

# M01\_PRACTICE\_Final\_Exam\_Ch1\_13\_Fall\_2024\_Net\_Learn

**Candidate:** Richard Habib (richard\_habib1)

**Date:** 12/1/2024, 3:06:12 PM • **Time Spent:** 02:16:06

**Score: 91%**

Passing Score: 50%

## Question 1.

✓ Correct

What is the function of duplex fiber deployment?

- ☐ It implements multiple channels distinguished by wavelengths.
- ☐ It uses a single strand for both transmit and receive.
- ☐ It uses multiple strands to implement Tx and Rx channels.
- ☒ It uses two strands for transmit (Tx) and receive (Rx).

### Explanation

Duplex fiber deployment uses two strands of fiber, one for transmitting data (Tx) and the other for receiving data (Rx). This setup is common in many fiber optic networks, providing a clear and separate path for data to travel in each direction, which helps in maintaining signal integrity and reducing interference.

A single strand for both transmit and receive describes Bi-Directional (BiDi) transmission, not duplex.

Using multiple strands to implement Tx and Rx channels is characteristic of parallel fiber deployment, not duplex.

Implementing multiple channels distinguished by wavelengths describes Wavelength Division Multiplexing (WDM), not duplex fiber deployment.

### References



#### 3.1.3 Transceiver Mismatch Issues

q\_transceiver\_duplex\_fiber\_deployment\_n09.question.fex

## Question 2.

✓ Correct

What property does a security group have regarding its filtering rules?

- ☐ Stateless
- ☐ Stateless with exceptions
- ☐ Stateful with exceptions
- ☒ Stateful

**Explanation**

Security groups in AWS are stateful, meaning they automatically allow return traffic for initiated connections without requiring explicit rules for the return traffic. This property simplifies the management of inbound and outbound rules.

Stateless filtering does not automatically allow return traffic for initiated connections, which is not how AWS security groups operate.

There is no such classification as "stateless with exceptions" for AWS security groups.

"Stateful with exceptions" is not a recognized property of AWS security groups; they are purely stateful without exceptions in their filtering behavior.

**References****14.3.6 Security Groups and Security Lists**

q\_sec\_group\_stateful\_property\_n09.question.fex

## Question 3.

× Incorrect

What does "availability" in the CIA Triad refer to?

- ☐ The data is stored and transferred as intended and that any modification is authorized.
- ☐ The system is protected against unauthorized access and attacks.
- ☐ Information is accessible to those authorized to view or modify it.
- ☒ Information is accessible to those authorized to view or modify it.

**Explanation**

The correct answer is that information is accessible to those authorized to view or modify it. Availability ensures that data, systems, and services are available to authorized users when needed. This involves protecting against attacks that can lead to unauthorized denial of service, ensuring system uptime, and providing reliable access to resources.

The data is stored and transferred as intended and that any modification is authorized describes "integrity," which is about ensuring data remains unchanged unless the change is authorized.

Information is accessible to those authorized to view or modify it describes "confidentiality," which is about restricting access to information to authorized individuals only.

The system is protected against unauthorized access and attacks is a broader security goal, not specifically related to the "availability" aspect of the CIA Triad.

**References****9.1.1 Common Security Terminology**

q\_sec\_concepts\_availability\_n09.question.fex

## Question 4.

✓ Correct

What is the primary purpose of content filtering in an organization's network?

- ☒ To block access to malicious websites
- ☐ To encrypt network traffic
- ☐ To increase network speed
- ☐ To monitor employee productivity

**Explanation**

Content filtering plays a crucial role in protecting an organization's network by preventing users from accessing websites that could be harmful or not suitable for the workplace. This is essential for maintaining network security and compliance with company policies.

Increasing network speed is not the primary purpose of content filtering, although it might be a secondary benefit if bandwidth-consuming sites are blocked.

Monitoring employee productivity might be a result of content filtering but is not its primary purpose.

Encrypting network traffic is the function of encryption protocols like TLS, not content filtering.

**References**

 **10.5.1 Security Rules and ACL Configuration**

 **10.5.3 Content Filtering**

 **10.5.7 Lab: Configure a Security Appliance**

 **10.5.8 Lab: Configure a Perimeter Firewall**

 **10.5.10 Lab: Permit Traffic**

q\_content\_filter\_primary\_purpose\_n09.question.fex

## Question 5.

✓ Correct

What does "integrity" in the context of the CIA Triad mean?

- ☐ The system is protected against unauthorized access and attacks.
- ☒ The data is stored and transferred as intended and that any modification is authorized.
- ☐ Information is accessible to those authorized to view or modify it.
- ☐ Certain information should only be known to certain people.

**Explanation**

The correct answer is that data is stored and transferred as intended and that any modification is authorized. Integrity ensures that data remains accurate and consistent during its lifecycle. This means that unauthorized changes to the data, whether in storage, processing, or transit, are prevented or detected.

Information is accessible to those authorized to view or modify it describes "availability," which is about ensuring authorized users have access to information and resources.

Certain information should only be known to certain people describes "confidentiality," which is about ensuring that information is only accessible to those who are authorized.

The system is protected against unauthorized access and attacks is a broader security goal, not specifically related to the "integrity" aspect of the CIA Triad.

**References****9.1.1 Common Security Terminology**

q\_sec\_concepts\_integrity\_n09.question.fex

## Question 6.

✓ Correct

How does a SAN provision access to storage devices?

- ☒ Using block input/output
- ☐ Through file-level input/output
- ☐ Via direct physical connections
- ☐ Through application-level protocols

**Explanation**

A SAN provisions access to storage devices using block input/output (I/O), where each read or write operation addresses the actual location of data on the media. This method is similar to direct-attached storage but is performed over a network.

File-level input/output is characteristic of NAS, not SAN.

SAN access is over a network, not through direct physical connections.

SANs operate at a lower level than application-level protocols, using block I/O for data access.

