



CompTIA

Exam Questions N10-009

CompTIA Network+ Exam

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

- (Topic 3)

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

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

Answer: B

Explanation:

The fire suppression system is a design consideration when building out an IDF because it can affect the safety and reliability of the network equipment and cabling. A fire suppression system is a system that detects and extinguishes fires in a building, using water, gas, or chemicals. Depending on the type of fire suppression system, it can have different impacts on the IDF design, such as:

? Water-based systems, such as sprinklers, can damage the network equipment and cabling if they are activated by a fire or a false alarm. Therefore, the IDF should be designed to protect the equipment and cabling from water exposure, such as using waterproof cabinets, drip pans, and conduits.

? Gas-based systems, such as clean agent systems, can displace the oxygen in the IDF and cause suffocation for anyone inside. Therefore, the IDF should be designed to allow for ventilation and air circulation, as well as warning signs and alarms to alert anyone in the IDF before the gas is released.

? Chemical-based systems, such as dry chemical systems, can leave a residue on the network equipment and cabling that can affect their performance and lifespan. Therefore, the IDF should be designed to minimize the contact between the chemical and the equipment and cabling, as well as provide a means for cleaning and restoring them after a fire.

The other options are not correct because:

? The source panel amperage is not a design consideration when building out an IDF, as it is determined by the electrical circuit and the power needs of the network equipment and cabling. The source panel amperage does not affect the layout, location, or protection of the IDF.

? The humidity levels are not a design consideration when building out an IDF, as they are controlled by the HVAC system and the ventilation of the IDF. The humidity levels do not affect the layout, location, or protection of the IDF.

? The cable transmission speeds are not a design consideration when building out an IDF, as they are determined by the type and quality of the network cabling and the network equipment. The cable transmission speeds do not affect the layout, location, or protection of the IDF.

NEW QUESTION 2

- (Topic 3)

A user in a branch office reports that access to all files has been lost after receiving a new PC. All other users in the branch can access fileshares. The IT engineer who is troubleshooting this incident is able to ping the workstation from the branch router, but the machine cannot ping the router. Which of the following is MOST likely the cause of the incident?

- A. Incorrect subnet mask
- B. Incorrect DNS server
- C. Incorrect IP class
- D. Incorrect TCP port

Answer: A

NEW QUESTION 3

- (Topic 3)

Which of the following protocols is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links?

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

Answer: A

NEW QUESTION 4

- (Topic 3)

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

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

Answer: A

NEW QUESTION 5

- (Topic 3)

Which of the following combinations of single cables and transceivers will allow a server to have 40GB of network throughput? (Select two).

- A. SFP+
- B. SFP
- C. QSFP+
- D. Multimode
- E. Cat 6a

F. Cat5e

Answer: CD

Explanation:

QSFP+ is a type of transceiver that supports 40 gigabit Ethernet (40GbE) over four lanes of 10 gigabit Ethernet (10GbE) each. QSFP+ stands for quad small form-factor pluggable plus, and it is a compact and hot-swappable module that plugs into a QSFP+ port on a network device. QSFP+ transceivers can support various types of cables and connectors, such as direct attach copper (DAC), active optical cable (AOC), or fiber optic cable. Multimode is a type of fiber optic cable that supports multiple modes of light propagation within the core. Multimode fiber optic cable can carry higher bandwidth and data rates than single-mode fiber optic cable, but over shorter distances. Multimode fiber optic cable is commonly used for short-reach applications, such as within a data center or a campus network. Multimode fiber optic cable can be paired with QSFP+ transceivers to achieve 40GbE connectivity.

The other options are not correct because they do not support 40GbE. They are:

? SFP+. SFP+ is a type of transceiver that supports 10 gigabit Ethernet (10GbE) over a single lane. SFP+ stands for small form-factor pluggable plus, and it is a compact and hot-swappable module that plugs into an SFP+ port on a network device. SFP+ transceivers can support various types of cables and connectors, such as direct attach copper (DAC), active optical cable (AOC), or fiber optic cable. However, SFP+ transceivers cannot support 40GbE by themselves, unless they are used in a breakout configuration with a QSFP+ transceiver.

? SFP. SFP is a type of transceiver that supports 1 gigabit Ethernet (1GbE) over a single lane. SFP stands for small form-factor pluggable, and it is a compact and hot-swappable module that plugs into an SFP port on a network device. SFP transceivers can support various types of cables and connectors, such as twisted-pair copper, coaxial cable, or fiber optic cable. However, SFP transceivers cannot support 40GbE by themselves, unless they are used in a breakout configuration with a QSFP+ transceiver.

? Cat 6a. Cat 6a is a type of twisted-pair copper cable that supports 10 gigabit Ethernet (10GbE) over distances up to 100 meters. Cat 6a stands for category 6 augmented, and it is an enhanced version of Cat 6 cable that offers better performance and reduced crosstalk. Cat 6a cable can be paired with 10Gbase-T transceivers to achieve 10GbE connectivity. However, Cat 6a cable cannot support 40GbE by itself, unless it is used in a breakout configuration with a QSFP+ transceiver.

? Cat 5e. Cat 5e is a type of twisted-pair copper cable that supports 1 gigabit Ethernet (1GbE) over distances up to 100 meters. Cat 5e stands for category 5 enhanced, and it is an improved version of Cat 5 cable that offers better performance and reduced crosstalk. Cat 5e cable can be paired with 1000base-T transceivers to achieve 1GbE connectivity. However, Cat 5e cable cannot support 40GbE by itself, unless it is used in a breakout configuration with a QSFP+ transceiver.

References1: QSFP+ - an overview | ScienceDirect Topics2: Multimode Fiber - an overview | ScienceDirect Topics3: Network+ (Plus) Certification | CompTIA IT Certifications4: SFP+ - an overview | ScienceDirect Topics5: SFP - an overview | ScienceDirect Topics6: Cat 6a - an overview | ScienceDirect Topics7: [Cat 5e - an overview | ScienceDirect Topics]

NEW QUESTION 6

- (Topic 3)

Which of the following focuses on application delivery?

- A. DaaS
- B. IaaS
- C. SaaS
- D. PaaS

Answer: C

Explanation:

SaaS is the cloud computing model that focuses on application delivery. SaaS stands for Software as a Service, which is a cloud computing model that provides software applications over the internet. SaaS allows customers to access and use software applications without installing or maintaining them on their own devices or servers. SaaS offers advantages such as scalability, accessibility, compatibility, and cost-effectiveness.

Customers can use SaaS applications on demand and pay only for what they use. References: [CompTIA Network+ Certification Exam Objectives], What Is Software as a Service (SaaS)? | IBM

NEW QUESTION 7

- (Topic 3)

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

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

Answer: A

Explanation:

LC (local connector) is the most likely fiber connector type to be used on a network interface card, because it is a small form factor connector that can fit more interfaces on a single card. LC connectors use square connectors that have a locking mechanism on the top, similar to an RJ45 copper connector. LC connectors are also compatible with SFP (small form-factor pluggable) modules that are often used to link a gigabit Ethernet port with a fiber network12.

References:

? Optical Fiber Connectors – CompTIA Network+ N10-007 – 2.11

? CompTIA Network+ Certification Exam Objectives2

NEW QUESTION 8

- (Topic 3)

Which of the following protocols can be used to change device configurations via encrypted and authenticated sessions? (Select TWO).

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

Answer: BD

NEW QUESTION 9

- (Topic 3)

Which of the following, in addition to a password, can be asked of a user for MFA?

- A. PIN
- B. Favorite color
- C. Hard token
- D. Mother's maiden name

Answer: A

Explanation:

MFA stands for Multi-Factor Authentication, which is a method of verifying the identity of a user by requiring two or more pieces of evidence that belong to different categories: something the user knows, something the user has, or something the user is. A password is something the user knows, and it is usually combined with another factor such as a PIN (Personal Identification Number) or a hard token (a physical device that generates a one-time code) that the user has. A favorite color or a mother's maiden name are not suitable for MFA, as they are also something the user knows and can be easily guessed or compromised.

References

- ? 1: Multi-Factor Authentication – N10-008 CompTIA Network+ : 3.1
- ? 2: CompTIA Network+ Certification Exam Objectives, page 13
- ? 3: CompTIA Network+ N10-008 Certification Study Guide, page 250
- ? 4: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 14

NEW QUESTION 10

- (Topic 3)

A customer is hosting an internal database server. None of the users are able to connect to the server, even though it appears to be working properly. Which of the following is the best way to verify traffic to and from the server?

- A. Protocol analyzer
- B. nmap
- C. ipconfig
- D. Speed test

Answer: A

Explanation:

A protocol analyzer is the best way to verify traffic to and from the server. A protocol analyzer, also known as a packet sniffer or network analyzer, is a tool that captures and analyzes the network packets that are sent and received by a device. A protocol analyzer can show the source and destination IP addresses, ports, protocols, and payload of each packet, as well as any errors or anomalies in the network communication. A protocol analyzer can help troubleshoot network connectivity issues by identifying the root cause of the problem, such as misconfigured firewall rules, incorrect routing, or faulty network devices¹².

To use a protocol analyzer to verify traffic to and from the server, the customer can follow these steps:

? Install a protocol analyzer tool on a device that is connected to the same network

as the server, such as Wireshark³ or Microsoft Network Monitor⁴.

? Select the network interface that is used to communicate with the server, and start capturing the network traffic.

? Filter the captured traffic by using the IP address or hostname of the server, or by using a specific port or protocol that is used by the database service.

? Analyze the filtered traffic and look for any signs of successful or failed connection attempts, such as TCP SYN, ACK, or RST packets, or ICMP messages.

? If there are no connection attempts to or from the server, then there may be a problem with the network configuration or device settings that prevent the traffic from reaching the server.

? If there are connection attempts but they are rejected or dropped by the server, then there may be a problem with the server configuration or service settings that prevent the traffic from being accepted by the server.

The other options are not the best ways to verify traffic to and from the server. nmap is a tool that can scan a network and discover hosts and services, but it cannot capture and analyze the network packets in detail. ipconfig is a command that can display and configure the IP settings of a device, but it cannot monitor or test the network communication with another device. Speed test is a tool that can measure the bandwidth and latency of a network connection, but it cannot diagnose or troubleshoot specific network problems.

