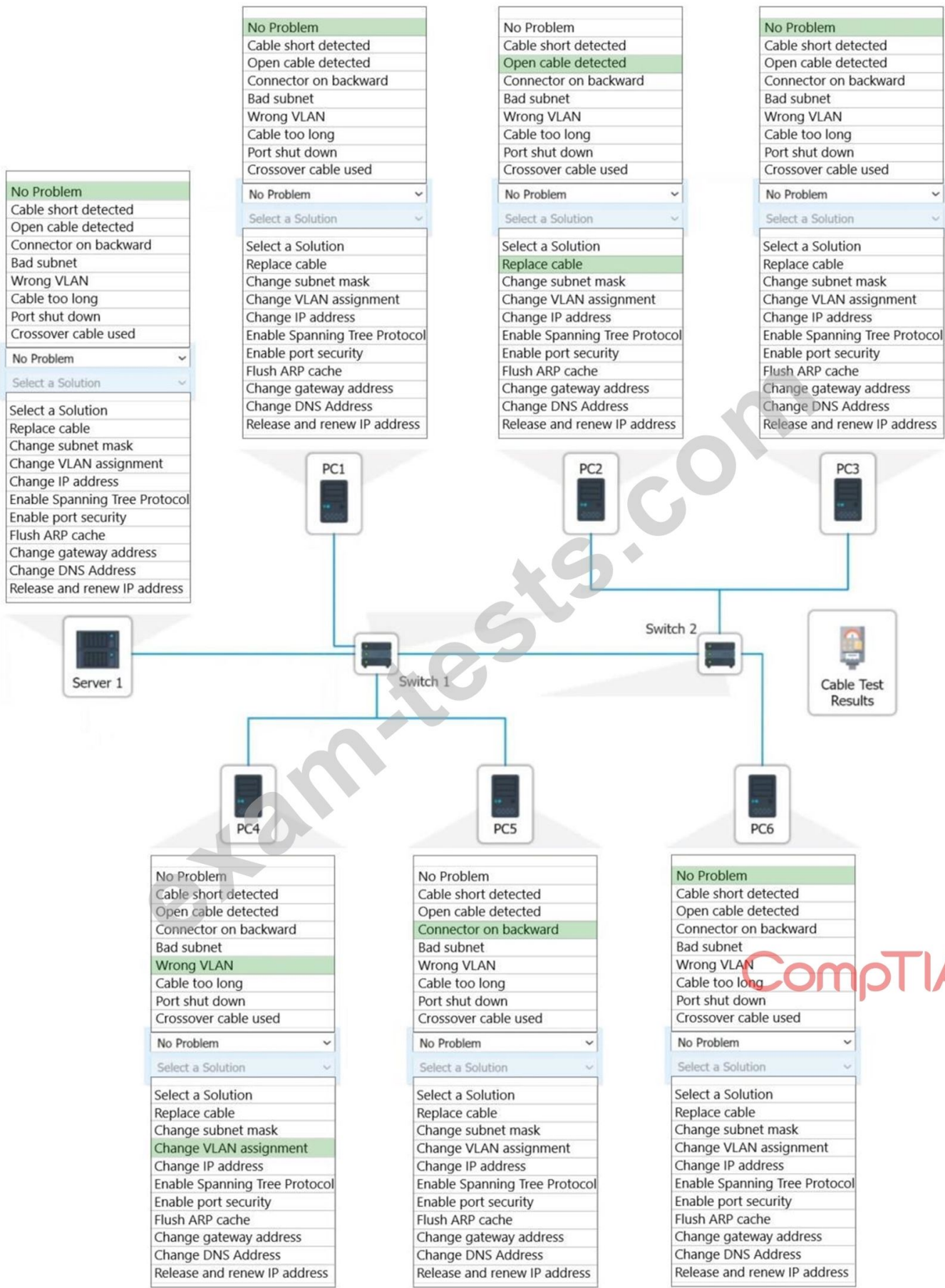
PC5

PC6





Answer:



NEW QUESTION: 944

In order to prepare for a fire or natural disaster, a Chief Executive Officer would like the network administrator to set up a site with no equipment. Which of the following should the network administrator set up?