**References**

**14.1.3 Storage Area Networks**



**14.1.4 Fibre Channel**



**14.1.5 Lab: Configure an iSCSI Target**



**14.1.6 Lab: Configure an iSCSI Initiator**

q\_san\_block\_input-output\_n09.question.fex

## Question 7.

✓ Correct

What factor is considered when there are identical paths with equal administrative distances to a destination?

- ☐ The path with the most recent update
- ☐ The path with the highest metric value
- ☒ The path with the lowest metric value
- ☐ The path with the shortest prefix length

**Explanation**

When there are identical paths with equal administrative distances, the path with the lowest metric value is preferred, as it represents the most efficient route.

The highest metric value indicates a less efficient route.

Prefix length is considered before comparing metric values when paths are not identical.

The timing of updates does not directly influence route selection in this context.

**References****5.2.1 Dynamic Routing Protocols****5.2.6 Route Selection**

q\_route\_missing\_identical\_paths\_n09.question.fex

## Question 8.

✓ Correct

Why do routers normally not forward broadcast traffic?

- ☐ Because routers operate at the network layer
- ☐ Because it can lead to IP address conflicts
- ☒ To prevent network congestion
- ☐ To ensure network security

**Explanation**














The correct answer is to prevent network congestion. Broadcasting across multiple subnets can lead to excessive network traffic, causing congestion and performance issues. Routers prevent this by not forwarding broadcast traffic by default.

IP address conflicts are not directly related to forwarding broadcast traffic.

While routers operate at the network layer, the reason they don't forward broadcast traffic is to prevent congestion, not because of their operational layer.

Security is a concern in network design, but the primary reason for not forwarding broadcast traffic is to prevent congestion.

**References**

-  **6.2.1 DHCP Process**
-  **6.2.2 DHCP Server Configuration**
-  **6.2.3 DHCP Options**
-  **6.2.4 DHCP Reservations and Exclusions**
-  **6.2.5 Lab: Configure a DHCP Server**
-  **6.2.6 Lab: Configure DHCP Server Options**
-  **6.2.7 Lab: Create DHCP Exclusions**
-  **6.2.8 Lab: Create DHCP Client Reservations**
-  **6.2.9 Configure Client Addressing**
-  **6.2.10 Lab: Configure Client Addressing for DHCP**
-  **6.3.2 IPv6 Interface Autoconfiguration and Testing**
-  **6.3.3 DHCPv6 Server Configuration**
-  **6.3.6 Set Up Alternate Addressing**



**6.4.1 DHCP Relay and IP Helper****6.4.2 DHCP Issues****6.4.3 Troubleshooting DHCP Exhaustion****6.4.4 Lab: Configure a DHCP Relay Agent****6.4.5 Lab: Add a DHCP Server on Another Subnet****6.4.6 Lab: Troubleshoot Address Pool Exhaustion****6.4.7 Lab: Explore DHCP Troubleshooting****6.4.8 Lab: Troubleshoot IP Configuration 1****6.4.9 Lab: Troubleshoot IP Configuration 2****6.4.10 Lab: Troubleshoot IP Configuration 3****6.6.1 Client DNS Issues**

q\_dhcp\_relay\_routers\_n09.question.fex

## Question 9.

✓ Correct

You are setting up a secure website for your online store. You want to ensure that all data transmitted between your website and your customers is encrypted.

Which of the following steps is essential for you to achieve this?

- ☐ Implement a CAPTCHA system on your website.
- ☐ Increase your website's bandwidth.
- ☐ Install a web analytics tool.
- ☒ Obtain and install a digital certificate.

**Explanation**

To secure data transmission between your website and your customers, you need to implement HTTPS, which is the secure version of HTTP enabled by TLS. Obtaining and installing a digital certificate from a trusted CA is essential for this process. The digital certificate will authenticate your website's identity to your customers and enable encrypted communication.

While useful for tracking website traffic and user behavior, web analytics tools do not encrypt data transmission.

Increasing bandwidth can improve website performance but does not secure data transmission.

CAPTCHA systems help differentiate human users from bots but do not encrypt or secure data transmission.

**References****6.5.10 DNS Security**

q\_tls\_digital\_certificate\_scenario\_n09.question.fex

## Question 10.

✓ Correct

What do "top talkers" and "top listeners" refer to in network analysis?

- ☒ Top talkers are interfaces generating the most outgoing traffic, while top listeners are the interfaces receiving the most incoming traffic.
- ☐ Top talkers are devices with the highest error rates in the network, while top listeners are devices with the highest packet loss rates.
- ☐ Top talkers are the most secure connections in a network, and top listeners are the least secure connections.
- ☐ Top talkers are the fastest network connections, while top listeners are the slowest network connections.

**Explanation**

In network analysis, "top talkers" and "top listeners" are terms used to identify network interfaces based on their traffic volume. Top talkers are those interfaces that send out the most data, indicating high outgoing traffic. This could be due to applications or devices that are heavily transmitting data across the network. On the other hand, top listeners are interfaces that receive the most data, indicating high incoming traffic. Identifying these interfaces helps network administrators understand traffic flow, pinpoint potential bottlenecks, and optimize network performance.

"Top talkers" and "top listeners" do not refer to error rates or packet loss rates. Instead, these terms specifically relate to the volume of traffic being sent or received by network interfaces. Error rates and packet loss are different metrics used in network analysis to assess the quality of connections and the reliability of data transmission, not the volume of traffic.

The concepts of "top talkers" and "top listeners" have nothing to do with security levels of connections. These terms are used to quantify traffic volume, not to evaluate the security or vulnerability of network connections. Security assessments in a network involve analyzing encryption standards, authentication protocols, and other security measures, not traffic volume.

"Top talkers" and "top listeners" refer to the amount of data being transmitted or received, not the speed of the connections. The speed of a network connection is determined by its bandwidth and latency, among other factors, and is a separate consideration from the volume of traffic that a connection handles. Identifying top talkers and top listeners helps in understanding traffic distribution and potential bottlenecks but does not directly measure the speed of network connections.