NEW QUESTION 10

- (Topic 3)

A VOIP phone is plugged in to a port but cannot receive calls. Which Of the following needs to be done on the port to address the issue?

- A. Trunk all VLANs on the port.
- B. Configure the native VLAN.
- C. Tag the traffic to voice VLAN.
- D. Disable VLANs.

Answer: C

Explanation:

To enable a VOIP phone to receive calls on a port, the traffic needs to be tagged to the voice VLAN that is configured on the switch. This allows the phone to communicate with the voice network and the PBX server. Tagging the traffic also separates the voice traffic from the data traffic that may be coming from a computer connected to the phone. The port should be configured to tag the traffic for the voice VLAN and untag the traffic for the data VLAN¹. Trunking all VLANs on the port is unnecessary and may cause security issues. Configuring the native VLAN is not relevant for this issue. Disabling VLANs would prevent the phone from working at all.

References:

Optical Fiber Connectors – CompTIA Network+ N10-007 – 2.13

? VoIP and computer on separate VLANs through one cable¹

NEW QUESTION 12

- (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: AF

NEW QUESTION 15

- (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 17

- (Topic 3)

Which of the following is a security flaw in an application or network?

- A. A threat
- B. A vulnerability
- C. An exploit
- D. A risk

Answer: B

Explanation:

A vulnerability is a security flaw in an application or network that can be exploited by an attacker, allowing them to gain access to sensitive data or take control of the system. Vulnerabilities can range from weak authentication methods to unpatched software, allowing attackers to gain access to the system or data they would not otherwise be able to access. Exploits are programs or techniques used to take advantage of vulnerabilities, while threats are potential dangers, and risks are the likelihood of a threat becoming a reality.

NEW QUESTION 21

- (Topic 3)

A technician received a report that some users in a large, 30-floor building are having intermittent connectivity issues. Users on each floor have stable connectivity, but do not have connectivity to other floors. Which of the following devices is MOST likely causing the issue?

- A. User devices
- B. Edge devices
- C. Access switch
- D. Core switch

Answer: D

Explanation:

A core switch is the most likely device causing the issue where users on each floor have stable connectivity, but do not have connectivity to other floors. A core switch is a high-performance switch that connects multiple access switches in a network. An access switch is a switch that connects end devices, such as computers and printers, to the network. A core switch acts as the backbone of the network, providing interconnection and routing between different subnets or VLANs. If the core switch is malfunctioning or misconfigured, it can prevent communication between different segments of the network, resulting in intermittent connectivity issues. References: [CompTIA Network+ Certification Exam Objectives], Core Switch vs Access Switch: What Are the Differences?

NEW QUESTION 24

- (Topic 3)

A network administrator is working to configure a new device to provide Layer 2 connectivity to various endpoints including several WAPs. Which of the following devices will the administrator MOST likely configure?

- A. WLAN controller
- B. Cable modem
- C. Load balancer
- D. Switch
- E. Hub

Answer: D

Explanation:

A switch is a device that provides Layer 2 connectivity to various endpoints by forwarding frames based on MAC addresses. A switch can also connect to several WAPs (wireless access points) to provide wireless connectivity to wireless devices.

NEW QUESTION 27

- (Topic 3)

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

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

Answer: D

Explanation:

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

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

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

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

References

What is a Default Gateway?

What's an IP Conflict and How Do You Resolve It? What is RIP (Routing Information Protocol)?

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

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

NEW QUESTION 30

- (Topic 3)

A WAN technician reviews activity and identifies newly installed hardware that is causing outages over an eight-hour period. Which of the following should be considered FIRST?

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

Answer: D

Explanation:

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

NEW QUESTION 35

- (Topic 3)

A network resource was accessed by an outsider as a result of a successful phishing campaign. Which of the following strategies should be employed to mitigate the effects of phishing?

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

Answer: A

Explanation:

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

NEW QUESTION 39

- (Topic 3)

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

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

Which of the following is MOST likely the Issue?

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

Answer: A

Explanation:

The switchport is shut down, which means it is administratively disabled and cannot forward traffic. The image shows that the switchport status is “down” and the protocol status is “down”, indicating that there is no physical or logical connection. The cable is plugged in, as shown by the “connected” message under the interface name. The loopback is not set, as shown by the “loopback not set” message under the encapsulation type. The bandwidth configuration is correct, as shown by the “BW 10000 Kbit/sec” message under the MTU size. References: [CompTIA Network+ Certification Exam Objectives], Domain 3.0 Infrastructure, Objective 3.1: Given a scenario, use appropriate networking tools, Subobjective: Command line tools (ping, netstat, tracer, etc.)

NEW QUESTION 44

- (Topic 3)

To access production applications and data, developers must first connect remotely to a different server. From there, the developers are able to access production data. Which of the following does this BEST represent?

- A. A management plane
- B. A proxy server
- C. An out-of-band management device
- D. A site-to-site VPN
- E. A jump box

Answer: E

NEW QUESTION 48

- (Topic 3)

Which of the following documents dictates the uptimes that were agreed upon by the involved parties?

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

Answer: C

Explanation:

An SLA (Service Level Agreement) is a document that defines the expected level of service and performance guaranteed by a service provider to a customer. It usually specifies metrics such as uptime, availability, reliability, response time, and compensation or penalties for not meeting the agreed standards. An SLA is a way of ensuring that both parties are clear about their roles and responsibilities, and that the customer receives the quality of service they paid for.

NEW QUESTION 51

- (Topic 3)

A company is designing a SAN and would like to use STP as its medium for communication. Which of the following protocols would BEST suit the company's needs?

- A. SFTP
- B. Fibre Channel
- C. iSCSI
- D. FTP

Answer: B

Explanation:

A SAN also employs a series of protocols enabling software to communicate or prepare data for storage. The most common protocol is the Fibre Channel Protocol (FCP), which maps SCSI commands over FC technology. The iSCSI SANs will employ an iSCSI protocol that maps SCSI commands over TCP/IP. STP (Spanning Tree Protocol) is a protocol used to prevent loops in Ethernet networks, and it is not a medium for communication in a storage area network (SAN). However, Fibre Channel is a protocol that is specifically designed for high-speed data transfer in SAN environments. It is a dedicated channel technology that provides high throughput and low latency, making it ideal for SANs. Therefore, Fibre Channel would be the best protocol for the company to use for its SAN. SFTP (Secure File Transfer Protocol), iSCSI (Internet Small Computer System Interface), and FTP (File Transfer Protocol) are protocols used for transferring files over a network and are not suitable for use in a SAN environment.

NEW QUESTION 53

- (Topic 3)

Which of the following would be BEST suited for a long cable run with a 40Gbps bandwidth?

- A. Cat 5e
- B. Cat 6a
- C. Cat 7

D. Cat 8

Answer: C

Explanation:

Cat 7 is a type of twisted-pair copper cable that supports up to 40 Gbps bandwidth and up to 100 meters cable length. Cat 7 is suitable for long cable runs that require high-speed data transmission. Cat 7 has better shielding and crosstalk prevention than lower categories of cables.

References: Network+ Study Guide Objective 1.5: Compare and contrast network cabling types, features and their purposes.

NEW QUESTION 56

- (Topic 3)

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

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

Answer: BC

Explanation:

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

---Outdated, insecure, and slow. This is your parents' protocol. It was a thing before the Web was born.

---The more well-known problem of the 15 hop limitation in which data must travel

---Convergence time is terrible for information propagation in a network

---Metrics. It determines the number of hops from source to destination, and gives no regard to other factors when determining the best path for data to travel

---Overhead. A good example would be routing tables. These are broadcast at half-minute intervals to other routers regardless of whether the data has changed or not. It's essentially like those old cartoons where the town guard in the walled city cries out, '10 o' the clock and all is well!'. RIPv2 introduced more security and reduced broadcast traffic, which is relevant for some available answers here.

NEW QUESTION 57

- (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 61

- (Topic 3)

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

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

Answer: A

NEW QUESTION 62

- (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 65

- (Topic 3)

A network administrator is decommissioning a server. Which of the following will the network administrator MOST likely consult?

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

Answer: D

NEW QUESTION 70

- (Topic 3)

Which of the following commands can be used to display the IP address, subnet address, gateway address, and DNS address on a Windows computer?

- A. netstat -a
- B. ifconfig
- C. ip addr
- D. ipconfig /all

Answer: D

Explanation:

The ipconfig command is a utility that allows you to view and modify the network configuration of a Windows computer. By running the command "ipconfig /all", you can view detailed information about the network configuration of your computer, including the IP address, subnet mask, default gateway, and DNS server addresses.

Option A (netstat -a) is a command that displays active network connections and their status, but it does not display IP address or other network configuration information. Option B (ifconfig) is a command used on Linux and Unix systems to view and modify network configuration, but it is not available on Windows. Option C (ip addr) is a command used on Linux and Unix systems to view and modify network configuration, but it is not available on Windows.

NEW QUESTION 75

- (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 78

- (Topic 3)

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

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

Answer: C

Explanation:

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

References

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

NEW QUESTION 79

- (Topic 3)

A network team is getting reports that air conditioning is out in an IDF. The team would like to determine whether additional network issues are occurring. Which of the following should the network team do?

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

Answer: D

Explanation:

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

NEW QUESTION 83

- (Topic 3)

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

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

Answer: AD

NEW QUESTION 88

- (Topic 3)

An engineer is using a tool to run an ICMP sweep of a network to find devices that are online. When reviewing the results, the engineer notices a number of workstations that are currently verified as being online are not listed in the report.

The tool was configured to scan using the following information: Network address: 172.28.16.0

CIDR: /22

The engineer collected the following information from the client workstation: IP address: 172.28.17.206

Subnet mask: 255.255.252.0

Which of the following MOST likely explains why the tool is failing to detect some workstations?

- A. The scanned network range is incorrect.
- B. The subnet mask on the client is misconfigured.
- C. The workstation has a firewall enabled.
- D. The tool is unable to scan remote networks.