- A. A site provided by the ISP
- B. A cold site
- C. A hot site
- D. A warm site

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 945

A local firm has hired a consulting company to clean up its IT infrastructure. The consulting company notices remote printing is accomplished by port forwarding via publicly accessible IPs through the firm's firewall Which of the following would be the MOST appropriate way to enable secure remote printing?

- A. VPN
- B. SSL
- C. SSH
- D. Telnet

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 946

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

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

Answer: D ([LEAVE A REPLY](#))

Explanation

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

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 947

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

- A. Secure web access to internal corporate resources.

- B.** Upgrade security via the use of an NFV technology
- C.** Connect two data centers across the internet.
- D.** Increase VPN availability by using a SDWAN technology.

Answer: A (LEAVE A REPLY)

* A clientless VPN is a type of VPN that does not require a dedicated software client to be installed on the user's device. Instead, it uses a web browser as the VPN client and provides secure access to web-based applications or resources¹².

* A clientless VPN is suitable for scenarios where the user needs to access internal corporate resources that are web-based, such as intranet sites, webmail, or web portals¹². This way, the user does not need to install or configure any additional software, and the VPN connection is established through the browser's SSL/TLS encryption¹².

* A clientless VPN is not suitable for scenarios where the user needs to access non-web-based applications or resources, such as file shares, remote desktops, or network printers¹². For these scenarios, a full VPN client is required, which can create a secure tunnel for all network traffic from the user's device¹².

* Therefore, option A is the most appropriate use case for the deployment of a clientless VPN, as it provides secure web access to internal corporate resources.

* The other options are not relevant to the use case of a clientless VPN, as they involve different types of VPN technologies or scenarios.

* Option B is incorrect because NFV (Network Function Virtualization) is a technology that virtualizes network functions, such as firewalls, routers, or load balancers, and runs them on software platforms instead of dedicated hardware devices³. NFV can improve security by reducing the attack surface, simplifying management, and enabling rapid deployment of security

* updates³. However, NFV is not a type of VPN, and it does not provide secure access to internal corporate resources.

* Option C is incorrect because connecting two data centers across the internet requires a site-to-site VPN, which is a type of VPN that creates a secure tunnel between two or more network locations, such as branch offices or data centers. A site-to-site VPN allows the network devices at each location to communicate with each other as if they were on the same local network. A site-to-site VPN requires a VPN gateway at each location, which can be a router, firewall, or VPN appliance.

A site-to-site VPN is not a clientless VPN, and it does not involve web browsers or web-based applications.

* Option D is incorrect because increasing VPN availability by using a SDWAN (Software-Defined Wide Area Network) technology is not a use case for a clientless VPN, but rather a benefit of using a SDWAN technology. A SDWAN is a technology that uses software to dynamically route network traffic over multiple WAN links, such as broadband, LTE, or MPLS. A SDWAN can improve VPN availability by providing redundancy, load balancing, and failover for VPN connections. A SDWAN can also simplify VPN deployment and management by using centralized policies and automation. However, a SDWAN is not a type of VPN, and it does not provide secure access to internal corporate resources.

References:

* : CompTIA Network+ N10-008 Study Guide, Chapter 7, Section 7.1, "VPN Concepts", page 381-382.

* : Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 7.1, "VPN Concepts", page 58.

- * : CompTIA Network+ N10-008 Study Guide, Chapter 5, Section 5.2, "NFV", page 264-265.
- * : Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 5.2, "NFV", page 38.
- * : CompTIA Network+ N10-008 Study Guide, Chapter 7, Section 7.1, "VPN Concepts", page 383-384.
- * : Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 7.1, "VPN Concepts", page 59.
- * : CompTIA Network+ N10-008 Study Guide, Chapter 5, Section 5.3, "SDWAN", page 266-267.
- * : Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 5.3, "SDWAN", page 39.

NEW QUESTION: 948

A network administrator walks into a datacenter and notices an unknown person is following closely. The administrator stops and directs the person to the security desk. Which of the following attacks did the network administrator prevent?