**References**

**8.6.1 Common Performance Issues****8.6.3 Flow Data****8.6.4 Traffic Testing Tools****8.6.5 Bandwidth Management**

q\_traffic\_analyze\_top\_talkers\_listeners\_n09.question.fex

**Question 11.**✓ **Correct**

Which cloud service model is best suited for businesses that want to develop and test applications without worrying about underlying infrastructure?

☐ FaaS

☐ IaaS

☐ SaaS

→ ☒ PaaS

**Explanation**

Platform as a Service (PaaS) is designed to provide developers with a platform that includes both infrastructure and development tools. This allows businesses to focus on developing and testing their applications without managing the underlying infrastructure.

IaaS provides the infrastructure but not the development tools needed for application development.

SaaS delivers software applications to end-users and is not designed for developing and testing applications.

FaaS (Function as a Service) is more specific to running individual functions in the cloud and does not provide a comprehensive platform for development and testing like PaaS.

**References****14.2.3 Cloud Service Models**

q\_cloud\_service\_paas\_example\_n09.question.fex

## Question 12.

× Incorrect

What is the purpose of a baseline in configuration management?

- ☐ To provide a temporary configuration for testing
- ☐ To document the unauthorized state of a CI
- ☐ To act as a backup configuration for emergency use
- ☐ To document the approved state of a CI

**Explanation**

A baseline in configuration management serves to document the approved or authorized state of a Configuration Item (CI), allowing for auditing processes to detect unexpected or unauthorized changes.

A baseline documents the authorized state, not unauthorized.

A baseline is not meant for temporary configurations but for establishing a standard or reference point.

A baseline is not a backup configuration; it's a reference point for the desired state of a CI.

**References****8.1.1 Configuration Management**

q\_operating\_baseline\_purpose\_n09.question.fex

## Question 13.

✓ Correct

What is a zone in the context of network security?

- ☐ An area of the network with a specific bandwidth allocation
- ☒ An area of the network where all hosts have the same level of trust
- ☐ A segment of the network that is isolated for performance testing
- ☐ A physical location within an organization

**Explanation**

In network security, a zone refers to an area of the network where all hosts within it have the same security configuration and level of trust. This concept is crucial for applying consistent security policies and controls within that zone to protect against threats and vulnerabilities.

A zone is not defined by physical location but by the logical grouping of network resources with similar security requirements and trust levels.

Zones are not categorized by bandwidth allocation but by security and trust levels.

Performance testing is not the basis for defining a network zone; zones are established for security purposes.

**References****11.1.1 Network Security Zones**

q\_net\_zones\_describe\_n09.question.fex

## Question 14.

✓ Correct

What is the preferred route selection when there are paths to the same destination with different prefix lengths?

- ☐ The path with the shortest prefix length
- ☐ The path with the highest metric value
- ☒ The path with the longest prefix length
- ☐ The path with the highest administrative distance

**Explanation**

The most specific path, which is the one with the longest prefix length, is preferred in route selection.

The shortest prefix length represents a less specific route.

The lowest metric value is preferred, not the highest.

The lowest administrative distance is preferred, indicating a more trustworthy source.

**References****5.2.1 Dynamic Routing Protocols****5.2.6 Route Selection**

q\_route\_missing\_perferred\_route\_selection\_n09.question.fex

## Question 15.

✓ Correct

What is a perimeter network also known as?

- ☐ A triple homed network
- ☐ A fully public network
- ☐ A neutral zone
- ☒ A demilitarized zone (DMZ)

**Explanation**

A perimeter network is also popularly referred to as a demilitarized zone (DMZ). This term, though somewhat vague and derived from marketing terminology, is used to describe internet-facing zones or hosts that are managed by a private organization to allow filtered public access while maintaining control and security.

A perimeter network is not a neutral zone; it is controlled and managed by a private organization for security purposes.

A triple homed network refers to a specific configuration of a firewall or router, not a synonym for a perimeter network.

A perimeter network is not fully public; it allows filtered access to certain services while protecting the internal network.

**References****11.1.1 Network Security Zones****11.1.2 Configuring a Screened Subnet****11.1.4 Screened Subnets****11.1.5 Lab: Configure a Screened Subnet (DMZ)****11.1.6 Lab: Configure Screened Subnets**

q\_screened\_subnets\_perimeter\_dmz\_n09.question.fex



## Question 16.

✓ Correct

What is the role of VLANs in network segmentation?

- ☐ To increase the physical security of network devices
- ☒ To create separate broadcast domains
- ☐ To enforce security policies at the application layer
- ☐ To provide wireless connectivity

**Explanation**

VLANs (Virtual Local Area Networks) play a crucial role in network segmentation by creating separate broadcast domains within a network. This logical separation allows for more granular control over traffic and enhances security by isolating different parts of the network.

VLANs are not related to wireless connectivity; they are used for segmenting wired networks.

VLANs operate at layers two and three of the OSI model and do not enforce security policies at the application layer.

VLANs are concerned with logical segmentation and do not directly impact the physical security of network devices.

**References****11.1.1 Network Security Zones**

q\_net\_zones\_vlan\_role\_n09.question.fex

## Question 17.

× Incorrect

What type of storage is typically used for OS and software images in a server environment?

- ☒ SAN
- ☐ Direct-attached storage
- ☐ NAS
- ☐ Cloud storage

**Explanation**

Direct-attached storage is typically used within a server to host the operating system and software images. This type of storage is directly connected to the server and is not shared across the network.

SAN is used for variable data that requires shared access, not for OS and software images.

NAS is network-attached storage, which is different from the direct-attached storage used for OS and software images.

Cloud storage is off-premises and not directly attached to the server.

**References****14.1.3 Storage Area Networks****14.1.4 Fibre Channel****14.1.5 Lab: Configure an iSCSI Target****14.1.6 Lab: Configure an iSCSI Initiator**

q\_san\_direct-attached\_n09.question.fex

## Question 18.

✓ Correct

What is one of the primary purposes of the Internet Message Access Protocol (IMAP)?

- ☐ To deliver email to hosts that are permanently available
- ☐ To connect to web servers
- ☒ To manage a mailbox on a server
- ☐ To encrypt email messages

**Explanation**

IMAP allows a client to manage the mailbox on the server, including organizing messages in folders and controlling when they are deleted. This is the primary purpose of IMAP, making it a powerful tool for email management.

