

CompTIA

Exam Questions N10-009

CompTIA Network+ Exam



NEW QUESTION 1

- (Exam Topic 1)

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

Explanation:

A hot site is a fully redundant site that can take over operations immediately if the primary site goes down. In this scenario, the company has set up two different datacenters across the country that are current on data and applications, and they can immediately switch from one datacenter to another in case of an outage.

References:

> Network+ N10-008 Objectives: 1.5 Compare and contrast disaster recovery concepts and methodologies.

NEW QUESTION 2

- (Exam Topic 1)

Which of the following TCP ports is used by the Windows OS for file sharing?

- A. 53
- B. 389
- C. 445
- D. 1433

Answer: C

Explanation:

TCP port 445 is used by the Windows OS for file sharing. It is also known as SMB (Server Message Block) or CIFS (Common Internet File System) and allows users to access files, printers, and other shared resources on a network. References:

<https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smb>

NEW QUESTION 3

- (Exam Topic 1)

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

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 4

- (Exam Topic 1)

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

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 5

- (Exam Topic 1)

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

- A. Layer 1
- B. Layer 2
- C. Layer 3
- D. Layer 4

Answer: C

Explanation:

An IP header can be found at the third layer of the OSI model, also known as the network layer. This layer is responsible for logical addressing, routing, and forwarding of data packets.

References:

➤ CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: Network Models, p. 82

NEW QUESTION 6

- (Exam Topic 1)

A workstation is configured with the following network details:

IP address	Subnet mask	Default gateway
10.1.2.23	10.1.2.0/27	10.1.2.1

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

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

Answer: D

Explanation:

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

NEW QUESTION 7

- (Exam Topic 1)

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

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>

NEW QUESTION 8

- (Exam Topic 1)

A network administrator discovers that users in an adjacent building are connecting to the company's guest wireless network to download inappropriate material. Which of the following can the administrator do to MOST easily mitigate this issue?

- A. Reduce the wireless power levels
- B. Adjust the wireless channels
- C. Enable wireless client isolation
- D. Enable wireless port security

Answer: A

Explanation:

Reducing the wireless power levels can limit the range of the guest wireless network and prevent users in an adjacent building from connecting to it. Adjusting the wireless channels or enabling wireless client isolation will not affect the signal strength or coverage of the guest network. Enabling wireless port security will not work on a guest network that does not use authentication or MAC address filtering. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 2.0 Network Operations, Objective 2.5 Given a scenario, implement appropriate wireless configuration settings; Guest WiFi Security - Cisco Umbrella

NEW QUESTION 9

- (Exam Topic 1)

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

- A. An incident response plan
- B. A business continuity plan
- C. A change management policy

D. An acceptable use policy

Answer: C

Explanation:

A change management policy is a document that outlines the procedures and guidelines for making changes to a network or system, including how changes are approved, tested, and implemented. By following a change management policy, organizations can ensure that unnecessary modifications to the network are not permitted and version control is maintained. References:

➤ Network+ N10-008 Objectives: 1.6 Given a scenario, implement network configuration and change management best practices.

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: B

Explanation:

The most effective security mechanism against physical intrusions due to stolen credentials would likely be a combination of several of these options. However, of the options provided, the most effective security mechanism would probably be an access control vestibule. An access control vestibule is a secure area that is located between the outer perimeter of a facility and the inner secure area. It is designed to provide an additional layer of security by requiring that individuals pass through a series of security checks before being allowed access to the secure area. This could include biometric authentication, access card readers, and motion detection cameras.

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

NEW QUESTION 10

- (Exam Topic 1)

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

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 15

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 20

- (Exam Topic 1)

A technician is configuring a network switch to be used in a publicly accessible location. Which of the following should the technician configure on the switch to prevent unintended connections?

- A. DHCP snooping
- B. Geofencing
- C. Port security
- D. Secure SNMP

Answer: C

Explanation:

Port security is a feature that restricts input to a switch port by limiting and identifying MAC addresses of the devices allowed to access the port. This prevents unintended connections from unauthorized devices or spoofed MAC addresses. Port security can also be configured to take actions such as shutting down the port or sending an alert when a violation occurs. 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.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-10/configuration_guide/se

NEW QUESTION 24

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 25

- (Exam Topic 1)

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: B

Explanation:

A default gateway is a device that routes traffic from one network to another network, such as the Internet. A default gateway is usually configured on each host device to specify the IP address of the router that connects the host's network to other networks. In this case, the user's device and the destination device are on different networks (192.168.1.0/24 and 192.168.2.0/24), so the user needs to configure a default gateway on their device to reach the destination device.

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 29

- (Exam Topic 1)

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

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

Answer: A

Explanation:

CVE stands for Common Vulnerabilities and Exposures, which is a list of publicly disclosed cybersecurity vulnerabilities that is free to search, use, and incorporate into products and services. CVE provides a standardized identifier and description for each vulnerability, as well as references to related sources of information.

CVE helps to track and document various types of known vulnerabilities and facilitates communication and coordination among security professionals. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://cve.mitre.org/cve/>

NEW QUESTION 30

- (Exam Topic 1)

After the A record of a public website was updated, some visitors were unable to access the website. Which of the following should be adjusted to address the issue?

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

Answer: A

Explanation:

TTL (Time To Live) should be adjusted to address the issue of some visitors being unable to access the website after the A record was updated. TTL is a value that specifies how long a DNS record should be cached by DNS servers and clients before it expires and needs to be refreshed. If the TTL is too high, some DNS

servers and clients may still use the old A record that points to the previous IP address of the website, resulting in connection failures. By lowering the TTL, the DNS servers and clients will update their cache more frequently and use the new A record that points to the current IP address of the website. References: <https://www.cloudflare.com/learning/dns/dns-records/dns-ttl/>

NEW QUESTION 31

- (Exam Topic 1)

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: A

Explanation:

Zero Trust is a security framework that requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust prevents attackers from moving laterally through a system by applying granular policies and controls based on the principle of least privilege and by segmenting and encrypting data flows across the network. 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.crowdstrike.com/cybersecurity-101/zero-trust-security/>

NEW QUESTION 33

- (Exam Topic 1)

A technician receives feedback that some users are experiencing high amounts of jitter while using the wireless network. While troubleshooting the network, the technician uses the ping command with the IP address of the default gateway and verifies large variations in latency. The technician thinks the issue may be interference from other networks and non-802.11 devices. Which of the following tools should the technician use to troubleshoot the issue?