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

Answer: B ([LEAVE A REPLY](#))

Tailgating represents the situation, when an individual without access authorization closely follows an authorized person in a reserved area. The malefactor takes advantage of the moment, when the authorized one opens the door with his badge - and sneaks inside before the door closes.

Piggybacking represents the situation, when someone accesses a reserved area with the permission obtained by deception of an authorized person.

NEW QUESTION: 949

A network technician is configuring a wireless network that consists of multiple APs for better coverage and allows roaming between the APs. Which of the following types of SSIDs should the technician configure?

- A. Independent Basic Service Set
- B. Basic Service Set
- C. Extended Service Set
- D. Distribution System Service

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 950

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

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

Answer: ([SHOW ANSWER](#))

The maximum transmission unit (MTU) is the largest size of a data packet that can be transmitted over a network. A standard Ethernet frame supports an MTU of 1500 bytes, which is the default value for most Ethernet networks.

Larger MTUs are possible with jumbo frames, but they are not widely supported and may cause fragmentation or compatibility issues. Reference: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), https://en.wikipedia.org/wiki/Maximum_transmission_unit

NEW QUESTION: 951

A network administrator is planning to implement device monitoring to enhance network visibility. The security team requires that the solution provides authentication and encryption.

Which of the following meets these requirements?

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

Answer: D (LEAVE A REPLY)

Explanation

SNMPv3 is a protocol that allows network administrators to monitor and manage network devices such as routers, switches, servers, printers, and more. SNMPv3 provides authentication and encryption features that ensure the security and integrity of the data exchanged between the management station and the network devices. SNMPv3 uses a user-based security model (USM) that supports three levels of security: noAuthNoPriv, authNoPriv, and authPriv. The noAuthNoPriv level provides no authentication or encryption, the authNoPriv level provides authentication but no encryption, and the authPriv level provides both authentication and encryption¹².

References

SNMP is one of the common network monitoring protocols covered in Objective 3.1 of the CompTIA Network+ N10-008 certification exam³.

SNMPv3 provides authentication and encryption features for network monitoring¹².

SNMPv3 uses a user-based security model with three levels of security¹².

1: SNMP - N10-008 CompTIA Network+ : 3.1 - Professor Messer IT Certification Training Courses 2:

CompTIA Network+ N10-008 Cert Guide, Chapter 13, page 413 3: CompTIA Network+ Certification Exam Objectives, page 7

NEW QUESTION: 952

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

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 953

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

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

Answer: ([SHOW ANSWER](#))