IMAP does not encrypt email messages; it is used for mailbox management. Encryption can be added with TLS or other security protocols.

SMTP, not IMAP, is used to deliver email to hosts. IMAP is focused on mailbox management.

IMAP is used for accessing and managing email mailboxes, not for connecting to web servers.

**References****7.3.2 Internet Message Access Protocol**

q\_mailbox\_imap\_primary\_purpose\_n09.question.fex

## Question 19.

✓ Correct

What is the maximum theoretical size of an IPv4 packet?

- ☐ 32 bits
- ☒ 65,535 bytes
- ☐ 1,500 bytes
- ☐ 1500 bits

**Explanation**

The maximum theoretical size of an IPv4 packet is 65,535 bytes. This limit is set by the total length field in the IPv4 header, which specifies the total size of the packet including the header and the payload.

1,500 bytes is typically the MTU for Ethernet frames, not the maximum size for an IPv4 packet.

32 bits refers to the size of the source and destination address fields, not the total packet size.

The size is measured in bytes, not bits, and 1500 bits is not the maximum size for an IPv4 packet.

**References****4.1.1 IPv4 Datagram Header**

q\_ipv4\_header\_packet\_size\_n09.question.fex

## Question 20.

✓ Correct

A multinational corporation has its main office in New York and branch offices in London, Tokyo, and Sydney. The corporation needs a network that can connect all these offices together, allowing for seamless communication and data transfer.

Which type of network would be MOST suitable for this setup?

- ☐ Small and Medium-sized Enterprise (SME) network
- ☐ Small Office/Home Office (SOHO) network
- ☐ Local Area Network (LAN)
- ☒ Wide Area Network (WAN)

**Explanation**

Wide Area Network (WAN) is the correct answer. A WAN is a network of networks, connected by long-distance links. A typical enterprise WAN would connect a main office site with multiple branch office sites, possibly in different countries. This is the most suitable type of network for a multinational corporation with offices in different countries.

A Local Area Network (LAN) is confined to a single geographical location and all nodes and segments are directly connected with cables or short-range wireless technologies. It would not be suitable for connecting offices in different countries.

A Small Office/Home Office (SOHO) network is designed for a small number of users in a single location, often using a single Internet router/switch/access point to provide connectivity. It would not be suitable for connecting multiple offices in different countries.

A Small and Medium-sized Enterprise (SME) is designed to support dozens of users in a single location, using structured cabling and multiple switches and routers to provide connectivity. It would not be suitable for connecting multiple offices in different countries.

**References****1.1.2 Network Types****1.1.3 Network Topology****1.1.4 Star Topology****1.1.7 Lab: Create Network Topologies**

q\_network\_types\_wan\_n09.question.fex

Question 21.

✓ Correct

What is the purpose of the **scp** command in SSH?

- ☐ To change the SSH server's configuration
- ☒ To securely copy files between hosts
- ☐ To list files in the remote directory
- ☐ To generate a new SSH key pair

### Explanation

The **scp** (secure copy) command is used within SSH to securely transfer files between hosts over the network. It uses SSH for data transfer and provides the same authentication and security as SSH.

Changing the server's configuration is not the purpose of **scp**; it's for file transfers.

Listing files in the remote directory is a function of **ls** in a shell session, not **scp**.

Generating a new SSH key pair is done with **ssh-keygen**, not **scp**.

### References

 **6.1.6 Common TCP and UDP Ports**

 **13.3.1 Remote Host Access**

 **13.3.2 Secure Shell**

q\_ssh\_commands\_scp\_n09.question.fex

## Question 22.

✓ Correct

What does MAC filtering on a switch allow an administrator to do?

- ☐ Monitor the amount of data transmitted by each MAC address.
- ☒ Define which MAC addresses are permitted to connect to a particular port.
- ☐ Limit the bandwidth usage per MAC address.
- ☐ Assign specific IP addresses to MAC addresses.

**Explanation**









MAC filtering enhances security by allowing only devices with specific MAC addresses to connect to a port, effectively controlling access based on hardware identifiers.

MAC filtering is about access control, not bandwidth management.

Assigning specific IP addresses to MAC addresses is incorrect as this task is typically handled by DHCP services, not MAC filtering.

Monitoring the amount of data transmitted by each MAC address is incorrect because MAC filtering's purpose is to control access, not to monitor data usage.

**References**

-  **3.1.6 Media Access Control Address Format**
-  **3.4.5 MAC Address Table**
-  **10.4.1 Network Access Control and Port Security**
-  **10.4.2 Lab: Secure Access to a Switch**
-  **10.4.3 Lab: Secure Access to a Switch 2**
-  **10.4.4 Lab: Disable Switch Ports - GUI**
-  **10.4.6 Port Guards**
-  **10.4.7 Lab: Harden a Switch**

q\_port\_security\_mac\_filtering\_n09.question.fex

## Question 23.

✓ Correct

How are the rules in a firewall's ACL processed?

- ☒ From top to bottom
- ☐ Randomly
- ☐ From bottom to top
- ☐ Simultaneously

**Explanation**

Firewall ACLs are processed sequentially from the top to the bottom. This order of processing is crucial for ensuring that the most specific rules are applied first. Once a rule that matches the traffic is found, the firewall takes the corresponding action (allow or block) and stops evaluating the rest of the rules. This method allows for efficient and precise control over network traffic.

From bottom to top is incorrect because it would mean the most general rules are evaluated first, which could lead to unintended access or blocking.

Random processing would result in unpredictable and unreliable firewall behavior, which is not acceptable in security contexts.

Firewalls do not process all rules simultaneously. Sequential processing is necessary to determine the specific action to take based on the order of the rules.