Answer: C

Explanation:

A firewall is a device or software that filters and controls the incoming and outgoing network traffic based on predefined rules. A firewall can block ICMP packets, which are used for ping and other diagnostic tools. If the workstation has a firewall enabled, it may not respond to the ICMP sweep and appear as offline. The engineer should check the firewall settings on the workstation and allow ICMP traffic if needed.

References: Network+ Study Guide Objective 4.1: Given a scenario, use the appropriate tool.

NEW QUESTION 93

- (Topic 3)

After upgrading to a SOHO router that supports Wi-Fi 6, the user determines throughput has not increased. Which of the following is the MOST likely cause of the issue?

- A. The wireless router is using an incorrect antenna type.
- B. The user's workstation does not support 802.11 ax.
- C. The encryption protocol is mismatched
- D. The network is experiencing interference.

Answer: B

Explanation:

The user's workstation does not support 802.11 ax, which is the technical name for Wi-Fi 6. Wi-Fi 6 is a new wireless standard that offers faster speeds, higher capacity, and lower latency than previous standards. However, to take advantage of these benefits, both the router and the workstation need to support Wi-Fi 6. If the workstation only supports an older standard, such as 802.11 ac or Wi-Fi 5, then the throughput will not increase even if the router supports Wi-Fi 6. References: [CompTIA Network+ Certification Exam Objectives], What is Wi-Fi 6? Here's what you need to know | PCWorld

NEW QUESTION 96

- (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 99

- (Topic 3)

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

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

Answer: A

NEW QUESTION 101

- (Topic 3)

A technician is investigating packet loss to a device that has varying data bursts throughout the day. Which of the following will the technician MOST likely configure to resolve the issue?

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

Answer: A

Explanation:

Ethernet flow control is a mechanism for temporarily stopping the transmission of data on Ethernet family computer networks. The goal of this mechanism is to avoid packet loss in the presence of network congestion.

Flow control is a mechanism that allows a device to regulate the amount of data it receives from another device, ensuring that the receiving device is not overwhelmed with data. If the device experiencing packet loss is receiving large bursts of data at times when it is not able to process it quickly enough, configuring flow control could help prevent packets from being lost.

"In theory, flow control can help with situations like a host that can't keep up with the flow of traffic. It enables the host to send an Ethernet PAUSE frame, which asks the switch to hold up for some amount of time so the host can catch its breath. If the switch can, it'll buffer transmissions until the pause expires, and then start sending again. If the host catches up early, it can send another PAUSE frame with a delay of zero to ask the switch to resume. In practice, flow control can cause latency trouble for modern real-time applications such as VoIP, and the same needs are usually met by QoS"

NEW QUESTION 103

- (Topic 3)

A network administrator is looking at switch features and is unsure whether to purchase a model with PoE. Which of the following devices that commonly utilize PoE should the administrator consider? (Select TWO)

- A. VoIP phones
- B. Cameras
- C. Printers
- D. Cable modems
- E. Laptops
- F. UPSs

Answer: AB

Explanation:

Power over Ethernet (PoE) is a technology that allows network-connected devices to receive power over the same Ethernet cables that are used for data transfer. PoE is commonly used to power devices such as VoIP phones and cameras, making it an ideal choice for network administrators looking for a cost-effective solution. PoE is not typically used for other devices such as printers, cable modems, laptops, and UPSs.

NEW QUESTION 106

- (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 108

- (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 110

- (Topic 3)

A technician is concerned about unauthorized personnel moving assets that are installed in a data center server rack. The technician installs a networked sensor that sends an alert when the server rack door is opened. Which of the following did the technician install?

- A. Cipher lock
- B. Asset tags
- C. Access control vestibule
- D. Tamper detection

Answer: D

Explanation:

Tamper detection is a physical security feature that can alert the technician when someone opens the server rack door without authorization. Tamper detection sensors can be installed inside the equipment or on the rack itself, and they can send an alert via email, SMS, or other methods. Tamper detection can help prevent unauthorized access, theft, or damage to the network assets.

References:

? Physical Security – N10-008 CompTIA Network+ : 4.51

NEW QUESTION 115

- (Topic 3)

AGRE tunnel has been configured between two remote sites. Which of the following features, when configured, ensures GRE overhead does not affect payload?

- A. jumbo frames
- B. Auto medium-dependent Interface
- C. Interface crossover
- D. Collision detection

Answer: A

Explanation:

One of the features that can be configured to ensure that GRE overhead does not affect payload is A. jumbo frames. Jumbo frames are Ethernet frames that have a payload size larger than 1500 bytes, which is the standard maximum transmission unit (MTU) for Ethernet. By using jumbo frames, more data can be sent in each packet, reducing the overhead ratio and improving efficiency.

Auto medium-dependent interface (MDI), interface crossover, and collision detection are features related to Ethernet physical layer connectivity, but they do not affect GRE overhead or payload.

NEW QUESTION 118

- (Topic 3)

Which of the following network types is composed of computers that can all communicate with one another with equal permissions and allows users to directly share what is on or attached to their computers?

- A. Local area network
- B. Peer-to-peer network
- C. Client-server network
- D. Personal area network

Answer: B

Explanation:

A peer-to-peer network is a type of network in which each computer (or node) can communicate directly with any other node, without requiring a central server or authority. Each node can act as both a client and a server, and can share its own resources, such as files, printers, or internet connection, with other nodes. A peer-to-peer network allows users to directly access and exchange what is on or attached to their computers, with equal permissions and responsibilities.

NEW QUESTION 121

- (Topic 3)

A network administrator received complaints of intermittent network connectivity issues. The administrator investigates and finds that the network design contains potential loop scenarios. Which of the following should the administrator do?

- A. Enable spanning tree.
- B. Configure port security.
- C. Change switch port speed limits.
- D. Enforce 802.1Q tagging.

Answer: A

Explanation:

Spanning tree is a protocol that prevents network loops by dynamically disabling or enabling switch ports based on the network topology. Network loops can cause intermittent connectivity issues, such as broadcast storms, MAC address table instability, and multiple frame transmission. By enabling spanning tree, the network administrator can ensure that there is only one active path between any two network devices at any given time. References:

? CompTIA Network+ N10-008 Certification Exam Objectives, page 91

? CompTIA Network+ Cert Guide: Switching and Virtual LANs, page 172

NEW QUESTION 123

- (Topic 3)

A network technician is responding to an issue with a local company. To which of the following documents should the network technician refer to determine the scope of the issue?

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

Answer: D

Explanation:

SLA stands for Service Level Agreement, and it is a contract that defines the expectations and responsibilities between a service provider and a customer. SLA can specify the quality, availability, and performance metrics of the service, as well as the penalties for non-compliance and the procedures for resolving issues. SLA can help the network technician determine the scope of the issue by providing the baseline and target values for the service, the escalation process and contacts, and the service credits or remedies for the customer⁴⁵.

CompTIA Network+ N10-008 Cert Guide - Chapter 15: Network Troubleshooting Methodology³⁵: What is a Service Level Agreement (SLA)? | ITIL | AXELOS

NEW QUESTION 125

- (Topic 3)

An on-call network technician receives an automated email alert stating that a power supply on a firewall has just powered down. Which of the following protocols would best allow for this level of detailed device monitoring?

- A. TFTP
- B. TLS
- C. SSL
- D. SNMP

Answer: D

Explanation:

SNMP stands for Simple Network Management Protocol, and it is a protocol that allows network devices to communicate their status, performance, and configuration information to a central management system. SNMP can be used to monitor and manage various aspects of network devices, such as CPU usage, memory utilization, interface statistics, temperature, voltage, power supply, etc. SNMP can also generate alerts or notifications when certain events or thresholds are reached, such as a power supply failure, a link down, or a high traffic volume. SNMP is widely used for network monitoring and troubleshooting purposes, as it provides a comprehensive and detailed view of the network health and performance.

The other options are not correct because they are not protocols that allow for detailed device monitoring. They are:

? TFTP. TFTP stands for Trivial File Transfer Protocol, and it is a protocol that allows for simple and fast file transfer between network devices. TFTP is often used to transfer configuration files, firmware updates, or boot images to network devices, such as routers, switches, or firewalls. TFTP does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.

? TLS. TLS stands for Transport Layer Security, and it is a protocol that provides encryption and authentication for data transmission over a network. TLS is often used to secure web traffic, email, or other applications that use TCP as the transport protocol. TLS does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.

? SSL. SSL stands for Secure Sockets Layer, and it is a protocol that provides encryption and authentication for data transmission over a network. SSL is the predecessor of TLS, and it is still used to secure some web traffic, email, or other applications that use TCP as the transport protocol. SSL does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.

References¹: What is SNMP? - Definition from WhatIs.com²: Network+ (Plus) Certification

| CompTIA IT Certifications³: What is TFTP? - Definition from WhatIs.com⁴: What is TLS? - Definition from WhatIs.com⁵: What is SSL? - Definition from WhatIs.com

NEW QUESTION 129

- (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 132

- (Topic 3)

Which of the following describes a network in which users and devices need to mutually authenticate before any network resource can be accessed?

- A. Least privilege

- B. Local authentication
- C. Zero trust
- D. Need to know

Answer: C

Explanation:

A zero trust network is a network in which users and devices need to mutually authenticate before any network resource can be accessed. A zero trust network assumes that no one and nothing can be trusted by default, even if they were previously verified or are within the network perimeter. A zero trust network uses various technologies and practices, such as data and log aggregation, cybersecurity analytics, continuous diagnostics and mitigation, user behavior analytics, microsegmentation, and identity and access management, to enforce granular and dynamic policies based on the context and behavior of the users and devices¹²³.