Explanation

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

NEW QUESTION: 954

SIMULATION

You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

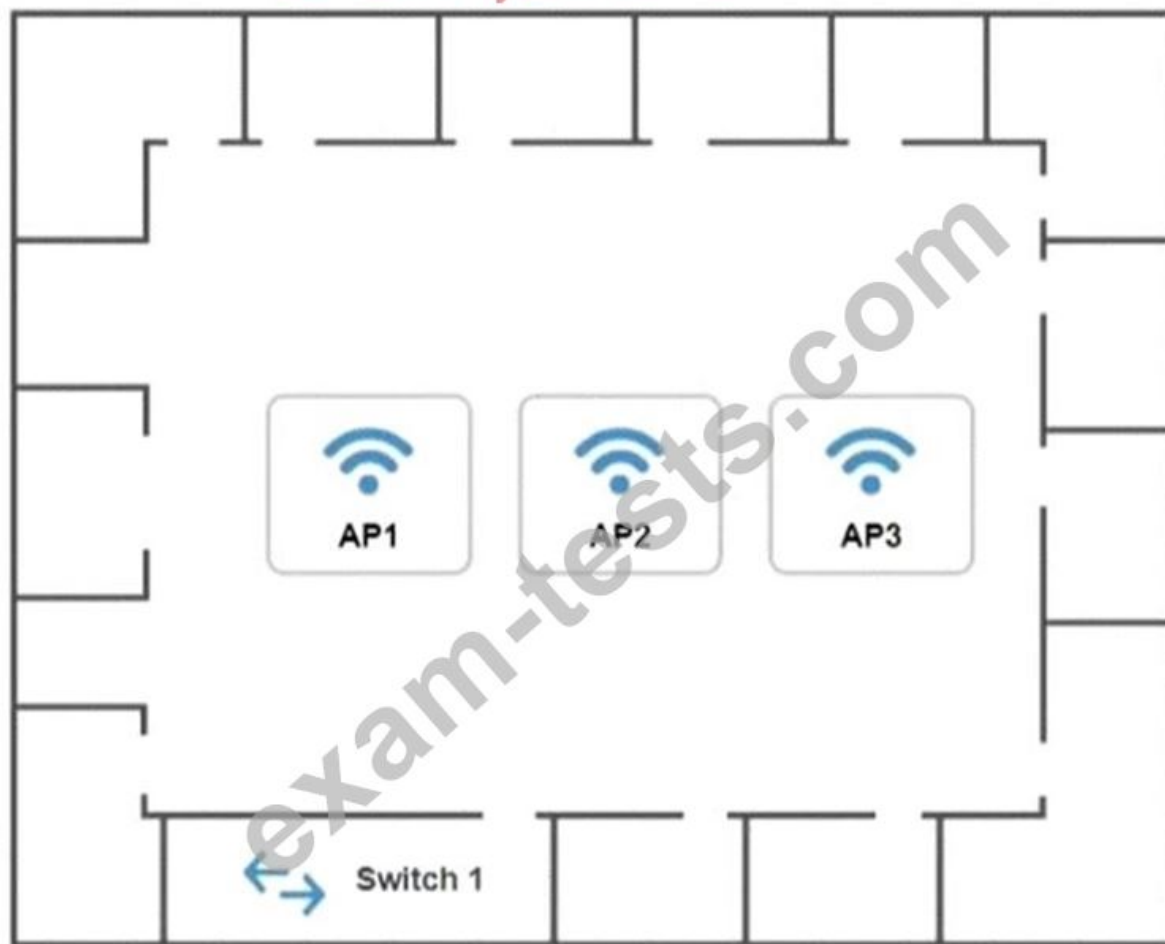
The SSIDs need to be configured as CorpNet with a key of S3cr3t!

The wireless signals should not interfere with each other

The subnet the Access Points and switch are on should only support 30 devices maximum The Access Points should be configured to only support TKIP clients at a maximum speed INSTRUCTIONS Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

CompTIA®



192.168.1.2
Speed: Auto
Duplex: Auto

AP1 Configuration

https://ap1.setup.do

Basic Configuration

Access Point Name

AP1

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

Yes

No

Wireless

Mode

B

G

Channel

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

AP2 Configuration



https://ap2.setup.do

Basic Configuration

Access Point Name

AP2

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B
G

Channel

1
2
3
4
5
6
7
8
9
10
11

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name

AP3

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B

G

Channel

1

2

3

4

5

6

7

8

9

10

11

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

Answer:

See explanation below.

Explanation

On the first exhibit, the layout should be as follows

The screenshot shows a web browser window titled "AP1 Configuration" with the URL "https://ap1.setup.do". The interface is divided into three main sections: "Basic Configuration", "Wireless", and "Wired".

Basic Configuration:

- Access Point Name: AP1
- IP Address: 192.168.1.32
- Gateway: 192.168.1.1
- SSID: CorpNet
- SSID Broadcast: ☒ Yes ☐ No

Wireless:

- Mode: B
- Channel: 3

Wired:

- Speed: ☐ Auto ☒ 100 ☐ 1000
- Duplex: ☐ Auto ☐ Half ☒ Full

Graphical user interface, text, application, chat or text message Description automatically generated

The screenshot shows a web browser window titled "Security Configuration". The interface includes the following settings:

- Security Settings: ☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise
- Key or Passphrase: S3cr3tl

Graphical user interface Description automatically generated

AP1 Configuration

https://ap1.setup.do

IP Address: 192.168.1.32 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode: B

Channel: 3

Wired

Speed: ☐ Auto ☒ 100 ☐ 1000

Duplex: ☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings: ☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Graphical user interface, text, application, chat or text message Description automatically generated

Security Configuration

Security Settings: ☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase: S3cr3tl