**References**

**10.5.1 Security Rules and ACL Configuration**



**10.5.5 Creating Firewall ACLs**



**10.5.6 Lab: Configure Network Security Appliance Access**



**10.5.7 Lab: Configure a Security Appliance**



**10.5.8 Lab: Configure a Perimeter Firewall**



**10.5.10 Lab: Permit Traffic**



**10.5.11 Lab: Block Source Hosts**

q\_acl\_rules\_top\_to\_bottom\_n09.question.fex



## Question 24.

✓ Correct

What distinguishes a Passive TAP from a SPAN/port mirroring connection?

- ☒ It physically copies the signal from the cabling to a monitor port.
- ☐ It requires special software to function.
- ☐ It can increase network speed.
- ☐ It can only monitor encrypted traffic.

**Explanation**

A Passive TAP is a hardware device that makes a physical copy of the data passing through a network cable to a monitoring port without affecting the original data flow. This ensures that all data, including potentially corrupt or malformed frames, is captured for analysis.

Passive TAPs monitor all traffic, not just encrypted traffic. Encryption does not affect a TAP's ability to copy data.

Passive TAPs are hardware devices and do not require software to operate. They work independently of software, making a direct copy of the traffic at the hardware level.

Passive TAPs do not affect network speed. They are designed to be transparent to the network, merely copying data for monitoring purposes without influencing network performance.

**References****8.5.1 Packet Capture**

q\_sniffers\_passive\_tap\_vs\_mirroring\_n09.question.fex

## Question 25.

✓ Correct

Which layer in the three-tiered network hierarchy is responsible for providing fault-tolerant interconnections between different access blocks?

- ☐ Core Layer
- ☐ Access Layer
- ☐ Wireless Access Layer
- ☒ Distribution Layer

**Explanation**

The distribution layer provides fault-tolerant interconnections between different access blocks and either the core or other distribution blocks. It is also used to implement traffic policies, such as routing boundaries, filtering, or quality of service (QoS).

The access layer connects end-user devices to the network.

The core layer provides a high-speed backbone for the network.

The Wireless Access Layer is not a standard layer in the three-tiered network hierarchy. The access layer includes both wired and wireless connections for end-user devices, but the "Wireless Access Layer" as a separate entity does not exist within this context.

**References****5.5.2 Three-Tiered Network Hierarchy****5.5.4 Lab: Create a Three-Tier Network**

q\_3tier\_distribution\_layer\_function\_n09.question.fex

## Question 26.

✓ Correct

Why is a zero trust architecture important in modern data centers?

- ☒ It requires each request between servers to be authorized.
- ☐ It allows unrestricted access between servers.
- ☐ It eliminates the need for physical security measures.
- ☐ It simplifies network design.

**Explanation**

Zero trust architecture is crucial because it implies a highly segmented network where each server-to-server request must be authenticated and authorized, enhancing security. It does not eliminate physical security, allow unrestricted access, or simplify network design.

Zero trust complements, rather than replaces, physical security measures.

Zero trust does the opposite of allowing unrestricted access between servers by enforcing strict access controls.

Zero trust can make network security more complex due to the need for continuous verification and authentication.

**References****14.1.1 Data Center Network Design**

q\_data\_center\_install\_zero\_trust\_n09.question.fex

## Question 27.

✓ Correct

Network data transfer works by modulating the properties of a transmission medium to encode a signal.

Which of the following BEST describes that process?

- ☒ The transmission of signals as electric current, infrared light, or radio waves
- ☐ The physical infrastructure, such as cables and switches, used to transmit data in a network
- ☐ A method of securing network data by encrypting the information before transmission
- ☐ The process of converting digital signals into analog signals for transmission over telephone lines

**Explanation**

The network data transfer process works by transmitting signals as electric current, infrared light, or radio waves. This is the fundamental method by which network signaling occurs, using electromagnetic waves to carry data.

The process of converting digital signals into analog signals for transmission over telephone lines describes modulation, specifically the process of converting digital signals into analog signals, which is not the definition of electromagnetic radiation.

A method of securing network data by encrypting the information before transmission describes a security measure, specifically encryption, which is used to protect data during transmission. While important for network security, it does not describe the physical means of transmitting signals.

The physical infrastructure, such as cables and switches, used to transmit data in a network refers to the physical components of a network used for data transmission, such as cables and switches. While these components may facilitate the transmission of network data.

**References****2.1.1 Network Data Transmission**

q\_data\_trans\_radiation\_def\_n09.question.fex

## Question 28.

✓ Correct

What type of events does an audit log generally record?

- ☐ Detailed descriptions of all user activities
- ☐ Performance metrics for compute resources
- ☒ Success/fail type events related to authentication
- ☐ System configuration backups

**Explanation**











Audit logs are focused on recording the success or failure of authentication and authorization attempts, providing a clear record of who has accessed or attempted to access the system.

While user activities related to access may be recorded, audit logs specifically track authentication and authorization events.

System configuration backups are not the purpose of audit logs.

Performance metrics are recorded in performance/traffic logs, not audit logs.

**References**

-  **8.4.1 Network Device Logs**
-  **8.4.2 Log Collectors and Syslog**
-  **8.4.3 Event Prioritization and Alerting**
-  **8.4.4 Security Information and Event Management**
-  **8.4.5 Log Reviews**
-  **8.4.6 Lab: Configure Logging in pfSense**
-  **8.4.7 Lab: Evaluate Event Logs in pfSense**
-  **8.4.8 Lab: Auditing Device Logs on a Cisco Switch**
-  **8.4.9 Lab: Configure Logging on Linux**
-  **8.4.10 Lab: View Event Logs**

q\_net\_logs\_audit\_success\_fail\_n09.question.fex

## Question 29.

✓ Correct

What is an SSH host key used for?

- ☒ Identifying the SSH server
- ☐ Encrypting all data sent over the network
- ☐ Speeding up the SSH connection process
- ☐ Storing user passwords securely

**Explanation**

The SSH host key is a public/private key pair used to identify the SSH server to clients. It ensures that the client is connecting to the correct server and not an imposter, helping to prevent on-path attacks.

While SSH does encrypt data, the host key's primary purpose is not to encrypt all data but to identify the server.

User passwords are not stored within the host key; they may be verified by the server during authentication but are not stored in the key itself.

The host key does not speed up the connection process; its role is in security and identification.