- A. NetFlow analyzer
- B. Bandwidth analyzer
- C. Protocol analyzer
- D. Spectrum analyzer

Answer: D

Explanation:

A spectrum analyzer is a tool that measures the frequency and amplitude of signals in a wireless network. It can be used to troubleshoot issues related to interference from other networks and non-802.11 devices, such as microwave ovens or cordless phones, by identifying the sources and levels of interference in the wireless spectrum. A spectrum analyzer can also help to optimize the channel selection and placement of wireless access points. 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.flukenetworks.com/blog/cabling-chronicles/what-spectrum-analyzer-and-how-do-you-use-it>

NEW QUESTION 38

- (Exam Topic 1)

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

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

Answer: C

Explanation:

The maximum transmission unit (MTU) is the largest size of a data packet that can be transmitted over a network. A standard Ethernet frame supports an MTU of 1500 bytes, which is the default value for most Ethernet networks. Larger MTUs are possible with jumbo frames, but they are not widely supported and may cause fragmentation or compatibility issues. 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/Maximum_transmission_unit

NEW QUESTION 43

- (Exam Topic 1)

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

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 46

- (Exam Topic 1)

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

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 47

- (Exam Topic 1)

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

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 50

- (Exam Topic 1)

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

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

Answer: D

Explanation:

In a star topology, all devices on a network connect to a central hub or switch, which acts as a common connection point. Ethernet LANs typically use a star topology, with each device connected to a central switch. References:

➤ Network+ N10-008 Objectives: 2.2 Explain common logical network topologies and their characteristics.

NEW QUESTION 55

- (Exam Topic 1)

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: A

Explanation:

NIC teaming, also known as network interface card teaming or link aggregation, allows multiple network interface cards to be grouped together to provide redundancy and increased throughput. In the event of a port failure on a switch, NIC teaming ensures that the file server remains connected to the LAN by automatically switching to another network interface card.

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

NEW QUESTION 58

- (Exam Topic 1)

SIMULATION

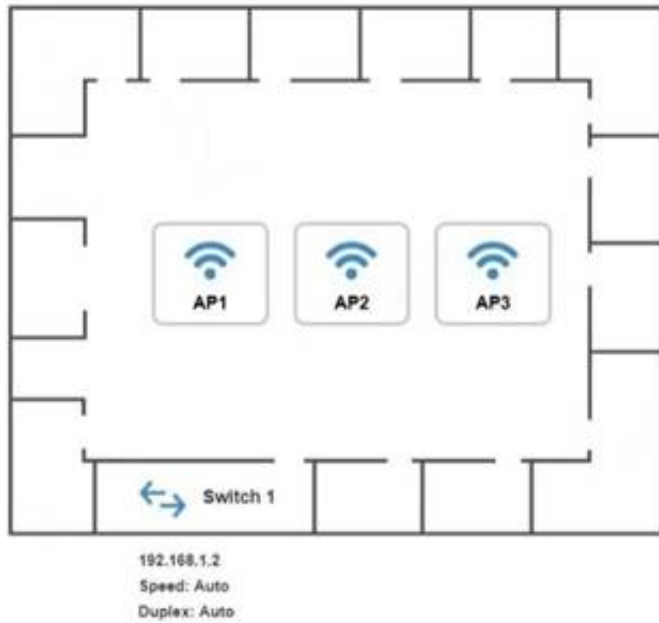
You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

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.



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

- A. Mastered
B. Not Mastered

Answer: A

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

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

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

S3cr3t!