Graphical user interface Description automatically generated

AP1 Configuration

←

→

↺

https://ap1.setup.do

IP Address

192.168.1.3

/

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes

☐ No

Wireless

Mode

G

Channel

3

Wired

Speed

☒ Auto

☐ 100

☐ 1000

Duplex

☒ Auto

☐ Half

☐ Full

Security Configuration

Security Settings

☐ None

☐ WEP

☒ WPA

☐ WPA2

☐ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Reset to Default

Save

Close

Exhibit 2 as follows

Access Point Name AP2

Graphical user interface Description automatically generated

AP2 Configuration

https://ap2.setup.do

Basic Configuration

Access Point Name: AP2

IP Address: 192.168.1.64 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode: B

Channel: 6

Wired

Speed: ☐ Auto ☒ 100 ☐ 1000

Duplex: ☐ Auto ☐ Half ☒ Full

Security Configuration

Reset to Default Save Close

Graphical user interface, text, application, chat or text message Description automatically generated

Security Configuration

Security Settings: ☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase: S3cr3t!

Graphical user interface Description automatically generated

AP2 Configuration

← → ↺

https://ap2.setup.do

IP Address

192.168.1.4

/

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

G

Channel

6

Wired

Speed

☒ Auto ☐ 100 ☐ 1000

Duplex

☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings

☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Reset to Default

Save

Close

Exhibit 3 as follows

Access Point Name AP3

Graphical user interface Description automatically generated

AP3 Configuration

[←](#)
[→](#)
[↺](#)

Basic Configuration

Access Point Name

AP3

IP Address

192.168.1.96 / 27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes
 ☐ No

Wireless

Mode

B

Channel

9

Wired

Speed

☐ Auto
 ☒ 100
 ☐ 1000

Duplex

☐ Auto
 ☐ Half
 ☒ Full

Security Configuration

Reset to Default

Save

Close

Graphical user interface, text, application, chat or text message Description automatically generated

Security Configuration

Security Settings

☐ None
 ☐ WEP
 ☐ WPA
 ☐ WPA2
 ☒ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Graphical user interface Description automatically generated

AP3 Configuration

https://ap3.setup.do

IP Address: 192.168.1.5 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode: G

Channel: 9

Wired

Speed: ☒ Auto ☐ 100 ☐ 1000

Duplex: ☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings: ☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase: S3cr3t!

Reset to Default Save Close

NEW QUESTION: 955

A network administrator creates a new network, 10.10.0.0/24, on a DHCP server. The administrator wants to ensure that 10.10.0.10-10.10.0.15 are not allocated to other devices.

Which of the following features should the administrator configure?

- A. Exclusion
- B. Relay
- C. Scope
- D. Reservation

Answer: (SHOW ANSWER)

NEW QUESTION: 956

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

- A. Polarization
- B. Channel utilization

- C. Channel bonding
- D. Antenna type
- E. MU-MIMO

Answer: D (LEAVE A REPLY)

* The antenna type is the factor that would most likely facilitate the correct accessibility to the Wi-Fi network, as it determines the shape, direction, and range of the wireless signal¹². Different types of antennas have different characteristics, such as gain, beamwidth, and polarization, that affect how well they can cover a given area and overcome obstacles or interference¹². For example, an omnidirectional antenna can radiate the signal in all directions, while a directional antenna can focus the signal in a specific direction¹². By choosing the appropriate antenna type for the rented office space, the network administrator can ensure a sufficient signal and reduce exposure to the wireless network.

* Polarization is the orientation of the electric field of the wireless signal, which can be either vertical, horizontal, or circular¹². Polarization affects the compatibility and performance of the wireless communication, as the transmitter and receiver antennas should have the same polarization to avoid signal loss¹². However, polarization alone would not facilitate the correct accessibility to the Wi-Fi network, as it depends on the antenna type and the environment¹².

* Channel utilization is the measure of how much a wireless channel is occupied by data transmission, management frames, or control frames¹³. Channel utilization affects the efficiency and throughput of the wireless network, as a high channel utilization can indicate congestion, interference, or contention¹³. However, channel utilization alone would not facilitate the correct accessibility to the Wi-Fi network, as it depends on the network design, configuration, and demand¹³.