**References**

**6.1.6 Common TCP and UDP Ports**



**13.3.1 Remote Host Access**



**13.3.2 Secure Shell**

q\_ssh\_commands\_ssh\_host\_key\_purpose\_n09.question.fex

## Question 30.

✓ Correct

What is the primary purpose of using different signaling and encoding methods in data transmission?

- ☐ To decrease the baud rate for longer distance transmissions
- ☐ To increase the physical size of the data packets being transmitted
- ☐ To simplify the data transmission process
- ☒ To represent more than one bit per symbol, thereby increasing efficiency

**Explanation**

One of the main advantages of using various signaling and encoding methods is to represent multiple bits with a single symbol. This increases the efficiency of data transmission by allowing more information to be transmitted in the same amount of time or over the same bandwidth.

The physical size of data packets is not directly related to signaling and encoding methods. These methods affect how data is represented and transmitted, not the size of the packets.

The primary goal of different signaling and encoding methods is not to decrease the baud rate. While some methods may be more suitable for long-distance transmissions due to their resilience against noise and attenuation, the main purpose is to increase transmission efficiency.

Signaling and encoding methods often add complexity to the data transmission process. This complexity is justified by the benefits of increased efficiency and error detection capabilities.

**References****2.6.1 Specification and Limitations**

q\_cable\_limit\_signaling\_and\_encoding\_n09.question.fex

## Question 31.

✓ Correct

How many non-overlapping channels are recommended in the 2.4 GHz band for IEEE 802.11b to avoid co-channel interference?

- ☒ 3
- ☐ 14
- ☐ 13
- ☐ 11

**Explanation**






Only channels 1, 6, and 11 do not overlap in the 2.4 GHz band, making them the recommended choices to avoid co-channel interference.

14 is the total number of channels available in some regions, but they overlap.

11 is the number of channels available in the Americas, but not all are non-overlapping.

13 is the number of channels available in Europe, but again, not all are non-overlapping.

**References**

-  **12.1.2 IEEE 802.11a and 5GHz Channel Bandwidth**
-  **12.1.3 IEEE 802.11b/g and 2.4GHz Channel Bandwidth**
-  **12.1.4 IEEE 802.11n, MIMO, and Channel Bonding**
-  **12.1.5 Wi-Fi 5 and Wi-Fi 6**
-  **12.2.2 Range and Signal Strength**

q\_2ghz\_3\_non-overlapping\_n09.question.fex



## Question 32.

✓ Correct

What issue arises when a host has an incorrect subnet mask that is longer than it should be?

- ☐ The host's IP address is automatically changed.
- ☐ The host cannot receive any communications.
- ☒ The host misroutes its replies, thinking communicating hosts are on a different subnet.
- ☐ The host correctly routes its replies without any issues.

**Explanation**

An incorrect, longer subnet mask causes the host to misinterpret the subnet boundaries, leading to misrouted replies.

The host can still receive communications, but it may misroute its replies.

The longer subnet mask causes misrouting issues.

Subnet masks do not affect the assignment of IP addresses; they define the network and host portions of an IP address.

**References****4.6.1 IP Configuration Issues**

q\_ip\_issues\_longer\_subnet\_mask\_n09.question.fex

## Question 33.

✓ Correct

Which of the following examples BEST describes shoulder surfing?

- ☒ Someone nearby watching you enter your password on your computer and recording it
- ☐ Finding someone's password in the trash can and using it to access their account
- ☐ Guessing someone's password because it is so common or simple
- ☐ Giving someone you trust your username and account password

**Explanation**

Shoulder surfing is watching and recording a password, pin, or access code that is being entered by someone nearby.

Password guessing happens when someone is able to easily guess a password, typically because it is very common, like their pet's name or their hobby.

Dumpster diving relies on finding sensitive information that has been discarded in garbage cans, dumpsters, or other unsecure places.

Social engineering attacks rely on human error. They work by convincing someone to give the attacker access because he or she tricks them into trusting him or her.

**References****9.5.1 Social Engineering Attacks**

q\_social\_engineering\_shoulder\_example\_02\_n09.question.fex

## Question 34.

✓ Correct

What is the default VLAN ID on a switch?

- ☐ 0
- ☐ 4094
- ☐ 1001
- ☒ 1

**Explanation**

VLAN 1 is the default VLAN on all switch ports unless explicitly configured otherwise. It serves as the default network segment for devices connected to the switch.

There is no VLAN ID 0 used in standard VLAN configurations.

VLAN ID 1001 falls within the normal range but is not the default VLAN.

VLAN ID 4094 is at the upper end of the extended range and is not used as a default VLAN.

**References****5.6.2 Virtual LAN IDs and Membership**

q\_vlan\_id\_default\_vlan\_id\_n09.question.fex

## Question 35.

✓ Correct

In WPA2, what is generated using the passphrase in PSK authentication?

- ☒ Pairwise master key (PMK)
- ☐ SAE protocol
- ☐ 4-way handshake
- ☐ Password Authenticated Key Exchange (PAKE)

**Explanation**

In WPA2-PSK authentication, the passphrase is used to generate a type of hash value referred to as the pairwise master key (PMK). This PMK is then used as part of the 4-way handshake to derive various session keys.

The SAE protocol is associated with WPA3, not generated using the passphrase in WPA2-PSK.

The 4-way handshake is a process, not something generated by the passphrase.

PAKE is a general method used in WPA3, not something generated by the passphrase in WPA2-PSK.

**References**

**12.3.1 Wi-Fi Encryption Standards**



**12.3.2 Personal Authentication**



**12.3.3 Enterprise Authentication**

q\_wifi\_auth\_pmk\_generation\_n09.question.fex

## Question 36.

✓ Correct

What protocol does WPA introduce to mitigate attacks against WEP?

- ☒ TKIP
- ☐ AES
- ☐ CCMP
- ☐ GCMP

**Explanation**

The Temporal Key Integrity Protocol (TKIP) was introduced with WPA as a stopgap solution to mitigate the vulnerabilities found in WEP, without requiring new hardware. TKIP included features like key mixing and a sequence counter to prevent replay attacks.