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

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

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

Security Settings

☐ None

☐ WEP

☐ WPA

☐ WPA2

☒ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

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

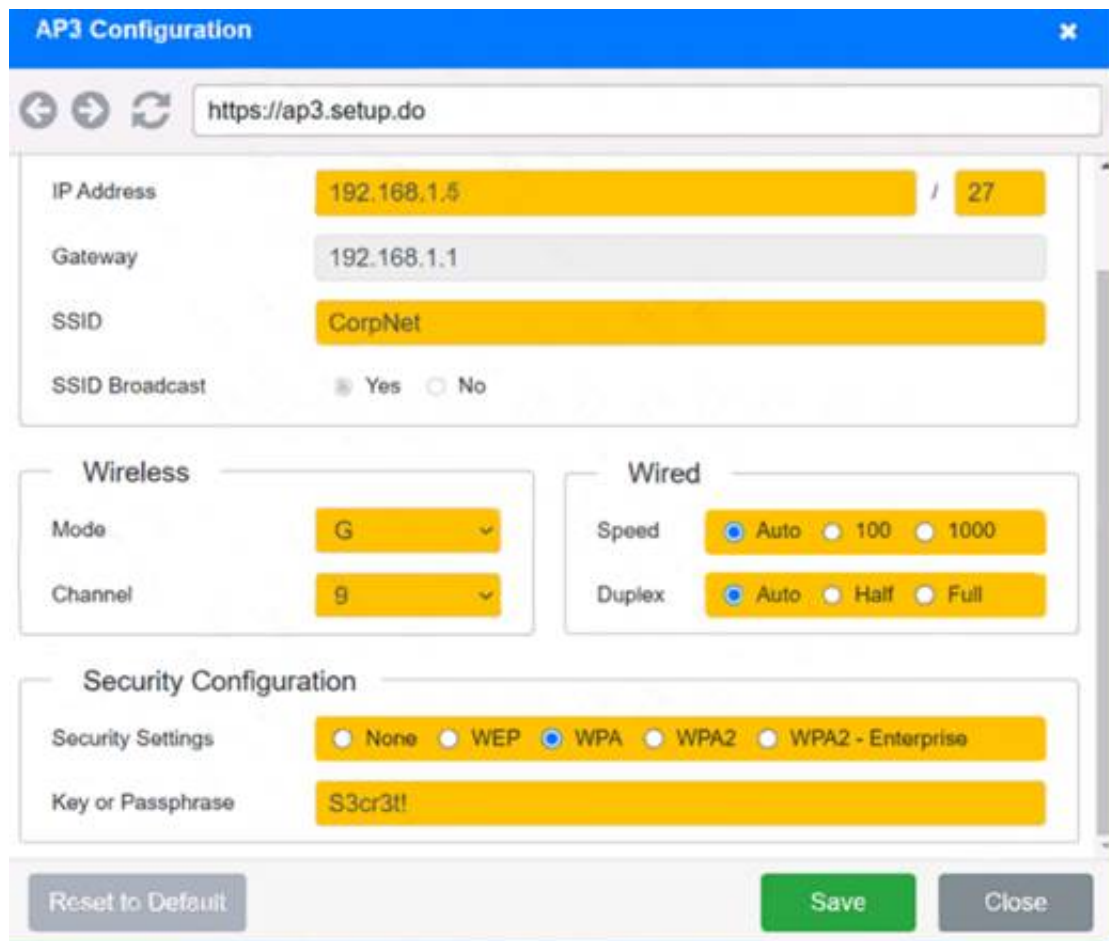
Key or Passphrase

S3cr3t!

Graphical user interface Description automatically generated

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>



The image shows a web-based configuration interface for an AP3 device. The window title is "AP3 Configuration". The address bar shows "https://ap3.setup.do". The configuration is divided into several sections:

- General Settings:**
 - 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!

At the bottom, there are three buttons: "Reset to Default", "Save", and "Close".

NEW QUESTION 59

- (Exam Topic 1)

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

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

Answer: B

Explanation:

BGP (Border Gateway Protocol) is a routing protocol used to exchange route information between public autonomous systems (AS). OSPF (Open Shortest Path First), EGRIP (Enhanced Interior Gateway Routing Protocol), and RIP (Routing Information Protocol) are all used for internal routing within a single AS. Therefore, BGP is the correct option to choose for this question.

References:

- > Network+ N10-007 Certification Exam Objectives, Objective 3.3: Given a scenario, configure and apply the appropriate routing protocol.
- > Cisco: Border Gateway Protocol (BGP) Overview

NEW QUESTION 61

- (Exam Topic 1)

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

Explanation:

Tailgating is a physical security attack where an unauthorized person follows an authorized person into a restricted area without proper identification or authorization. The network administrator prevented this attack by stopping and directing the person to the security desk. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 3.0 Network Security, Objective 3.1 Compare and contrast risk-related concepts.

NEW QUESTION 63

- (Exam Topic 1)

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

Explanation:

When evaluating a firewall to protect a datacenter's east-west traffic, it is important to consider traffic between VMs running on different hosts. This type of traffic is referred to as east-west traffic and is often protected by internal firewalls. By implementing firewalls, an organization can protect their internal network against

threats such as lateral movement, which can be caused by attackers who have breached a perimeter firewall. References: Network+ Certification Study Guide, Chapter 5: Network Security

NEW QUESTION 68

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 72

- (Exam Topic 1)

Which of the following connector types would have the MOST flexibility?

- A. SFP
- B. BNC
- C. LC
- D. RJ45

Answer: A

Explanation:

SFP (Small Form-factor Pluggable) is a connector type that has the most flexibility. It is a hot-swappable transceiver that can support different speeds, distances, and media types depending on the module inserted. It can be used for both copper and fiber connections and supports various protocols such as Ethernet, Fibre Channel, and SONET. References: <https://www.fs.com/what-is-sfp-transceiver-aid-11.html>

NEW QUESTION 76

- (Exam Topic 1)

Which of the following would MOST likely be used to review previous upgrades to a system?

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

Answer: B

Explanation:

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

NEW QUESTION 80

- (Exam Topic 1)

The following configuration is applied to a DHCP server connected to a VPN concentrator:

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 81

- (Exam Topic 1)

A network administrator needs to query the NSs for a remote application. Which of the following commands would BEST help the administrator accomplish this

task?

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

Answer: A

Explanation:

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

NEW QUESTION 82

- (Exam Topic 2)

Which of the following uses the destination IP address to forward packets?

- A. A bridge
- B. A Layer 2 switch
- C. A router
- D. A repeater

Answer: C

Explanation:

A router is a device that uses the destination IP address to forward packets between different networks. A bridge and a Layer 2 switch operate at the data link layer and use MAC addresses to forward frames within the same network. A repeater is a device that amplifies or regenerates signals at the physical layer.

NEW QUESTION 86

- (Exam Topic 2)

A business is using the local cable company to provide Internet access. Which of the following types of cabling will the cable company MOST likely use from the demarcation point back to the central office?

- A. Multimode
- B. Cat 5e
- C. RG-6
- D. Cat 6
- E. 100BASE-T

Answer: C

Explanation:

RG-6 is a type of coaxial cable that is commonly used by cable companies to provide Internet access from the demarcation point back to the central office. It has a thicker conductor and better shielding than RG-59, which is another type of coaxial cable. Multimode and Cat 5e are types of fiber optic and twisted pair cables respectively, which are not typically used by cable companies. Cat 6 and 100BASE-T are standards for twisted pair cables, not types of cabling.

NEW QUESTION 89

- (Exam Topic 2)

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

Explanation:

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.