* Channel bonding is the technique of combining two adjacent channels into one wider channel to increase the bandwidth and throughput of the wireless network¹. Channel bonding can improve the performance of the wireless network, especially for applications that require high data rates, such as video streaming¹. However, channel bonding alone would not facilitate the correct accessibility to the Wi-Fi network, as it also introduces some challenges, such as increased interference, reduced channel availability, and compatibility issues¹.

* MU-MIMO (Multi-User Multiple Input Multiple Output) is a technology that allows a wireless access point to transmit data to multiple devices simultaneously using multiple antennas and spatial streams¹. MU-MIMO can enhance the capacity and efficiency of the wireless network, especially for high-density environments, such as offices, classrooms, or stadiums¹. However, MU-MIMO alone would not facilitate the correct accessibility to the Wi-Fi network, as it also requires some conditions, such as compatible devices, sufficient signal strength, and optimal antenna placement¹.

References:

- * 1: CompTIA Network+ N10-008 Study Guide, Chapter 4: Wireless Technologies
- * 2: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 42: Wireless Antennas
- * 3: Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 43: Wireless Troubleshooting
- * : Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 41: Wireless Channels
- * : Professor Messer's CompTIA N10-008 Network+ Course Notes, Page 40: Wireless Technologies

NEW QUESTION: 957

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

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

Answer: B (LEAVE A REPLY)

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

Load balancing is a technique that distributes network traffic across multiple servers or devices for improved availability and scalability, which does not

NEW QUESTION: 958

A network engineer is investigating issues on a Layer 2 switch. The department typically shares a switchport during meetings for presentations, but after the first user shares, no other users can connect. Which of the following is MOST likely related to this issue?

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

Answer: C (LEAVE A REPLY)

The issue described in the scenario suggests that the switchport is being shut down after the first user connects. This is a common behavior when port security is enabled on a switchport, which limits the number of MAC addresses that can connect to the port. Once the limit is reached, the switchport is shut down to prevent unauthorized devices from connecting.

NEW QUESTION: 959

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

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

Answer: B,E ([LEAVE A REPLY](#))

A botnet is a network of compromised devices that are remotely controlled by a malicious actor, usually for the purpose of launching distributed denial-of-service (DDoS) attacks, sending spam, stealing data, or performing other malicious activities¹.

A malware infection is a common way of compromising internet-connected devices and making them part of a botnet. Malware is any software that is designed to harm or exploit a device, a network, or a user. Malware can be delivered through various methods, such as phishing emails, malicious downloads, drive-by downloads, or removable media². Malware can infect a device and allow a remote attacker to take control of it, monitor its activities, or use its resources³.

The use of default credentials is another common way of compromising internet-connected devices and making them part of a botnet. Default credentials are the username and password combinations that are preconfigured by the manufacturer or vendor of a device, such as a router, a camera, or a printer. Default credentials are often easy to guess or find online, and many users do not change them after setting up their devices. This makes the devices vulnerable to unauthorized access and manipulation by attackers who can scan the internet for devices with default credentials and add them to their botnet .

A deauthentication attack is a type of wireless attack that aims to disconnect a legitimate user from a wireless network by sending spoofed deauthentication frames to the user's device or the access point (AP). A deauthentication attack can cause a denial of service, disrupt network communication, or facilitate other attacks, such as capturing the handshake during the reconnection process. However, a deauthentication attack does not compromise the device or make it part of a botnet.

IP spoofing is a technique of forging the source IP address of a packet to make it appear as if it came from a different device or location. IP spoofing can be used to bypass security filters, hide the identity of the attacker, or launch reflection or amplification attacks. However, IP spoofing does not compromise the device or make it part of a botnet, unless it is combined with other methods, such as malware infection or exploitation of vulnerabilities.

Firmware corruption is a condition where the firmware of a device, which is the software that controls its basic functions and operations, becomes damaged or altered due to various reasons, such as power surges, hardware failures, malicious attacks, or improper updates. Firmware corruption can cause the device to malfunction, lose data, or become inaccessible. However, firmware corruption does not compromise the device or make it part of a botnet, unless it is caused by a malicious attack that replaces the firmware with a malicious version.