References:

- ? What is Zero Trust? | Internet of Things | CompTIA³
- ? The Death of the Perimeter: Zero Trust is (Almost) Here to Stay | Cybersecurity | CompTIA²
- ? CompTIA Network+ Certification Exam N10-008 Practice Test 17 - ExamCompass¹

NEW QUESTION 134

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 139

SIMULATION - (Topic 3)

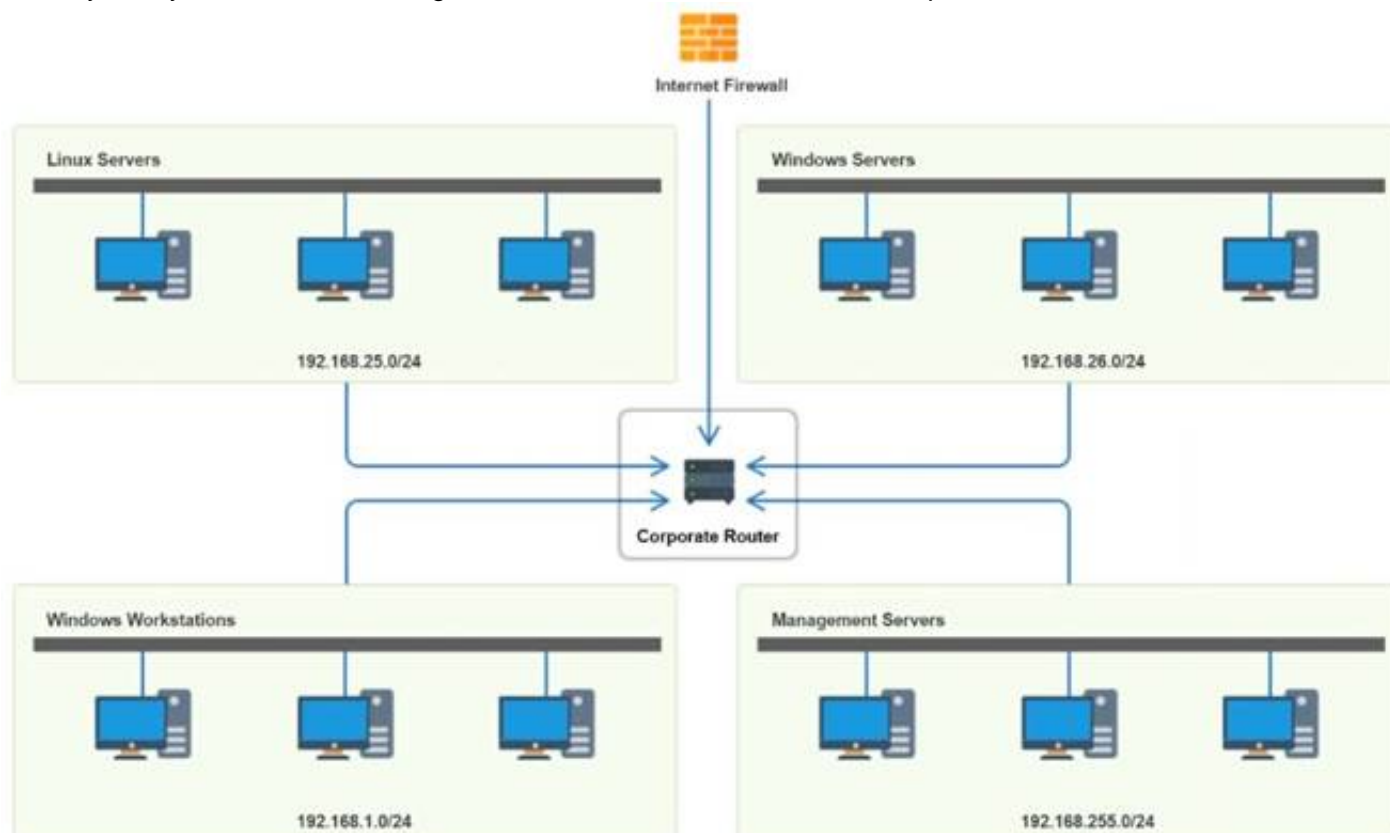
You have been tasked with implementing an ACL on the router that will:

- * 1. Permit the most commonly used secure remote access technologies from the management network to all other local network segments
- * 2. Ensure the user subnet cannot use the most commonly used remote access technologies in the Linux and Windows Server segments.
- * 3. Prohibit any traffic that has not been specifically allowed.

INSTRUCTIONS

Use the drop-downs to complete the ACL

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



Router Access Control List ✕					
Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
2	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
3	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
7	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	Any	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Router Access Control List					
Rule	Source	Destination	Protocol	Service	Action
1	192.168.255.0	192.168.26.0	TCP	SSH	Allow
2	192.168.255.0	192.168.25.0	TCP	SSH	Allow
3	192.168.255.0	192.168.1.0	TCP	SSH	Allow
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0	Any	TCP	RDP	Deny
7	192.168.1.0	Any	TCP	VNC	Deny
8	192.168.1.0	Any	Any	Any	Allow
9	Any	Any	Any	Any	Deny

NEW QUESTION 144

- (Topic 3)

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

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

Answer: A

Explanation:

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

References:

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

? CompTIA Network+ Certification Exam Objectives, page 142

NEW QUESTION 148

- (Topic 3)

A network technician is troubleshooting a network issue for employees who have reported issues with speed when accessing a server in another subnet. The server is in another building that is 410ft (125m) away from the employees' building. The 10GBASE-T connection between the two buildings uses Cat 5e. Which of the following BEST explains the speed issue?

- A. The connection type is not rated for that distance
- B. A broadcast storm is occurring on the subnet.
- C. The cable run has interference on it
- D. The connection should be made using a Cat 6 cable

Answer: D

Explanation:

The 10GBASE-T connection between the two buildings uses Cat 5e, which is not rated for a distance of 410ft (125m). According to the CompTIA Network+ Study Manual, for 10GBASE-T connections, "Cat 5e is rated for up to 55m, Cat 6a is rated for 100m, and Cat 7 is rated for 150m." Therefore, the speed issue is likely due to the fact that the connection type is not rated for the distance between the two buildings. To resolve the issue, the technician should consider using a Cat 6a or Cat 7 cable to increase the distance the connection is rated for.

NEW QUESTION 150

- (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 151

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 155

- (Topic 3)

A network administrator is troubleshooting a connection to a remote site. The administrator runs a command and sees the following output:

```
Tracing route to 10.10.0.22 over a maximum of 30 hops:
 0  14ms  20ms  15ms  192.168.1.253
 1  10ms  15ms  12ms  172.16.0.21
 2   5ms   10ms  10ms  10.10.5.3
 3  10ms  15ms  12ms  10.12.2.1
 4   5ms   10ms  10ms  10.10.5.3
 5  10ms  15ms  12ms  10.12.2.1
 6   5ms   10ms  10ms  10.10.5.3
 7  10ms  15ms  12ms  10.12.2.1
```

Which of the following is the cause of the connection issue?

- A. Routing loop
- B. Asymmetrical routing
- C. Broadcast storm
- D. Switching loop

Answer: A

Explanation:

The cause of the connection issue is a routing loop. A routing loop is a situation where a packet is forwarded in circles between routers, never reaching its destination. A routing loop can be caused by misconfigured or inconsistent routing tables, or by routing protocols that do not update their information properly. A routing loop can be detected by using the traceroute command, which shows the path taken by a packet from the source to the destination. The traceroute output in the image shows that the packet is bouncing back and forth between two routers, 10.12.2.1 and 10.12.2.2, indicating a routing loop. References: CompTIA Network+ N10-008 Certification Study Guide, page 181; The Official CompTIA Network+ Student Guide (Exam N10-008), page 7-9.

NEW QUESTION 156

- (Topic 3)

A user reports that a crucial fileshare is unreachable following a network upgrade that was completed the night before. A network technician confirms the problem exists. Which of the following troubleshooting Steps should the network technician perform NEXT?

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

Answer: A

Explanation:

Establishing a theory of probable cause is the third step in the general troubleshooting process, after identifying the problem and gathering information. Establishing a theory of probable cause involves using the information gathered to formulate one or more possible explanations for the problem and testing them to verify or eliminate them. In this scenario, the network technician has confirmed the problem exists and should proceed to establish a theory of probable cause based on the information available, such as the network upgrade that was completed the night before. Implementing a solution to fix the problem is the fifth step in the general troubleshooting process, after establishing a plan of action. Implementing a solution involves applying the chosen method or technique to resolve the problem and verifying its effectiveness. In this scenario, the network technician has not established a plan of action yet and should not implement a solution without knowing the cause of the problem. Creating a plan of action to resolve the problem is the fourth step in the general troubleshooting process, after establishing a theory of probable cause. Creating a plan of action involves selecting the best method or technique to address the problem based on the available resources, constraints, and risks. In this scenario, the network technician has not established a theory of probable cause yet and should not create a plan of action without knowing the cause of the problem. Documenting the problem and the solution is the seventh and final step in the general troubleshooting process, after implementing preventive measures.

Documenting the problem and the solution involves recording the details of the problem, its symptoms, its cause, its solution, and its preventive measures for future reference and improvement. In this scenario, the network technician has not implemented preventive measures yet and should not document the problem and the solution without resolving and preventing it.

NEW QUESTION 158

- (Topic 3)

A company realizes that only half of its employees work in the office, and the employees who work from home no longer need a computer at the office. Which of the following security measures should the network administrator implement when removing a computer from a cubicle?

- A. Disable DHCP on the computer being removed.
- B. Place the switch port in a private VLAN.
- C. Apply a firewall rule to block the computer's IP address.
- D. Remove the employee's network access.

Answer: D

Explanation:

The best security measure to implement when removing a computer from a cubicle is to remove the employee's network access. This will prevent the employee from accessing any network resources or data from the computer, as well as prevent any unauthorized users from using the computer to access the network. Removing the employee's network access can be done by deleting or disabling the user account, revoking the credentials, or changing the permissions.

The other options are not as effective or necessary as removing the employee's network access. They are:

- Disabling DHCP on the computer being removed will prevent the computer from obtaining an IP address from the network, but it will not prevent the computer from using a static IP address or accessing the network through another device.
- Placing the switch port in a private VLAN will isolate the computer from other devices on the network, but it will not prevent the computer from accessing the network through another port or device.
- Applying a firewall rule to block the computer's IP address will prevent the computer from communicating with the network, but it will not prevent the computer from changing its IP address or accessing the network through another device.

References

- 1: CompTIA Network+ N10-008 Cert Guide - O'Reilly Media
- 2: Network+ (Plus) Certification | CompTIA IT Certifications
- 3: 10 Ways to Secure Office Workstations - Computer Security

NEW QUESTION 163

- (Topic 3)

Which of the following use cases would justify the deployment of an mGRE hub-and-spoke topology?