References:

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

NEW QUESTION 93

- (Exam Topic 2)

A network administrator is reviewing interface errors on a switch. Which of the following indicates that a switchport is receiving packets in excess of the configured MTU?

- A. CRC errors
- B. Giants
- C. Runts
- D. Flooding

Answer: B

Explanation:

Giants are packets that exceed the configured MTU (Maximum Transmission Unit) of a switchport or interface, which causes them to be dropped or fragmented by the switch or router. The MTU is the maximum size of a packet that can be transmitted without fragmentation on a given medium or protocol. Giants can indicate misconfiguration or mismatch of MTU values between devices or interfaces on a network, which can cause performance issues or errors. CRC errors are errors that occur when the cyclic redundancy check (CRC) value of a packet does not match the calculated CRC value at the destination, which indicates corruption or alteration of data during transmission due to noise, interference, faulty cabling, etc., but not necessarily exceeding MTU values. Runts are packets that are smaller than the minimum size allowed by the medium or protocol, which causes them to be dropped or ignored by the switch or router. Flooding is a technique where a switch sends packets to all ports except the source port when it does not have an entry for the destination MAC address in its MAC address table, which can cause congestion or broadcast storms on a network.

NEW QUESTION 95

- (Exam Topic 2)

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

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

Answer: E

Explanation:

Using an out-of-band access method is the best way to prevent unauthorized access to the legacy switches that do not support cryptographic functions. Out-of-band access is a method of accessing a network device through a dedicated channel that is separate from the main network traffic. Out-of-band access can use physical connections such as serial console ports or dial-up modems, or logical connections such as VPNs or firewalls. Out-of-band access provides more security and reliability than in-band access, which uses the same network as the data traffic and may be vulnerable to attacks or failures. References:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15mt/fundamentals-15-mt-book/>

NEW QUESTION 97

- (Exam Topic 2)

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.
- C. The technician can move the computer to another zone or request an exception from the administrator.
- D. 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.
- E. 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: B

Explanation:

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. References:

<https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

NEW QUESTION 99

- (Exam Topic 2)

Which of the following protocol types describes secure communication on port 443?

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

Answer: C

Explanation:

TCP is the protocol type that describes secure communication on port 443. TCP (Transmission Control Protocol) is a connection-oriented protocol that provides reliable and ordered delivery of data packets over an IP network. TCP uses port numbers to identify different applications or services on a device. Port 443 is the default port for HTTPS (Hypertext Transfer Protocol Secure), which is an extension of HTTP that uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security) encryption to protect data in transit between a web server and a web browser. References:

<https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION 102

- (Exam Topic 2)

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

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 AP1. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html> 1

NEW QUESTION 103

- (Exam Topic 2)

A wireless network was installed in a warehouse for employees to scan crates with a wireless handheld scanner. The wireless network was placed in the corner of the building near the ceiling for maximum coverage. However, users in the offices adjacent to the warehouse have noticed a large amount of signal overlap from the new network. Additionally, warehouse employees report difficulty connecting to the wireless network from the other side of the building; however, they have no issues when they are near the antenna. Which of the following is MOST likely the cause?

- A. The wireless signal is being refracted by the warehouse's windows
- B. The antenna's power level was set too high and is overlapping
- C. An omnidirectional antenna was used instead of a unidirectional antenna
- D. The wireless access points are using channels from the 5GHz spectrum

Answer: C

Explanation:

An omnidirectional antenna was used instead of a unidirectional antenna, which is most likely the cause of the wireless network issues. An omnidirectional antenna provides wireless coverage in all directions from the antenna, which can cause signal overlap with adjacent offices and interference with other wireless networks. A unidirectional antenna, on the other hand, provides wireless coverage in a specific direction from the antenna, which can reduce signal overlap and interference and increase signal range and quality. A unidirectional antenna would be more suitable for a warehouse environment where users are located on one side of the building1. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html> 1

NEW QUESTION 107

- (Exam Topic 2)

An organization wants to implement a method of centrally managing logins to network services. Which of the following protocols should the organization use to allow for authentication, authorization, and auditing?

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

Answer: B

Explanation:

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

NEW QUESTION 110

- (Exam Topic 2)

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

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>

NEW QUESTION 111

- (Exam Topic 2)

Which of the following policies is MOST commonly used for guest captive portals?

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

Answer: A

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 112

- (Exam Topic 2)

Which of the following is a system that is installed directly on a server's hardware and abstracts the hardware from any guest machines?

- A. Storage array
- B. Type 1 hypervisor
- C. Virtual machine
- D. Guest QS

Answer: B

Explanation:

A type 1 hypervisor is a system that is installed directly on a server's hardware and abstracts the hardware from any guest machines. A hypervisor is a software layer that enables virtualization by creating and managing virtual machines (VMs) on a physical host. A type 1 hypervisor, also known as a bare-metal hypervisor or a native hypervisor, runs directly on the host's hardware without requiring an underlying operating system (OS). It provides better performance and security than a type 2 hypervisor, which runs on top of an existing OS and relies on it for hardware access. References:

<https://www.vmware.com/topics/glossary/content/hypervisor>

NEW QUESTION 114

- (Exam Topic 2)

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

Explanation:

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 119

- (Exam Topic 2)

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

Explanation:

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

NEW QUESTION 124

- (Exam Topic 2)

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

Explanation:

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

NEW QUESTION 125

- (Exam Topic 2)

An IDS was installed behind the edge firewall after a network was breached. The network was then breached again even though the IDS logged the attack. Which of the following should be used in place of these devices to prevent future attacks?

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

Answer: C

Explanation:

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

NEW QUESTION 126

- (Exam Topic 2)

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

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

Answer: C

Explanation:

Role-based access is a security capability that assigns permissions to users based on their roles or functions within an organization. It allows the network administrator to maintain these permissions with the least administrative effort, as they only need to configure the security groups for each role once and then assign users to those groups. Mandatory access control is a security capability that assigns permissions based on security labels or classifications, which requires more administrative effort to maintain. User-based permissions are a security capability that assigns permissions to individual users, which is not scalable or efficient for large organizations. Least privilege is a security principle that states that users should only have the minimum level of access required to perform their tasks, which is not a security capability by itself.