A dictionary attack is a type of brute-force attack that tries to guess the password of a user or a device by using a list of common or likely passwords, such as those found in a dictionary, a database, or a previous breach. A dictionary attack can be used to compromise a device and make it part of a botnet, but only if the device has a weak or predictable password. Therefore, a dictionary attack is not a direct way of compromising a device, but rather a means of exploiting the use of default or weak credentials.

Reference:

1: Botnet

2: Malware

3: How Malware Can Turn Your Device into a Botnet

4: [Default Credentials]

5: [How Default Credentials Can Lead to IoT Botnets]

6: [Deauthentication Attack]

7: [IP Spoofing]

8: [Firmware Corruption]

9: [Dictionary Attack]

NEW QUESTION: 960

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

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

Answer: C ([LEAVE A REPLY](#))

Explanation

EIGRP is an advanced distance vector routing protocol that is able to automatically update routing tables and also uses features of link-state routing protocols, such as the ability to send updates about the current topology of the network. EIGRP also has the ability to use a variety of algorithms to determine the best route for a packet to take, allowing for more efficient routing across the network.

NEW QUESTION: 961

Which of the following steps of the troubleshooting methodology would most likely include checking through each level of the OSI model after the problem has been identified?

- A. Establish a theory.
- B. Implement the solution.
- C. Create a plan of action.
- D. Verify functionality.

Answer: C ([LEAVE A REPLY](#))

Creating a plan of action is the step of the troubleshooting methodology that would most likely include checking through each level of the OSI model after the problem has been identified. According to the web search results, the troubleshooting methodology consists of the following steps: 12 Define the problem: Identify the symptoms and scope of the problem, and gather relevant information from users, devices, and logs.

Establish a theory: Based on the information collected, hypothesize one or more possible causes of the problem, and rank them in order of probability.

Test the theory: Test the most probable cause first, and if it is not confirmed, eliminate it and test the next one.

Repeat this process until the root cause is found or a new theory is needed.

Create a plan of action: Based on the confirmed cause, devise a solution that can resolve the problem with minimal impact and risk. The solution may involve checking through each level of the OSI model to ensure that all layers are functioning properly and that there are no configuration errors, physical damages, or logical inconsistencies

34 Implement the solution: Execute the plan of action, and monitor the results. If the problem is not solved, revert to the previous state and create a new plan of action.

Verify functionality: Confirm that the problem is fully resolved and that the network is restored to normal operation.

Perform preventive measures if possible to avoid recurrence of the problem.

Document the findings: Record the problem description, the solution, and the outcome. Update any relevant documentation, such as network diagrams, policies, or procedures.

Reference 1: Troubleshooting Methods for Cisco IP Networks 2: Troubleshooting Methodologies - CBT IT Certification Training 3: How to use the OSI Model to Troubleshoot Networks 4: How is the OSI model used in troubleshooting? - Sage-Answer

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpsPASS.com/CompTIA/N10-008-practice-exam-dumps.html> (1075 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 962

A network engineer needs to create a subnet that has the capacity for five VLANs. with the following number of clients lo be allowed on each:

VLAN 10	50 users
VLAN 20	35 users
VLAN 30	20 users
VLAN 40	75 users
VLAN 50	130 users

Which of the following is the SMALLEST subnet capable of this setup that also has the capacity to double the number of clients in the future?

- A. 10.0.0.0/23
- B. 10.0.0.0/22
- C. 10.0.0.0/24
- D. 10.0.0.0/21

Answer: B (LEAVE A REPLY)

NEW QUESTION: 963

Given the following Information:

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

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 964

A network administrator needs to add access points to the network because coverage in some areas is improper. Which of the following should the administrator do first?

- A. Interference analysis
- B. Wireless survey
- C. Traffic analysis
- D. Packet capture

Answer: B (LEAVE A REPLY)

A wireless survey is the first step that a network administrator should do before adding access points to the network. A wireless survey is a process of collecting data about the wireless environment, such as signal strength, channel usage, interference, and coverage. A wireless survey can help the network administrator to determine the optimal locations and configurations for the access points to provide the best possible coverage and performance for the wireless network. A wireless survey can also help to identify and troubleshoot any issues that may cause improper coverage in some areas.