- A. An increase in network security using encryption and packet encapsulation
- B. A network expansion caused by an increase in the number of branch locations to the headquarters
- C. A mandatory requirement to increase the deployment of an SDWAN network
- D. An improvement in network efficiency by increasing the useful packet payload

Answer: B

Explanation:

mGRE (Multipoint GRE) is a type of GRE (Generic Routing Encapsulation) tunnel that allows a single interface to support multiple tunnel endpoints, instead of having to configure a separate point-to-point tunnel for each destination. mGRE simplifies the configuration and management of large-scale VPN networks, such as DMVPN (Dynamic Multipoint VPN), which is a Cisco technology that uses mGRE, NHRP (Next Hop Resolution Protocol), and IPsec to create secure and dynamic VPN connections between a hub and multiple spokes¹.

A network expansion caused by an increase in the number of branch locations to the headquarters would justify the deployment of an mGRE hub-and-spoke topology, because it would reduce the complexity and overhead of configuring and maintaining multiple point-to-point tunnels between the hub and each spoke. mGRE would also enable spoke-to-spoke communication without having to go through the hub, which would improve the network performance and efficiency²³. The other options are not directly related to the use case of mGRE hub-and-spoke topology. An increase in network security using encryption and packet encapsulation can be achieved by using IPsec, which is a separate protocol that can be applied to any type of GRE tunnel, not just mGRE. A mandatory requirement to increase the deployment of an SDWAN network can be met by using various technologies and vendors, not necessarily mGRE or DMVPN. An improvement in network efficiency by increasing the useful packet payload can be achieved by using various techniques, such as compression, fragmentation, or QoS, not specifically mGRE.

ReferencesUnderstanding Cisco Dynamic Multipoint VPN - DMVPN, mGRE, NHRPmGRE Easy Steps - Cisco CommunityWhat is DMVPN (Dynamic Multipoint VPN), NHRP, mGRE and How to configu - Cisco Community

NEW QUESTION 166

- (Topic 3)

A network consultant is installing a new wireless network with the following specifications:

5GHz

1,300Mbps 20/40/80MHz

Which of the following standards should the network consultant use?

- A. 802.11a
- B. 802.11ac
- C. 802.11b
- D. 802.11n

Answer: B

NEW QUESTION 168

- (Topic 3)

An administrator needs to ensure an access switch is sending the appropriate logs to the network monitoring server. Which of the following logging levels is most appropriate for the access layer switch?

- A. Level 0

- B. Level 2
- C. Level 5
- D. Level 7

Answer: C

Explanation:

Logging levels are used to categorize the severity and importance of log messages generated by network devices. The lower the level, the higher the priority. Level 0 is the most critical, while level 7 is the most verbose and least important. Level 5 is the default logging level for most Cisco devices, and it corresponds to notifications. Notifications are messages that indicate normal but significant events, such as interface status changes, configuration changes, or system restarts. These messages are useful for monitoring the health and performance of the network, and they do not generate excessive traffic or consume too much memory or CPU resources. Therefore, level 5 is the most appropriate logging level for an access layer switch, which connects end devices to the network and does not need to log debug or informational messages.

ReferencesHow to configure logging in Cisco IOSCisco Guide to Harden Cisco IOS DevicesCisco Privilege Levels – Explanation and Configuration

NEW QUESTION 170

- (Topic 3)

A network administrator walks into a data center and notices an unknown person is following closely. The administrator stops and directs the person to the security desk.

Which of the following attacks did the network administrator prevent?

- A. Evil twin
- B. Tailgating
- C. Piggybacking
- D. Shoulder surfing

Answer: B

Explanation:

Tailgating is a type of physical security attack in which an unauthorized person follows an authorized person into a restricted area, such as a data center, without proper identification or authentication. Tailgating can allow attackers to access sensitive data, equipment, or network resources, or to plant malicious devices or software. The network administrator prevented tailgating by stopping and directing the unknown person to the security desk, where they would have to verify their identity and purpose.

ReferencesDigital Threats and Cyberattacks at the Network LevelNetwork attacks and how to prevent them

NEW QUESTION 173

- (Topic 3)

A technician reviews a network performance report and finds a high level of collisions happening on the network. At which of the following layers of the OSI model would these collisions be found?

- A. Layer 1
- B. Layer 3
- C. Layer 4
- D. Layer 7

Answer: A

Explanation:

Collisions occur when two or more devices try to transmit signals on the same physical medium at the same time. This causes interference and data loss. Collisions can only happen at the physical layer of the OSI model, which is responsible for transmitting and receiving raw bits over a physical medium such as a cable or a wireless channel. The physical layer does not have any mechanism to prevent or resolve collisions. Therefore, higher layers of the OSI model, such as the data link layer, need to implement protocols to detect and recover from collisions, such as CSMA/CD for Ethernet networks. ReferencesCollision in computer networkingData Link Layer | Layer 2 | The OSI-Model

NEW QUESTION 177

- (Topic 3)

A non-employee was able to enter a server room. Which of the following could have prevented this from happening?

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

Answer: B

Explanation:

A biometric reader is a device that scans a person's physical characteristics, such as fingerprints, iris, or face, and compares them to a database of authorized users. A biometric reader can be used to restrict access to a server room and prevent unauthorized entry. A biometric reader provides a high level of security and cannot be easily bypassed or duplicated.

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

NEW QUESTION 182

- (Topic 3)

Which of the following is used when a workstation sends a DHCP broadcast to a server on another LAN?

- A. Reservation

- B. Dynamic assignment
- C. Helper address
- D. DHCP offer

Answer: C

Explanation:

A helper address is an IP address that is configured on a router interface to forward DHCP broadcast messages to a DHCP server on another LAN. A DHCP broadcast message is a message that a workstation sends when it needs to obtain an IP address from a DHCP server. Since broadcast messages are not routed across different networks, a helper address is needed to relay the DHCP broadcast message to the DHCP server on another network. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 199)

NEW QUESTION 184

- (Topic 3)

Which of the following would be increased by adding encryption to data communication across the network?

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

Answer: D

Explanation:

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

NEW QUESTION 189

- (Topic 3)

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

- ? 110
- ? 66

- A. BiX
- B. Krone

Answer: A

Explanation:

A 110 block is a type of punch-down block that is used to terminate twisted-pair cables in Ethernet networks. It is a non-proprietary standard that is widely used in structured cabling systems for voice and data applications. A 110 block can support up to 100 MHz of bandwidth and can be used with Cat 3, Cat 5, Cat 5e, and Cat 6 cables¹².

A 66 block is another type of punch-down block that is mainly used for telephone wiring. It is an older and less reliable standard than the 110 block and does not support high-speed data transmission³. A BiX block is a proprietary punch-down block that is developed by NORDX/CDT and is mostly used in Canada. It can support up to 250 MHz of bandwidth and can be used with Cat 5e and Cat 6 cables⁴. A Krone block is another proprietary punch-down block that is developed by ADC Krone and is mostly used in Europe. It can support up to 100 MHz of bandwidth and can be used with Cat 5 and Cat 5e cables. Therefore, the best option for the customer who wants to use non-proprietary standards is the 110 block.

NEW QUESTION 191

- (Topic 3)

A technician is troubleshooting a user's connectivity issues and finds that the computer's IP address was changed to 169.254.0.1. Which of the following is the most likely reason?

- A. Two or more computers have the same IP address in the ARP table.
- B. The computer automatically set this address because the DHCP was not available.
- C. The computer was set up to perform as an NTP server.
- D. The computer is on a VPN and is the first to obtain a different IP address in that network.

Answer: B

Explanation:

IP addresses beginning with 169.254. are called link-local addresses or APIPA (Automatic Private IP Addressing)¹. They are assigned by the computer itself when it cannot reach a DHCP server to obtain a valid IP address from the network². This can happen for several reasons, such as a faulty router, a misconfigured network, or a disconnected cable³.

To troubleshoot this issue, the technician should check the network settings, the router configuration, and the physical connection of the computer. The technician should also try to renew the IP address by using the command `ipconfig /renew` in Windows or `dhclient` in Linux. If the problem persists, the technician may need to contact the network administrator or the ISP for further assistance.

NEW QUESTION 193

- (Topic 3)

Which of the following would be the MOST cost-effective recovery solution for a company's lower-priority applications?

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

Answer: C

NEW QUESTION 197

- (Topic 3)

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

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

Answer: A

Explanation:

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

A toner can also be used to locate breaks or shorts in a cable, or to verify continuity. References:

? Using a Toner and Probe - CompTIA Network+ Certification (N10-008): The Total Course Video

? CompTIA Network+ Certification Exam Objectives, page 141

NEW QUESTION 200

- (Topic 3)

Which of the following authentication methods requires a user to enter a password and scan a fingerprint?

- A. Single sign-on
- B. Kerberos
- C. Multifactor
- D. Network access control

Answer: C

Explanation:

Multifactor authentication is a method of verifying a user's identity by requiring more than one factor, such as something the user knows, something the user has, or something the user is. A password is something the user knows, and a fingerprint is something the user is. Therefore, a user who needs to enter a password and scan a fingerprint is using multifactor authentication.

NEW QUESTION 203

- (Topic 3)

Which of the following attacks, if successful, would provide a malicious user who is connected to an isolated guest network access to the corporate network?

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

Answer: A

Explanation:

The attack which, if successful, would provide a malicious user who is connected to an isolated guest network access to the corporate network is VLAN hopping. VLAN hopping is an attack technique which involves tricking a switch into sending traffic from one VLAN to another. This is done by sending specially crafted packets, which force the switch to send traffic from one VLAN to another, thus allowing the malicious user to gain access to the corporate network.

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

NEW QUESTION 206

- (Topic 3)

The results of a recently completed site survey indicate a significant, undesired RSSI in the parking lot and other exterior areas near the like to mitigate access to the wireless network in exterior access areas. The current access point settings are listed in the following table:

Name	Power	Antenna type	Channel	SSID	Passphrase
AP1	High	Omnidirectional	1	Corp01	P\$ssw0rd
AP2	Medium	Omnidirectional	6	Corp01	P\$ssw0rd
AP3	Medium	Directional	9	Corp01	P\$ssw0rd

Which of the following is the BEST step for the technician to take to resolve the issue?