NEW QUESTION 131

- (Exam Topic 2)

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: C

Explanation:

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 134

- (Exam Topic 2)

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: C

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 137

- (Exam Topic 2)

Which of the following OSI model layers is where conversations between applications are established, coordinated, and terminated?

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

Answer: A

Explanation:

Reference: <https://www.techtarget.com/searchnetworking/definition/OSI#:~:text=The%20session%20layer,and%20termina>

The session layer is where conversations between applications are established, coordinated, and terminated. It is responsible for creating, maintaining, and ending sessions between different devices or processes. The physical layer deals with the transmission of bits over a medium. The presentation layer formats and translates data for different applications. The data link layer provides reliable and error-free delivery of frames within a network.

NEW QUESTION 138

- (Exam Topic 2)

During the security audit of a financial firm the Chief Executive Officer (CEO) questions why there are three employees who perform very distinct functions on the server. There is an administrator for creating users another for assigning the users to groups and a third who is the only administrator to perform file rights assignment Which of the following mitigation techniques is being applied'

- A. Privileged user accounts
- B. Role separation
- C. Container administration
- D. Job rotation

Answer: B

Explanation:

Role separation is a security principle that involves dividing the tasks and privileges for a specific business process among multiple users. This reduces the risk of fraud and errors, as no one user has complete control over the process. In the scenario, there are three employees who perform very distinct functions on the server, which is an example of role separation. References: <https://hyperproof.io/resource/segregation-of-duties/>

NEW QUESTION 142

- (Exam Topic 2)

A technician is deploying a low-density wireless network and is contending with multiple types of building materials. Which of the following wireless frequencies would allow for the LEAST signal attenuation?

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

Answer: A

Explanation:

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

NEW QUESTION 146

- (Exam Topic 2)

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: D

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 10m1s. 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 147

- (Exam Topic 2)

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: B

Explanation:

* 255.255.252.1 is a subnet mask that allows for 1022 network-connected devices on the same subnet, which is the smallest subnet that can accommodate 412 devices. The subnet mask determines how many bits are used for the network portion and how many bits are used for the host portion of an IP address. A smaller subnet mask means more bits are used for the network portion and less bits are used for the host portion, which reduces the number of available hosts on the subnet. 255.255.0.0 allows for 65534 hosts on the same subnet, which is too large. 255.255.254.0 allows for 510 hosts on the same subnet, which is also too large. 255.255.255.0 allows for 254 hosts on the same subnet, which is too small.

NEW QUESTION 148

- (Exam Topic 2)

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

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 151

- (Exam Topic 2)

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

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

Answer: B

Explanation:

netstat -a is a command that displays information about active TCP connections and listening ports on a system. A network administrator can use netstat -a to check if the database engine is listening on a certain port, as well as verify if there are any connections established to or from that port. References:

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

NEW QUESTION 155

- (Exam Topic 2)

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

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

Answer: B

Explanation:

The default gateway is the setting that the user most likely misconfigured on the PC that caused it to be unable to access websites by both FQDN and IP. The default gateway is a device, usually a router or a firewall, that connects a local network to other networks such as the Internet. It acts as an intermediary between devices on different networks and forwards packets based on their destination IP addresses. If the default gateway is not configured correctly on a PC, it will not be able to communicate with devices outside its local network, such as web servers or DNS servers. References:

<https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/16448-default-gateway.html>

NEW QUESTION 160

- (Exam Topic 2)

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

Explanation:

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. References: <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-work>

NEW QUESTION 163

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 165

- (Exam Topic 2)

A company wants to implement a large number of WAPs throughout its building and allow users to be able to move around the building without dropping their connections Which of the following pieces of equipment would be able to handle this requirement?

- A. A VPN concentrator
- B. A load balancer
- C. A wireless controller
- D. A RADIUS server

Answer: C

Explanation:

A wireless controller would be able to handle the requirement of implementing a large number of WAPs throughout the building and allowing users to move around without dropping their connections. A wireless controller is a device that centrally manages and configures multiple wireless access points (WAPs) on a network. It can provide features such as load balancing, roaming, security, QoS, and monitoring for the wireless network. A wireless controller can also support wireless mesh networks, where some WAPs act as relays for other WAPs to extend the wireless coverage. References: <https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/index.html>

NEW QUESTION 166

- (Exam Topic 3)

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: CD

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 169

- (Exam Topic 3)

A network technician needs to ensure the company's external mail server can pass reverse lookup checks. Which of the following records would the technician

MOST likely configure? (Choose Correct option and give explanation directly from CompTIA Network+ Study guide or documents)

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

Answer: A

Explanation:

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

NEW QUESTION 170

- (Exam Topic 3)

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

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 171

- (Exam Topic 3)

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: D

NEW QUESTION 174

- (Exam Topic 3)

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

Explanation:

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.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.9: Compare and contrast common network service types.

NEW QUESTION 178

- (Exam Topic 3)

An administrator is investigating reports of network slowness in a building. While looking at the uplink interface statistics in the switch's CLI, the administrator discovers the uplink is at 100% utilization. However, the administrator is unsure how to identify what traffic is causing the saturation. Which of the following tools should the administrator utilize to identify the source and destination addresses of the traffic?