<https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guide/>

NEW QUESTION: 965

A Chief Information Officer (CIO) wants to improve the availability of a company's SQL database. Which of the following technologies should be utilized to achieve maximum availability?

- A. Clustering
- B. Port aggregation
- C. NIC teaming
- D. Snapshots

Answer: A (LEAVE A REPLY)

Clustering, if one server goes offline for any reason, the database is still available via other servers in the cluster. NIC teaming won't work if the server goes offline and maximum availability would not be achieved.

NEW QUESTION: 966

A network technician notices the site-to-site VPN and Internet connection have not come back up at a branch office after a recent power outage. Which of the following is an out-of-band method the technician would MOST likely utilize to check the branch office's router status?

- A. Travel to the branch office
- B. Use a modem to console into the router
- C. Hire a contractor to go on-site
- D. Walk a user through troubleshooting the connection

Answer: B (LEAVE A REPLY)

NEW QUESTION: 967

At which of the following OSI model layers does a MAC filter list for a wireless infrastructure operate?

- A. Physical

- B. Data link
- C. Network
- D. Session

Answer: B (LEAVE A REPLY)

NEW QUESTION: 968

A network administrator would like to enable NetFlow on a Layer 3 switch but is concerned about how the feature may impact the switch. Which of the following metrics should the administrator graph using SNMP to BEST measure the feature's impact?

- A. Electrical consumption
- B. Bandwidth usage
- C. Temperature
- D. CPU usage

Answer: D (LEAVE A REPLY)

NEW QUESTION: 969

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

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

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

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

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 970

Which of the following routing protocols is BEST suited for use on a perimeter router?

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

Answer: [\(SHOW ANSWER\)](#)

BGP stands for Border Gateway Protocol and it is used to exchange routing information between autonomous systems (AS) on the Internet. A perimeter router is a router that connects an AS to another AS or to the Internet. Therefore, BGP is the best suited routing protocol for a perimeter router.

References: Network+ Study Guide Objective 2.4: Compare and contrast the characteristics of network topologies, types and technologies.

NEW QUESTION: 971

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

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

Answer: [B \(LEAVE A REPLY\)](#)

Explanation

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

NEW QUESTION: 972

A company cell phone was stolen from a technician's vehicle. The cell phone has a passcode, but it contains sensitive information about clients and vendors. Which of the following should also be enabled?

- A. Factory reset
- B. Autolock
- C. Encryption
- D. Two-factor authentication

Answer: [C \(LEAVE A REPLY\)](#)

Encryption is the process of transforming data into an unreadable format using a secret key or algorithm. It can protect sensitive information from unauthorized access or theft, even if the device is lost or stolen.

Factory reset is the process of restoring a device to its original settings and deleting all user data and applications. It can be used to erase personal information from a device before selling or disposing of it, but it does not prevent data recovery by forensic tools. Therefore, option A is incorrect.

Autolock is the feature that automatically locks a device after a period of inactivity or when the power button is pressed. It can prevent unauthorized access to a device by requiring a passcode, pattern, fingerprint, or face

recognition to unlock it. However, it does not protect the data stored on the device from being extracted by other means. Therefore, option B is incorrect.

Two-factor authentication is the method of verifying a user's identity by requiring two pieces of evidence, such as a password and a code sent to a phone or email. It can enhance the security of online accounts and services, but it does not apply to the data stored on a device. Therefore, option D is incorrect.

Reference:

CompTIA Network+ N10-008 Study Guide, Chapter 9: Network Security, pages 403-404, 407-408, 411-412.

Professor Messer's Network+ Video Course, Section 5.1: Network Security Devices and Technologies, videos 5.1.1 - 5.1.3, 5.1.6, 5.1.7.

CompTIA Network+ (N10-008) Sample Questions, Question 15.

Valid N10-008 Dumps shared by BraindumpsPass.com for Helping Passing N10-008 Exam!

BraindumpsPass.com now offer the **newest N10-008 exam dumps**, the BraindumpsPass.com N10-008 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com N10-008 dumps with Test Engine here: <https://www.braindumpspass.com/CompTIA/N10-008-practice-exam-dumps.html> (**1075** Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)