- A. Reconfigure AP2 and AP3 for non-overlapping channels
- B. Implement directional antennas on AP1 and AP2.
- C. Raise the power settings on AP2 and AP3.
- D. Change the SSID on AP1 and AP2.

Answer: B

Explanation:

Implementing directional antennas on AP1 and AP2 is the best step for the technician to take to resolve the issue of undesired RSSI in the parking lot and other exterior areas near the building. RSSI stands for received signal strength indicator, which is a measure of how well a device can receive a wireless signal from an access point (AP). An AP is a device that provides wireless connectivity to a network. An antenna is a device that radiates or receives electromagnetic waves. A directional antenna is an antenna that focuses the wireless signal in a specific direction, resulting in higher gain and longer range. By using directional antennas on AP1 and AP2, which are located near the exterior walls of the building, the technician can reduce the wireless signal leakage to the outside areas and improve the wireless coverage inside the building. References: [CompTIA Network+ Certification Exam Objectives], What Is RSSI and How Does It Affect Wireless Networks?, Directional Antennas: Everything You Need to Know

NEW QUESTION 209

- (Topic 3)

A network administrator is creating a subnet for a remote office that has 53 network devices. An additional requirement is to use the most efficient subnet. Which of the following CIDR notations indicates the appropriate number of IP addresses with the LEAST amount of unused addresses? (Choose Correct option and give explanation directly from CompTIA Network+ Study guide or documents)

- A. /24
- B. /26
- C. /28
- D. /32

Answer: B

Explanation:

This CIDR notation indicates that there are 64 IP addresses, of which 62 are usable for network devices. This provides the LEAST amount of unused addresses, making it the most efficient subnet for a remote office with 53 network devices. According to the CompTIA Network+ Study Guide, "Subnetting allows you to divide one large network into smaller, more manageable networks or subnets."

NEW QUESTION 214

- (Topic 3)

Which of the following connector types would be used to connect to the demarcation point and provide network access to a cable modem?

- A. F-type
- B. RJ45
- C. LC
- D. RJ11

Answer: A

Explanation:

An F-type connector is a type of coaxial connector that is commonly used to connect a cable modem to the demarcation point, which is the point at which the cable provider's network ends and the customer's network begins. The F-type connector is a threaded connector that is typically used for television, cable modem, and satellite antenna connections.

NEW QUESTION 219

- (Topic 3)

A support agent receives a report that a remote user's wired devices are constantly disconnecting and have slow speeds. Upon inspection, the support agent sees that the user's coaxial modem has a signal power of -97dB Which of the following should the support agent recommend to troubleshoot the issue?

- A. Removing any splitters connected to the line
- B. Switching the devices to wireless
- C. Moving the devices closer to the modem
- D. Lowering the network speed

Answer: A

Explanation:

A splitter is a device that divides a coaxial cable into two or more branches, allowing multiple devices to share the same cable connection. However, a splitter also reduces the signal strength and quality of the cable, which can affect the performance and reliability of the devices connected to it. A signal power of -97dB is very low and indicates a weak or poor cable signal, which can cause constant disconnections and slow speeds.

The support agent should recommend removing any splitters connected to the line and connecting the coaxial modem directly to the cable outlet. This can help to improve the signal power and quality of the cable, and thus enhance the performance and reliability of the wired devices. Alternatively, the support agent can also suggest using a signal amplifier or booster, which is a device that increases the signal strength and quality of the cable, to compensate for the signal loss caused by the splitter.

The other options are not correct because they are not the best recommendations to troubleshoot the issue. They are:

? Switching the devices to wireless. Switching the devices to wireless may not solve

the issue, as the wireless connection may also depend on the cable signal and quality. Moreover, switching the devices to wireless may introduce other problems, such as interference, security, or compatibility issues, that can affect the performance and reliability of the devices.

? Moving the devices closer to the modem. Moving the devices closer to the modem

may not solve the issue, as the problem is not related to the distance between the devices and the modem, but to the signal power and quality of the cable.

Moreover, moving the devices closer to the modem may not be feasible or convenient for the user, depending on the layout and setup of the location.

? Lowering the network speed. Lowering the network speed may not solve the issue,

as the problem is not related to the bandwidth or capacity of the network, but to the signal power and quality of the cable. Moreover, lowering the network speed may degrade the user experience and satisfaction, as the user may not be able to access or use the network services or applications as expected.

References1: Network+ (Plus) Certification | CompTIA IT Certifications2: What is a Coaxial Splitter? - Definition from Techopedia3: What is a Signal Amplifier? - Definition from Techopedia

NEW QUESTION 223

- (Topic 3)

A SQL server connects over port:

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

Answer: C

Explanation:

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

NEW QUESTION 227

- (Topic 3)

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

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

Answer: D

NEW QUESTION 228

- (Topic 3)

An engineer is designing a network topology for a company that maintains a large on-premises private cloud. A design requirement mandates internet-facing hosts to be partitioned off from the internal LAN and internal server IP ranges. Which of the following defense strategies helps meet this requirement?

- A. Implementing a screened subnet
- B. Deploying a honeypot
- C. Utilizing network access control
- D. Enforcing a Zero Trust model

Answer: A

Explanation:

A screened subnet is a network topology that uses two firewalls to isolate a segment of the network from both the internal LAN and the internet. The screened subnet, also known as a demilitarized zone (DMZ), hosts the internet-facing servers that need to be accessible from outside the network, such as web servers, mail servers, or DNS servers. The first firewall, also known as the external firewall, filters the traffic between the internet and the DMZ, allowing only the necessary ports and protocols to pass through. The second firewall, also known as the internal firewall, filters the traffic between the DMZ and the internal LAN, allowing only authorized and secure connections to access the internal resources. This way, the screened subnet provides a layer of protection for both the internet-facing hosts and the internal LAN from potential attacks¹².

The other options are not defense strategies that help meet the design requirement of partitioning off the internet-facing hosts from the internal LAN and internal server IP ranges. Deploying a honeypot is a deception technique that lures attackers to a fake system or network that mimics the real one, in order to monitor their activities and collect information about their methods and motives. However, a honeypot does not isolate or protect the internet-facing hosts from the rest of the network³. Utilizing network access control is a security method that enforces policies on who or what can access the network resources, based on factors such as identity, role, device type, location, or time. However, network access control does not create a separate segment for the internet-facing hosts from the internal LAN. Enforcing a Zero Trust model is a security paradigm that assumes no trust for any entity inside or outside the network, and requires continuous verification and validation of every request and transaction. However, a Zero Trust model does not necessarily imply a specific network topology or architecture for separating the internet-facing hosts from the internal LAN.

NEW QUESTION 233

- (Topic 3)

Which of the following is a major difference between a router and a Layer 3 switch?

- A. A router can perform PAT, but a Layer 3 switch cannot.
- B. A Layer 3 switch is more efficient than a router.
- C. A router uses higher speed interfaces than a Layer 3 switch.
- D. A Layer 3 switch can run more routing protocols than a router.

Answer: A

Explanation:

PAT (Port Address Translation) is a type of Network Address Translation (NAT) that allows multiple devices to share a single public IP address by using different port numbers. PAT enables devices to access the internet without exposing their private IP addresses. A router is a device that can perform PAT by translating the source IP address and port number of outgoing packets and the destination IP address and port number of incoming packets. A Layer 3 switch is a device that can perform basic routing functions by using IP addresses, but it cannot perform PAT or other advanced routing features that a router can.

NEW QUESTION 236

- (Topic 3)

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

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

Answer: D

NEW QUESTION 237

- (Topic 3)

A network administrator replaced a faulty NIC in a printer, but the printer is still not reachable. The printer is configured with the correct IP address, mask, and gateway, and a link light is lit on the switch port that the printer is attached to.

Which of the following is the best command for the administrator to run first on the switch?

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

Answer: A

Explanation:

The best command for the administrator to run first on the switch is show vlan, which displays the VLAN configuration information on the switch, such as the VLAN IDs, names, and ports. The show vlan command can help the administrator to verify if the printer is assigned to the correct VLAN, and if there is any mismatch or misconfiguration that prevents the printer from being reachable. The show route command displays the routing table on the switch, which is not relevant for the printer connectivity, as the printer is configured with the correct gateway. The show arp command displays the ARP cache on the switch, which maps the IP addresses to the MAC addresses of the devices. The show arp command can help the administrator to check if the switch has learned the MAC address of the printer, but it is not the best command to run first, as the ARP cache can be cleared or updated frequently. The show config command displays the running configuration on the switch, which includes the VLAN configuration, but it also includes other information that is not related to the printer issue, such as the hostname, the interface settings, the security settings, and so on. The show config command can be overwhelming and time-consuming to analyze, so it is not the best command to run first.

References

? 1: VLANs and Trunking – N10-008 CompTIA Network+ : 2.3

? 2: N10-008 CompTIA Network+ : 5.5

? 3: Interface Configurations – N10-008 CompTIA Network+ : 2.3

? 4: Configuring VLANs – CompTIA Network+ N10-006 – 2.6

NEW QUESTION 241

- (Topic 3)

Classification using labels according to information sensitivity and impact in case of unauthorized access or leakage is a mandatory component of:

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

Answer: C

Explanation:

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

NEW QUESTION 243

- (Topic 3)

A company wants to mitigate unauthorized physical connectivity after implementing a hybrid work schedule. Which of the following will the company most likely configure?