- A. SNMP
- B. Traps
- C. Syslog
- D. NetFlow

Answer: D

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 181

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 182

- (Exam Topic 3)

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: B

Explanation:

To prevent IP address conflicts when allocating a portion of a DHCP scope's subnet for statically assigned devices, it is recommended to use the concept of DHCP exclusion ranges. DHCP exclusion ranges allow a DHCP administrator to specify a range of IP addresses within the scope that should not be assigned to DHCP clients. This can be useful in situations where some devices on the network need to be assigned static IP addresses, as it ensures that the statically assigned addresses do not overlap with addresses assigned by the DHCP server. To set up a DHCP exclusion range, the administrator needs to specify the start and end IP addresses of the range, as well as the subnet mask. The DHCP server will then exclude the specified range of addresses from its pool of available addresses, and will not assign them to DHCP clients. By using DHCP exclusion ranges, the technician can ensure that the statically assigned addresses do not conflict with addresses assigned by the DHCP server, and can prevent IP address conflicts on the network.

Anthony Sequeira

"Another frequent configuration you might make in a DHCP implementation is to configure an exclusion range. This is a portion of the address pool that you never want leased out to clients in the network. Perhaps you have numbered your servers 192.168.1.1–192.168.1.10. Because the servers are statically configured with these addresses, you exclude these addresses from the 192.168.1.0/24 pool of addresses."

Mike Meyers

"Exclusion ranges represent an IP address or range of IP addresses from the pool of addresses that are not to be given out by the DHCP server. Exclusions should be made for the static addresses manually configured on servers and router interfaces, so these IP addresses won't be offered to DHCP clients."

NEW QUESTION 186

- (Exam Topic 3)

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? (Select TWO).

- A. 22
- B. 23
- C. 69
- D. 443
- E. 587
- F. 8080

Answer: BC

NEW QUESTION 187

- (Exam Topic 3)

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

Explanation:

* 802.11 g 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 190

- (Exam Topic 3)

A network administrator notices excessive wireless traffic occurring on an access point after normal business hours. The access point is located on an exterior wall. Which of the following should the administrator do to limit wireless access outside the building?

- A. Set up a private VLAN.
- B. Disable roaming on the WAP.
- C. Change to a directional antenna.
- D. Stop broadcasting of the SSID.

Answer: C

Explanation:

A directional antenna is a type of antenna that radiates or receives radio waves in a specific direction. This can help limit wireless access outside the building by focusing the signal towards the intended area and reducing the signal strength in other directions. A private VLAN is a feature that isolates network devices within a VLAN. Disabling roaming on the WAP prevents wireless clients from switching to another WAP when the signal is weak. Stopping broadcasting of the SSID hides the network name from wireless clients, but does not prevent them from connecting if they know the SSID.

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 192

- (Exam Topic 3)

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

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 197

- (Exam Topic 3)

Which of the following would MOST likely utilize PoE?

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

Answer: A

Explanation:

A camera is most likely to utilize PoE (Power over Ethernet). PoE is a technology that allows electrical power to be delivered over Ethernet cables. It is used to power a variety of devices, such as cameras, phones, access points, and other networking equipment. Cameras are particularly well-suited for PoE because they are often installed in locations where it is difficult or impossible to run electrical power. By using PoE, cameras can be powered directly over the Ethernet cable, eliminating the need for separate power cables and outlets. Other devices, such as printers, hubs, and modems, are less likely to utilize PoE because they typically do not need to be powered over Ethernet. These devices are usually powered by AC (alternating current) power and are typically connected to a power outlet rather than an Ethernet cable.

NEW QUESTION 202

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 207

- (Exam Topic 3)

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: A

Explanation:

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 208

- (Exam Topic 3)

A technician installed an 8-port switch in a user's office. The user needs to add a second computer in the office, so the technician connects both PCs to the switch and connects the switch to the wall jack. However, the new PC cannot connect to network resources. The technician then observes the following:

- The new computer does not get an IP address on the client's VLAN.
- Both computers have a link light on their NICs.
- The new PC appears to be operating normally except for the network issue.
- The existing computer operates normally.

Which of the following should the technician do NEXT to address the situation?

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

Answer: A

NEW QUESTION 212

- (Exam Topic 3)

Which of the following devices is used to configure and centrally manage access points installed at different locations?

- A. Wireless controller
- B. Load balancer
- C. Proxy server
- D. VPN concentrator

Answer: A

Explanation:

Access points (APs) can be configured and centrally managed using a wireless LAN controller (WLC). A WLC is a device that connects to multiple APs and provides centralized management and control of those APs. The WLC can be used to configure settings such as wireless network parameters, security settings, and quality of service (QoS) policies. Additionally, the WLC can be used to monitor the status of connected APs, track client connections, and gather statistics on network usage. Some vendors such as Cisco, Aruba, Ruckus, etc. provide wireless LAN controllers as part of their wireless networking solutions.

NEW QUESTION 215

- (Exam Topic 3)

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. Allow connections only to an internal proxy server.
- B. Deploy an IDS system and place it in line with the traffic.
- C. Create a screened network and move the devices to it.
- D. Use a host-based network firewall on each device.

Answer: A

Explanation:

An internal proxy server is a server that acts as an intermediary between internal devices and external servers on the internet. An internal proxy server can be used to limit the ability of devices to perform only HTTPS connections to an internet update server by filtering and forwarding the requests and responses based on predefined rules or policies. An internal proxy server can also prevent the devices from being exposed to the public internet by hiding their IP addresses and providing a layer of security and privacy.

NEW QUESTION 220

- (Exam Topic 3)

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

Explanation:

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 225

- (Exam Topic 3)

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

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

Answer: C

Explanation:

To monitor and provide traffic segmentation across the network, a technician may use the concept of VLANs (Virtual Local Area Networks). VLANs are a way of dividing a single physical network into multiple logical networks, each with its own unique identifier or "tag."

By assigning each department a specific VLAN identifier, the technician can segment the network traffic and ensure that the different departments' traffic is kept separate from one another. This can help to improve network security, performance, and scalability, as well as allowing for better monitoring and control of the network traffic.

To implement VLANs, the technician will need to configure VLAN tagging on the network devices, such as switches and routers, and assign each department's devices to the appropriate VLAN. The technician may also need to configure VLAN trunking to allow the different VLANs to communicate with each other.