AES is an encryption standard used in WPA2, not a protocol to mitigate attacks.

CCMP is introduced with WPA2 as a replacement for TKIP, offering enhanced security.

GCMP is used in WPA3, not in WPA, and serves a different purpose.

**References****12.3.1 Wi-Fi Encryption Standards**

q\_wireless\_encrypt\_tkip\_mitigate\_attacks\_n09.question.fex

## Question 37.

✓ Correct

What is the purpose of using a VPN with an open Wi-Fi network?

- ☒ To create an encrypted tunnel for secure communication
- ☐ To allow unrestricted access to all network resources
- ☐ To bypass the need for a captive portal
- ☐ To decrease the network's bandwidth usage

**Explanation**

A VPN creates an encrypted "tunnel" between the user's device and the VPN server, securing the user's internet activities from eavesdropping on an open Wi-Fi network. This is crucial for protecting sensitive data when using unsecured networks.

Using a VPN does not decrease bandwidth usage; it encrypts data, which can sometimes increase bandwidth usage due to encryption overhead.

A VPN does not grant unrestricted access to all network resources but secures the user's internet traffic.

The purpose of a VPN is not to bypass captive portals but to secure data transmission over unsecured networks.

**References**

**13.2.2 Tunneling Protocols**



**13.2.8 Lab: Configure a Remote Access VPN**



**13.2.9 Lab: Configure an iPad VPN Connection**



**13.2.10 Lab: Configure a RADIUS Solution**

q\_captive\_portal\_vpn\_use\_n09.question.fex

## Question 38.

✓ Correct

What is the primary purpose of Wavelength Division Multiplexing (WDM)?

- ☐ To decrease the overall data transmission rate
- ☐ To increase the latency of data transmission
- ☒ To provision multiple channels over one or two strands of fiber
- ☐ To reduce the bandwidth of individual channels

**Explanation**








WDM allows for the transmission of multiple data channels over a single or dual fiber strand(s) by using different wavelengths for each channel, thereby increasing the capacity of the fiber without needing additional strands.

WDM does not reduce the bandwidth of individual channels; it allows multiple channels to coexist on the same fiber strand.

WDM aims to efficiently use fiber strands to increase capacity, not to increase latency. In fact, it can help in reducing overall network latency by optimizing the use of available infrastructure.

WDM is used to increase the data transmission rate by allowing multiple channels to transmit data simultaneously over the same fiber, not to decrease it.

**References**

-  **2.3.1 Structured Cabling System**
-  **2.3.4 Structured Cable Installation**
-  **2.3.6 Lab: Explore Multiple Locations in a Lab**
-  **2.3.8 Lab: Connect Patch Panel Cables 1**
-  **2.3.9 Lab: Connect Patch Panel Cables 2**
-  **2.4.4 Fiber Optic Cable Installation**
-  **2.4.7 Wavelength Division Multiplexing**

q\_wave\_multi\_primary\_purpose\_n09.question.fex

## Question 39.

✓ Correct

What does the client do to ensure the offered IP address is not already in use?

- ☐ Sends a DHCPDISCOVER packet
- ☐ Sends a DHCPOFFER packet
- ☐ Sends a DHCPREQUEST packet
- ☒ Broadcasts an ARP message

**Explanation**














After receiving a DHCPACK, the client broadcasts an ARP message to ensure the offered IP address is not already in use.

Sending a DHCPDISCOVER packet is used to find DHCP servers, not to check for IP address conflicts.

Sending a DHCPOFFER packet is a server action, not a client action.

Sending a DHCPREQUEST packet is used to request an IP address, not to check for its availability.

**References**

-  **6.2.1 DHCP Process**
-  **6.2.2 DHCP Server Configuration**
-  **6.2.3 DHCP Options**
-  **6.2.4 DHCP Reservations and Exclusions**
-  **6.2.5 Lab: Configure a DHCP Server**
-  **6.2.6 Lab: Configure DHCP Server Options**
-  **6.2.7 Lab: Create DHCP Exclusions**
-  **6.2.8 Lab: Create DHCP Client Reservations**
-  **6.2.9 Configure Client Addressing**
-  **6.2.10 Lab: Configure Client Addressing for DHCP**
-  **6.3.2 IPv6 Interface Autoconfiguration and Testing**
-  **6.3.3 DHCPv6 Server Configuration**
-  **6.3.6 Set Up Alternate Addressing**



**6.4.1 DHCP Relay and IP Helper****6.4.2 DHCP Issues****6.4.3 Troubleshooting DHCP Exhaustion****6.4.4 Lab: Configure a DHCP Relay Agent****6.4.5 Lab: Add a DHCP Server on Another Subnet****6.4.6 Lab: Troubleshoot Address Pool Exhaustion****6.4.7 Lab: Explore DHCP Troubleshooting****6.4.8 Lab: Troubleshoot IP Configuration 1****6.4.9 Lab: Troubleshoot IP Configuration 2****6.4.10 Lab: Troubleshoot IP Configuration 3****6.6.1 Client DNS Issues**

q\_dhcp\_overview\_arp\_message\_broadcast\_n09.question.fex

## Question 40.

✓ Correct

What mechanism do stations use to determine an appropriate data rate based on signal quality?

- ☐ Adaptive Frequency Selection
- ☐ Signal Quality Assessment
- ☐ Fixed Rate Selection
- ☒ Dynamic Rate Switching/Selection (DRS)

**Explanation**

The correct answer is Dynamic Rate Switching/Selection (DRS). DRS allows stations to dynamically adjust the data rate based on the quality of the signal, ensuring optimal performance under varying conditions.

Fixed Rate Selection is incorrect because it implies a static choice that does not adapt to signal quality changes.

Signal Quality Assessment and Adaptive Frequency Selection are incorrect as they describe processes or concepts that are related to but not specifically the mechanism by which data rates are adjusted based on signal quality.

**References****12.2.2 Range and Signal Strength**

q\_signal\_strength\_drs\_n09.question.fex

## Question 41.

✓ Correct

What is the primary purpose of a data center?