- A. Intrusion prevention system
- B. DHCP snooping
- C. ARP inspection
- D. Port security

Answer: D

Explanation:

Port security is a feature that allows network administrators to limit the number of devices that can connect to a switch port, based on the MAC address of the device. This can prevent unauthorized physical connectivity by blocking any device that is not on the allowed list or exceeding the maximum number of devices per port. Port security can also trigger an action, such as shutting down the port or sending an alert, when a violation occurs. References: CompTIA Network+ N10-008 Cert Guide - O'Reilly Media, Chapter 14: Securing a Basic Network, page 512

NEW QUESTION 244

- (Topic 3)

A user is unable to reach any resources on the internet. A technician goes to the site and obtains the following output from the workstation:

Network Destination	Netmask	Gateway	Interface	Metric
10.10.51.0	255.255.255.0	On-Link	10.10.51.147	291
10.10.51.147	255.255.255.255	On-Link	10.10.51.147	291
10.10.51.255	255.255.255.255	On-Link	10.10.51.147	297
127.0.0.0	255.0.0.0	On-Link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-Link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-Link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-Link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-Link	10.10.51.147	291
255.255.255.255	255.255.255.255	On-Link	127.0.0.1	331
255.255.255.255	255.255.255.255	On-Link	10.10.51.147	291

Which of the following commands should the technician use to correct the issue?

- A. route ADD 0.0.0.0 MASK 0.0.0.0 10.10.51.10 metric 35
- B. route CHANGE 10.10.51.0 MASK 255.255.255.255 10.10.52.1 metric 5
- C. route CHANGE 10.10.51.255 MASK 255.0.0.0 On-Link metric 1
- D. route DELETE 127.255.255.255

Answer: A

Explanation:

The route command is used to view and manipulate the IP routing table in Windows operating systems⁴⁵⁶. The routing table contains information about how to reach different network destinations. The output from the workstation shows that the routing table does not have a default gateway, which is a router that forwards packets to other networks that are not directly connected to the local network. A default gateway is usually specified by a route with a destination of 0.0.0.0 and a netmask of 0.0.0.0, which matches any IP address. To correct the issue, the technician can use the route ADD command to add a default gateway to the routing table. The syntax of the command is:

route ADD <destination> MASK <netmask> <gateway> metric <metric>

The destination and netmask parameters should be 0.0.0.0 to indicate a default route. The gateway parameter should be the IP address of the router that can reach the internet, which is 10.10.51.10 in this case. The metric parameter is an optional value that indicates the cost or preference of the route, which can be used to choose between multiple routes to the same destination. A lower metric means a higher preference. The metric parameter can be any integer between 1 and 9999. In this case, the metric parameter can be 35 or any other value.

Therefore, the correct command is:

route ADD 0.0.0.0 MASK 0.0.0.0 10.10.51.10 metric 35

NEW QUESTION 245

- (Topic 3)

An attacker targeting a large company was able to inject malicious A records into internal name resolution servers. Which of the following attack types was MOST likely used?

- A. DNS poisoning
- B. On-path
- C. IP spoofing
- D. Rogue DHCP

Answer: A

NEW QUESTION 246

- (Topic 3)

Which of the following security concepts is related to ensuring that encrypted data is not edited while in transit?

- A. Zero trust
- B. Integrity
- C. Availability
- D. Confidentiality

Answer: B

Explanation:

Integrity is the security concept that is related to ensuring that encrypted data is not edited while in transit. Integrity is one of the three main goals of information security, along with confidentiality and availability. Integrity means that data is protected from unauthorized modification or corruption during storage, processing, or transmission. Integrity can be achieved by using various techniques, such as hashing, digital signatures, checksums, or message authentication codes (MACs). These techniques can verify the authenticity and validity of the data by detecting any changes or tampering that may have occurred. References: [CompTIA Network+ Certification Exam Objectives], What Is Data Integrity? | Definition & Examples | Forcepoint

NEW QUESTION 247

- (Topic 3)

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

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

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

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

Answer: B

NEW QUESTION 249

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 250

- (Topic 3)

An IT administrator received an assignment with the following objectives

- Conduct a total scan within the company's network for all connected hosts
- Detect all the types of operating systems running on all devices
- Discover all services offered by hosts on the network
- Find open ports and detect security risks.

Which of the following command-line tools can be used to achieve these objectives?

- A. nmap
- B. arp
- C. netstat
- D. tcpdump

Answer: A

Explanation:

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

NEW QUESTION 253

- (Topic 3)

An application is not working. When the log files are reviewed, the application continuously tries to reach the following destination:

Destination
::1/128

Which of the following is most likely associated with this IP address?

- A. APIPA
- B. Default gateway
- C. Link local
- D. Loopback

Answer: D

Explanation:

The IP address ::1/128 is the loopback address of the local host in IPv6, which is the equivalent of the 127.0.0.1 in IPv4. The loopback address is a virtual interface

that loops all traffic back to itself, the local host. The loopback address is used for testing and troubleshooting purposes, such as checking the connectivity and configuration of the network stack. If an application tries to reach the loopback address, it means that it is not communicating with any external network or server, but only with itself.

The other options are not correct because they are not associated with the IP address ::1/128. They are:

? APIPA. APIPA stands for Automatic Private IP Addressing, which is a feature that allows a device to assign itself a private IPv4 address in the range of 169.254.0.0/16 when no DHCP server is available. APIPA does not apply to IPv6 addresses, and it is not related to the loopback address.

? Default gateway. The default gateway is the IP address of the router or device that connects a local network to other networks. The default gateway is usually the first or last usable IP address in a subnet, and it is not the same as the loopback address.

? Link local. Link local addresses are IPv6 addresses that are used for communication within a single network segment or link. Link local addresses have the prefix fe80::/10, and they are not routable or reachable from other networks. Link local addresses are not the same as the loopback address.

References1: Loopback Address - ::1/128 - ipUpTime.net2: Network+ (Plus) Certification | CompTIA IT Certifications3: Reserved IP addresses - Wikipedia

NEW QUESTION 257

- (Topic 3)

A public, wireless ISP mounts its access points on top of traffic signal poles. Fiber-optic cables are installed from a fiber switch through the ground and up the pole to a fiber-copper media converter, and then connected to the AP. In one location, the switchport is showing sporadic link loss to the attached AP. A similar link loss is not seen at the AP interface. The fiber-optic cable is moved to another unused switchport with a similar result. Which of the following steps should the assigned technician complete NEXT?

- A. Disable and enable the switchport.
- B. Clean the fiber-optic cable ends.
- C. Replace the media converter.
- D. Replace the copper patch cord.

Answer: B

Explanation:

Fiber-optic cables are cables that use light signals to transmit data over long distances at high speeds. Fiber-optic cables are sensitive to dirt, dust, moisture, or other contaminants that can interfere with the light signals and cause link loss or signal degradation. To troubleshoot link loss issues with fiber-optic cables, one of the steps that should be completed next is to clean the fiber-optic cable ends with a lint-free cloth or a specialized cleaning tool. Cleaning the fiber-optic cable ends can remove any dirt or debris that may be blocking or reflecting the light signals and restore the link quality.

NEW QUESTION 259

- (Topic 3)

A customer hired a network consultant to install a new wireless network with the following specifications:

* 2.4GHz

* 11Mbps

* 20MHz

Which of the following standards best fits these requirements?

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

Answer: B

Explanation:

The 802.11b standard is a wireless networking protocol that operates in the 2.4GHz frequency band and supports a maximum data rate of 11Mbps. It uses a 20MHz channel width and a direct-sequence spread spectrum (DSSS) modulation technique2. The 802.11b standard was released in 1999 and is backward compatible with the original 802.11 standard3. The other standards do not match the specifications given by the customer. 802.11ac operates in the 5GHz band and supports higher data rates up to 6.9Gbps.

* 802.11g also operates in the 2.4GHz band but supports data rates up to 54Mbps. 802.11n can operate in both 2.4GHz and 5GHz bands and supports data rates up to 600Mbps. It also uses a wider channel width of 40MHz and a multiple-input multiple-output (MIMO) technology3.

References2 - 802.11 Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a - Lifewire3 - Introduction to WLAN Frequency Bands | Engineering Education (EngEd ...

NEW QUESTION 261

- (Topic 3)

Which of the following is an example of on-demand scalable hardware that is typically housed in the vendor's data center?

- A. DaaS
- B. IaaS
- C. PaaS
- D. SaaS

Answer: B

Explanation:

IaaS is an example of on-demand scalable hardware that is typically housed in the vendor's data center. IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources over the internet. IaaS allows customers to rent servers, storage, network devices, and other hardware components from a cloud service provider, rather than purchasing and maintaining them on-premise. IaaS offers advantages such as scalability, flexibility, cost-effectiveness, and reliability. Customers can adjust their hardware resources according to their needs and pay only for what they use. Customers can also access their hardware resources from anywhere via a web browser or an API. References: [CompTIA Network+ Certification Exam Objectives], What Is Infrastructure as a Service (IaaS)? | IBM

NEW QUESTION 264

- (Topic 3)

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

- A. Console
- B. Split tunnel
- C. Jump box
- D. Out of band

Answer: D

Explanation:

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

NEW QUESTION 266

- (Topic 3)

A technician is tasked with setting up a mail server and a DNS server. The mail port should be secured and have the ability to transfer large files. Which of the following ports should be opened? (Select TWO).

- A. 22
- B. 53
- C. 110
- D. 389
- E. 995
- F. 3389

Answer: BE

Explanation:

Port 53 is used for DNS, which is a service that translates domain names into IP addresses. Port 995 is used for POP3S, which is a protocol for receiving email messages securely. POP3S supports large file transfers and encryption. Therefore, these two ports should be opened for the mail server and the DNS server project

NEW QUESTION 270

- (Topic 3)

A network administrator is planning to implement device monitoring to enhance network visibility. The security team requires that the solution provides authentication and encryption.

Which of the following meets these requirements?

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

Answer: D

Explanation:

SNMPv3 is a protocol that allows network administrators to monitor and manage network devices such as routers, switches, servers, printers, and more. SNMPv3 provides authentication and encryption features that ensure the security and integrity of the data exchanged between the management station and the network devices. SNMPv3 uses a user-based security model (USM) that supports three levels of security: noAuthNoPriv, authNoPriv, and authPriv. The noAuthNoPriv level provides no authentication or encryption, the authNoPriv level provides authentication but no encryption, and the authPriv level provides both authentication and encryption¹².

References

? SNMP is one of the common network monitoring protocols covered in Objective 3.1 of the CompTIA Network+ N10-008 certification exam³.

? SNMPv3 provides authentication and encryption features for network monitoring¹².