By using VLANs, the technician can effectively monitor and segment the network traffic, providing better control and visibility into the network.

NEW QUESTION 228

- (Exam Topic 3)

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

Explanation:

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

NEW QUESTION 229

- (Exam Topic 3)

A network administrator installed an additional IDF during a building expansion project. Which of the following documents need to be updated to reflect the change? (Select TWO).

- A. Data loss prevention policy
- B. BYOD policy
- C. Acceptable use policy
- D. Non-disclosure agreement
- E. Disaster recovery plan
- F. Physical network diagram

Answer: BF

NEW QUESTION 232

- (Exam Topic 3)

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

- A. 445
- B. 554
- C. 587
- D. 5060

Answer: B

Explanation:

RTSP stands for Real Time Streaming Protocol and is an application-level network protocol designed for controlling media playback on streaming media servers. RTSP uses the default transport layer port number 554 for both TCP and UDP1. Port 445 is used for SMB (Server Message Block), a protocol for file and printer sharing. Port 587 is used for SMTP (Simple Mail Transfer Protocol), a protocol for sending email messages. Port 5060 is used for SIP (Session Initiation Protocol), a protocol for initiating and managing multimedia sessions.

References: 1 Real Time Streaming Protocol - Wikipedia (https://en.wikipedia.org/wiki/Real_Time_Streaming_Protocol)

NEW QUESTION 236

- (Exam Topic 3)

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

Explanation:

VLAN (virtual LAN) tags are used to identify packets as belonging to a particular VLAN. VLANs are used to segment a network into logical sub-networks, and each VLAN is assigned a unique VLAN tag. If the VLAN tag is not configured correctly, the computer may not be able to access network resources.

NEW QUESTION 237

- (Exam Topic 3)

A network administrator would like to purchase a device that provides access ports to endpoints and has the ability to route between networks. Which of the following would be BEST for the administrator to purchase?

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

Answer: B

NEW QUESTION 240

- (Exam Topic 3)

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

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 242

- (Exam Topic 3)

A network technician is implementing a solution that will allow end users to gain access to multiple applications after logging on. Which of the following authentication methods would allow this type of access?

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

Answer: A

NEW QUESTION 243

- (Exam Topic 3)

A help desk technician is concerned that a client's network cable issues may be causing intermittent connectivity. Which of the following would help the technician determine if this is the issue?

- A. Run the show interface command on the switch
- B. Run the traceroute command on the server
- C. Run iperf on the technician's desktop
- D. Ping the client's computer from the router
- E. Run a port scanner on the client's IP address

Answer: A

Explanation:

To determine if a client's network cable issues may be causing intermittent connectivity, the help desk technician can run the show interface command on the switch. This command allows the technician to view the status and statistics of the various interfaces on the switch, including the physical link status and the number of transmitted and received packets. If the interface is experiencing a large number of errors or dropped packets, this could indicate a problem with the network cable or with the connection between the client's device and the switch.

"Cisco routers and switches have a show interfaces IOS command that provides interface statistics/status information, including link state (up/down), speed/duplex, send/receive traffic, cyclic redundancy checks (CRCs), and protocol packet and byte counts."

NEW QUESTION 248

- (Exam Topic 3)

Which of the following allows for an devices within a network to share a highly reliable time source?

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

Answer: A

Explanation:

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

NEW QUESTION 250

- (Exam Topic 3)

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: A

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 254

- (Exam Topic 3)

On a network with redundant switches, a network administrator replaced one of the switches but was unable to get a connection with another switch. Which of the following should the administrator check after successfully testing the cable that was wired for TIA/EIA-568A on both ends?

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

Answer: A

Explanation:

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

NEW QUESTION 256

- (Exam Topic 3)

A network administrator needs to provide evidence to confirm that recent network outages were caused by increased traffic generated by a recently released application. Which of the following actions will BEST support the administrator's response?

- A. Generate a network baseline report for comparison.
- B. Export the firewall traffic logs.
- C. Collect the router's NetFlow data.
- D. Plot interface statistics for dropped packets.

Answer: C

NEW QUESTION 259

- (Exam Topic 3)

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

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 261

- (Exam Topic 3)

A new company recently moved into an empty office space. Within days, users in the next 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

NEW QUESTION 264

- (Exam Topic 3)

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

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 268

- (Exam Topic 3)

An IT technician needs to increase bandwidth to a server. The server has multiple gigabit ports. Which of the following can be used to accomplish this without replacing hardware?

- A. STP
- B. 802.1Q
- C. Duplex
- D. LACP

Answer: D

Explanation:

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

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.5: Compare and contrast network cabling types, standards and speeds.

NEW QUESTION 272

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 277

- (Exam Topic 3)

A Network engineer is investigating issues on a Layer 2 Switch. The department typically snares 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

NEW QUESTION 278

- (Exam Topic 3)

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

NEW QUESTION 280

- (Exam Topic 3)

A Wi-Fi network was originally configured to be able to handle interference from a microwave oven. The microwave oven was recently removed from the office. Now the network administrator wants to optimize the system to maximize the range of the signal. The main sources of signal degradation are the numerous cubicles and wooden walls between the WAP and the intended destination. Which of the following actions should the administrator take?

- A. Implement CDMA.
- B. Change from omni to directional.
- C. Change the SSID.
- D. Change the frequency.

Answer: D

Explanation:

- the microwave was already removed from the office
- the signal is OK now
- Notice that the question mentions "numerous cubicles and wooden walls" - meaning the signal now won't have the interference as before
- KEY POINT: the admin wants to "maximize the range of the signal:"
Manually change the frequency to 2.4 GHz for more reliable speeds and range. While 5 GHz gives you a stronger signal, it doesn't travel through walls or ceilings as well, so it doesn't give you the best range.
"Microwave ovens: Older microwave ovens, which might not have sufficient shielding, can emit relatively high-powered signals in the 2.4GHz band, resulting in significant interference with WLAN devices operating in the 2.4GHz band."