? SNMPv3 uses a user-based security model with three levels of security¹².

1: SNMP - N10-008 CompTIA Network+ : 3.1 - Professor Messer IT Certification Training Courses 2: CompTIA Network+ N10-008 Cert Guide, Chapter 13, page 413 3: CompTIA Network+ Certification Exam Objectives, page 7

NEW QUESTION 271

- (Topic 3)

A technician is investigating a misconfiguration on a Layer 3 switch. When the technician logs in and runs a command, the following data is shown:

Which of the following commands generated this output?

- A. show route
- B. show config
- C. show interface
- D. tcpdump
- E. netstat —s

Answer: C

Explanation:

The output shown in the image is from the show interface command, which displays information about the status and configuration of a network interface on a switch or router. The output includes the interface name, description, MAC address, IP address, speed, duplex mode, status, and statistics. The show route command displays the routing table of the device. The show config command displays the current configuration of the device. The tcpdump command captures and analyzes network traffic. The netstat -s command displays statistics for each protocol.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.4: Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

NEW QUESTION 272

- (Topic 3)

A company's management team wants to implement NAC on the wired and wireless networks. Which of the following is an authentication component that must be used in this solution?

- A. IPSec
- B. 802.1X
- C. EAP
- D. TACACS+

Answer: B

Explanation:

802.1X is an authentication component that must be used in a network access control (NAC) solution. NAC is a method of enforcing security policies on devices that want to access a network, by verifying their identity, compliance, and authorization. 802.1X is a standard that defines how to provide authentication for devices trying to connect to a LAN or WLAN. It uses the Extensible Authentication Protocol (EAP) to exchange authentication information between the device (supplicant), the network access device (authenticator), and the authentication server (typically RADIUS or TACACS+). 802.1X can prevent unauthorized devices from accessing the network, and can also assign them to different VLANs or apply different policies based on their role or group.

IPSec is a protocol suite that provides encryption, authentication, and integrity for IP packets. It can be used to create secure VPN tunnels between networks or hosts. IPSec is not an authentication component for NAC, but rather a security component for protecting data in transit.

EAP is a framework that supports multiple authentication methods, such as passwords, certificates, tokens, or biometrics. EAP is used by 802.1X to provide authentication for network access, but it is not a component by itself. EAP requires a carrier protocol, such as 802.1X, to transport the authentication messages.

TACACS+ is a protocol that provides authentication, authorization, and accounting (AAA) services for network devices or users. It can be used as an authentication server for 802.1X, but it is not an authentication component for NAC by itself. TACACS+ requires a client-server protocol, such as 802.1X, to communicate with the network access device. ReferencesWhat is 802.1X Network Access Control (NAC)?Compare TACACS + and RADIUS802.1X: What EXACTLY is it regarding WPA and EAP?CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION 274

- (Topic 3)

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

- A. /24
- B. /26
- C. /28
- D. /30

Answer: D

Explanation:

A /30 subnet is the smallest possible subnet that can be used for a point-to-point configuration between two routers. A /30 subnet has only two usable host addresses, one for each router, and a network address and a broadcast address. A /30 subnet conserves IP space by minimizing the number of wasted addresses. A /24, /26, or /28 subnet would have more usable host addresses than needed for a point-to-point configuration and would waste IP space.

References:

? Routing Technologies – N10-008 CompTIA Network+ : 2.21

? CompTIA Network+ Certification Exam Objectives, page 10

NEW QUESTION 279

- (Topic 3)

A local service provider connected 20 schools in a large city with a fiber-optic switched network. Which of the following network types did the provider set up?

- A. LAN
- B. MAN
- C. CAN
- D. WAN

Answer: B

Explanation:

MAN stands for Metropolitan Area Network, and it is a type of network that covers a large geographic area, such as a city or a county. MANs are often used to connect multiple LANs (Local Area Networks) within a region, such as schools, offices, or government buildings. MANs typically use high-speed and high-capacity transmission media, such as fiber-optic cables, to provide fast and reliable data communication. MANs can also provide access to WANs (Wide Area Networks), such as the Internet, or other services, such as cable TV or VoIP.

The other options are not correct because they are not the type of network that covers a large city. They are:

? LAN. LAN stands for Local Area Network, and it is a type of network that covers a

small geographic area, such as a home, an office, or a building. LANs are often used to connect multiple devices, such as computers, printers, or phones, within a single network. LANs typically use low-cost and low-capacity transmission media, such as twisted-pair cables, to provide data communication. LANs can also provide access to other networks, such as MANs or WANs, through routers or gateways.

? CAN. CAN stands for Campus Area Network, and it is a type of network that

covers a moderate geographic area, such as a university, a hospital, or a military base. CANs are often used to connect multiple LANs within a campus, such as different departments, buildings, or facilities. CANs typically use medium-cost and medium-capacity transmission media, such as coaxial cables, to provide data communication. CANs can also provide access to other networks, such as MANs or WANs, through routers or gateways.

? WAN. WAN stands for Wide Area Network, and it is a type of network that covers

a very large geographic area, such as a country, a continent, or the world. WANs are often used to connect multiple MANs or LANs across different regions, such as

different cities, states, or countries. WANs typically use high-cost and high- capacity transmission media, such as satellite links, to provide data communication.

WANs can also provide access to various services, such as the Internet, email, or VPN.

References1: What is a Metropolitan Area Network (MAN)? - Definition from

Techopedia2: Network+ (Plus) Certification | CompTIA IT Certifications3: What is a Local Area Network (LAN)? - Definition from Techopedia4: What is a Campus

Area Network (CAN)? - Definition from Techopedia5: What is a Wide Area Network (WAN)? - Definition from Techopedia

NEW QUESTION 282

- (Topic 3)

A WAN technician reviews activity and identifies newly installed hardware that is causing outages over an eight-hour period. Which of the following should be considered FIRST?

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

Answer: D

NEW QUESTION 284

- (Topic 3)

A network engineer turned on logging to assist with troubleshooting a suspected configuration issue. Which log level provides the most informative log information?

- A. FATAL
- B. ERROR
- C. DEBUG
- D. WARN

Answer: C

Explanation:

DEBUG is the log level that provides the most informative log information for troubleshooting a suspected configuration issue. Logging is a feature that allows network devices to record events and messages related to their operation and status. Logging can help network engineers to monitor, diagnose, and resolve network problems. Log levels are categories that indicate the severity or importance of a log message. Different log levels provide different amounts of detail and verbosity. DEBUG is the lowest log level, which means it provides the most detailed and verbose information about every action and event that occurs on a network device. DEBUG can help network engineers to identify configuration errors, misbehaving processes, or unexpected outcomes. However, DEBUG can also generate a lot of noise and overhead, which can affect the performance and availability of the network device. Therefore, DEBUG should be used sparingly and only when necessary. References: [CompTIA Network+ Certification Exam Objectives], Understanding Logging Levels - Cisco

NEW QUESTION 288

- (Topic 3)

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

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

Answer: D

Explanation:

A MAC filter list is a security feature that allows or denies access to a wireless network based on the MAC address of the device. A MAC address is a unique identifier assigned to a network interface card (NIC) at the physical layer of the OSI model. However, MAC filtering operates at the data link layer of the OSI model, where MAC addresses are used to encapsulate and deliver data frames between devices on the same network segment. References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.1: Given a scenario, install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.

NEW QUESTION 293

- (Topic 3)

A network consultant is setting up a new wireless infrastructure. The new infrastructure is primarily focused on supporting legacy equipment that does not support the newest standards. Which of the following frequency ranges will the consultant most likely have to support?

- A. 2.4GHz
- B. 5GHz
- C. 5.9GHz
- D. 6GHz

Answer: A

Explanation:

The most likely frequency range that the network consultant will have to support is 2.4GHz. This is because the most common legacy wireless standards, 802.11b and 802.11g, use the 2.4GHz range. IEEE 802.11a uses 5GHz exclusively, and 5.9GHz and 6GHz are not widely used by legacy equipment. Therefore, A. 2.4GHz is the correct answer.

<https://www.networkcomputing.com/networking/wireless-beginners-part-1-rf-and-waves>

NEW QUESTION 296

- (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 299

- (Topic 3)

An administrator wants to increase the availability of a server that is connected to the office network. Which of the following allows for multiple NICs to share a single IP address and offers maximum performance while providing fault tolerance in the event of a NIC failure?

- A. Multipathing
- B. Spanning Tree Protocol
- C. First Hop Redundancy Protocol
- D. Elasticity

Answer: A

Explanation:

Reference: <https://docs.oracle.com/cd/E19455-01/806-6547/6jffv7oma/index.html>

NEW QUESTION 301

- (Topic 3)

A software developer changed positions within a company and is now a sales engineer. The security team discovered that the former software developer had been modifying code to implement small features requested by customers. Which of the following would be the best thing for the security administrator to implement to prevent this from happening?

- A. A software patching policy
- B. A role-based access control policy
- C. Firewalls on the software development servers
- D. Longer and more complex password requirements

Answer: B

Explanation:

A role-based access control (RBAC) policy is a security measure that assigns permissions and privileges to users based on their roles and responsibilities within an organization. RBAC helps to enforce the principle of least privilege, which states that users should only have the minimum level of access required to perform their tasks. RBAC also helps to prevent unauthorized access, modification, or misuse of sensitive data or resources by limiting the scope and impact of user actions.

A software patching policy, firewalls on the software development servers, and longer and more complex password requirements are all good security practices, but they do not directly address the issue of preventing the former software developer from modifying code. A software patching policy ensures that software is updated regularly to fix bugs and vulnerabilities, but it does not prevent a user from introducing new code changes. Firewalls on the software development servers protect the servers from external attacks, but they do not prevent a user from accessing the servers internally. Longer and more complex password requirements make it harder for attackers to guess or crack passwords, but they do not prevent a user from using their own valid credentials.

References

1: Role-Based Access Control (RBAC) - Definition and Examples 2: Network+ (Plus) Certification | CompTIA IT Certifications

3: [What is the Principle of Least Privilege? - Definition from Techopedia]

NEW QUESTION 304

.....

Relate Links

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

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

Contact us

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

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