NEW QUESTION 281

- (Exam Topic 3)

A company wants to add a local redundant data center to its network in case of failure at its primary location. Which of the following would give the LEAST amount of redundancy for the company's network?

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

Answer: A

NEW QUESTION 285

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 286

- (Exam Topic 3)

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

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 287

- (Exam Topic 3)

A network technician recently installed 35 additional workstations. After installation, some users are unable to access network resources. Many of the original workstations that are experiencing the network access issue were offline when the new workstations were turned on. Which of the following is the MOST likely cause of this issue?

- A. Incorrect VLAN setting
- B. Insufficient DHCP scope
- C. Improper NIC setting
- D. Duplicate IP address

Answer: B

NEW QUESTION 292

- (Exam Topic 3)

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

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

Answer: B

Explanation:

The best choice for configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch is to use full duplex and 1GB speed for all interfaces that are participating in the link aggregation. This will allow for maximum throughput, as the full duplex connection will enable simultaneous sending and receiving of data, and the 1GB speed will ensure that the data is transferred quickly.

According to the CompTIA Network+ Study Guide, "Full-duplex Ethernet allows the network adapter to transmit and receive data simultaneously, which can result in double the bandwidth of half-duplex Ethernet." Additionally, the official text states, "Ethernet and Fast Ethernet use different speeds for data transmission, with Ethernet being 1,000 megabits (1 gigabit) per second and Fast Ethernet being 100 megabits per second."

NEW QUESTION 295

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 299

- (Exam Topic 3)

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

Explanation:

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 302

- (Exam Topic 3)

A network technician is having issues connecting an IoT sensor to the internet. The WLAN settings were enabled via a custom command line, and a proper IP address assignment was received on the wireless 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 if an encryption protocol mismatch exists.
- B. Verifying if a captive portal is active for the WLAN.
- C. Verifying the minimum RSSI for operation in the device's documentation
- D. Verifying EIRP power settings on the access point.

Answer: C

Explanation:

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

NEW QUESTION 303

- (Exam Topic 3)

Which of the following is considered a physical security detection device?

- A. Cameras
- B. Biometric readers
- C. Access control vestibules
- D. Locking racks

Answer: A

NEW QUESTION 308

- (Exam Topic 3)

An administrator would like to allow Windows clients from outside the office to access workstations without using third-party software. Which of the following access methods would meet this requirement?

- A. Remote desktop gateway
- B. Split tunnel
- C. Site-to-site VPN
- D. VNC

Answer: A

Explanation:

To allow Windows clients from outside the office to access workstations without using third-party software, the administrator can use the Remote Desktop Protocol (RDP). RDP is a built-in feature of the Windows operating system that allows users to remotely connect to and control other Windows computers over a network connection.

To use RDP, the administrator will need to enable the Remote Desktop feature on the workstations that need to be accessed, and ensure that the appropriate firewall rules are in place to allow RDP traffic to pass through. The administrator will also need to provide the remote users with the necessary credentials to access the workstations.

Once RDP is set up and configured, the remote users can use the Remote Desktop client on their own computers to connect to the workstations and access them as if they were physically present in the office. This allows the administrator to provide remote access to the workstations without the need for any additional software or third-party tools.

NEW QUESTION 311

- (Exam Topic 3)

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: B

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 314

- (Exam Topic 3)

While walking 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

Explanation:

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 319

- (Exam Topic 3)

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

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 320

- (Exam Topic 3)

An ISP is unable to provide services to a user in a remote area through cable and DSL. Which of the following is the NEXT best solution to provide services without adding external infrastructure?

- A. Fiber
- B. Leased line
- C. Satellite
- D. Metro optical

Answer: C

Explanation:

If an ISP is unable to provide services to a user in a remote area through cable and DSL, the next best solution to provide services without adding external infrastructure would likely be satellite. Satellite is a wireless communication technology that uses a network of satellites orbiting the Earth to transmit and receive data. It is well-suited for providing connectivity to remote or rural areas where other types of infrastructure may not be available or may be cost-prohibitive to install.

NEW QUESTION 324

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 328

- (Exam Topic 3)

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

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

Answer: B

Explanation:

802.11b (Wi-Fi 1)
11 Mbps
100 meter maximum effective range
802.11a (Wi-Fi 2)
54 Mbps
50 meter maximum effective range

NEW QUESTION 331

- (Exam Topic 3)

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

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 336

- (Exam Topic 3)

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: C

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.

NEW QUESTION 337

- (Exam Topic 3)

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

Explanation:

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 341

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 346

- (Exam Topic 3)

A new office space is being designed. The network switches are up, but no services are running yet. A network engineer plugs in a laptop configured as a DHCP client to a switch. Which 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

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 351

- (Exam Topic 3)

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

Answer: D

NEW QUESTION 353

- (Exam Topic 3)

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: A

NEW QUESTION 356

- (Exam Topic 3)

A network technician is planning a network scope. The web server needs to be within 12.31 69.1 to 12.31.69.29. Which of the following would meet this requirement?

- A. Lease time
- B. Range reservation
- C. DNS
- D. Superscope

Answer: A

NEW QUESTION 359

- (Exam Topic 3)

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

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

Answer: A

Explanation:

Throughput is the actual amount of data that can be transferred over a network in a given time. Throughput can be affected by various factors such as congestion, interference, errors, or hardware limitations. If the throughput is lower than the configured internet connection speed, it can cause a significant delay in data transmission. The ISP should check the throughput and identify the source of the problem.

References: Network+ Study Guide Objective 2.2: Explain the concepts and characteristics of routing and switching.

NEW QUESTION 364

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

N10-009 Practice Exam Features:

- * N10-009 Questions and Answers Updated Frequently
- * N10-009 Practice Questions Verified by Expert Senior Certified Staff
- * N10-009 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * N10-009 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The N10-009 Practice Test Here](#)