- ☐ To serve as a storage facility for physical documents
- ☐ To provide a workspace for employees
- ☐ To function as a retail space for technology products
- ☒ To host network services and server resources

**Explanation**

A data center is dedicated to provisioning server resources and hosting network services such as authentication, addressing, name resolution, application servers, and storage area networks (SANs). It is not meant for employee workspaces, storing physical documents, or functioning as a retail space.

Although data centers may have staff, their main function is not to serve as a workspace but to house computing and networking equipment.

Data centers are focused on digital data storage and processing, not physical documents.

Data centers are operational facilities for IT infrastructure, not retail spaces.

**References****14.1.1 Data Center Network Design**

q\_data\_center\_install\_primary\_purpose\_n09.question.fex

## Question 42.

✓ Correct

Which of the following is an example of Software as a Service (SaaS)?

- ☐ Oracle Database
- ☒ Microsoft Office 365
- ☐ OpenStack
- ☐ Amazon Elastic Compute Cloud

**Explanation**

Microsoft Office 365 is a subscription service that gives users access to various Microsoft applications and services over the Internet. This is a classic example of SaaS, where software is provided as a service rather than installed on individual devices.

Amazon Elastic Compute Cloud (EC2) is an example of IaaS, not SaaS.

Oracle Database can be part of PaaS when provided as a cloud service, not SaaS.

OpenStack is an open-source cloud computing platform for public and private clouds, more aligned with IaaS.

**References****14.2.3 Cloud Service Models**

q\_cloud\_service\_saas\_example\_n09.question.fex

## Question 43.

✓ Correct

A network architect is reviewing a network where application services and resources are centrally provisioned, managed, and secured.

What is this type of network called?

- ☐ SOHO
- ☒ Client server
- ☐ Peer to peer
- ☐ Point to point

**Explanation**

A client-server network is one where some nodes, such as PCs, laptops, and smartphones, act mostly as clients. Application services and resources are centrally provisioned, managed, and secured.

A peer-to-peer network is one where each end system acts as both client and server. A peer-to-peer network is a decentralized model where provision, management, and security of services and data distributes around the network.

In the simplest type of topology, a single link gets established between two nodes. This is known as a point-to-point link.

Small office/home office (SOHO) networks are business-oriented networks, possibly using a centralized server in addition to client devices and printers, but often still using a single Internet router/switch/access point.

**References****1.1.2 Network Types****1.1.3 Network Topology****1.1.4 Star Topology****1.1.7 Lab: Create Network Topologies**

q\_net\_concepts\_client\_server\_02\_n09.question.fex

## Question 44.

✓ Correct

What is the primary purpose of using a hybrid topology in modern networks?

- ☐ To limit the number of devices in the network
- ☒ To implement redundancy and fault tolerance
- ☐ To reduce the overall cost of the network infrastructure
- ☐ To simplify network design and management

**Explanation**

Hybrid topologies are often used to ensure network reliability and availability through redundancy and fault tolerance.

While cost can be a factor, the primary purpose of a hybrid topology is not necessarily to reduce costs but to enhance network capabilities.

Hybrid topologies can actually complicate network design and management due to their complexity.

A hybrid topology can actually increase the number of devices and connections to achieve its goals of redundancy and fault tolerance.

**References****5.5.1 Hybrid Topology**

q\_hybrid\_modern\_network\_purpose\_n09.question.fex

## Question 45.

✓ Correct

What is a common consequence of rogue devices and services in a network?

- ☐ Increased network security.
- ☒ Creation of new unmonitored attack surfaces.
- ☐ Improved network efficiency.
- ☐ Reduction in IT department workload.

**Explanation**

Rogue devices and services create new unmonitored attack surfaces that malicious adversaries can exploit, posing significant security risks.

Rogue devices and services typically compromise network efficiency by introducing security risks.

Rogue devices and services decrease network security by operating outside of administrative control.

The introduction of rogue devices and services increases the IT department's workload due to the need to identify and mitigate these security risks.

**References****9.4.1 Rogue Devices and Services**

q\_rogue\_devices\_common\_consequence\_n09.question.fex

## Question 46.

✓ Correct

What is a Content Delivery Network (CDN)?

- ☐ A type of IaaS focused on providing storage solutions
- ☐ A cloud service model for delivering software applications
- ☐ A service that provides tools for application development
- ☒ A network of servers used to deliver content to users worldwide

**Explanation**

A Content Delivery Network (CDN) is a system of distributed servers that deliver web content and other web services to users based on their geographic locations. The goal is to provide high availability and performance by distributing the service spatially relative to end-users.

CDNs do not provide tools for application development; they are focused on content delivery.

CDNs are not a cloud service model like SaaS; they are a specific infrastructure setup for content delivery.

While CDNs involve storage, they are not a type of IaaS focused solely on providing storage solutions; their primary purpose is efficient content delivery.

**References****14.2.4 Content Delivery Networks**

q\_cloud\_service\_cdn\_description\_n09.question.fex



## Question 47.

✓ Correct

What is the signal to noise ratio (SNR)?

- ☐ The ratio of network throughput to bit rate
- ☐ The ratio of data transfer rate to latency
- ☒ The ratio of signal strength to noise level
- ☐ The ratio of encryption strength to decryption time

**Explanation**

SNR is a critical metric in wireless communications that compares the level of a desired signal to the level of background noise. A higher SNR indicates a clearer signal, which is essential for achieving optimal wireless performance.

The ratio of data transfer rate to latency describes a different aspect of network performance and is not related to SNR.

The ratio of encryption strength to decryption time pertains to security measures, not the clarity or quality of a wireless signal.

The ratio of network throughput to bit rate describes aspects of data transfer rates, not the quality of the signal in terms of its clarity or usability.

**References****12.4.1 Wireless Performance Assessment**

q\_wifi\_assess\_snr\_description\_n09.question.fex

## Question 48.

✓ Correct

What distinguishes an Operational Technology (OT) network from a standard IT data network?

- ☐ OT networks cannot use industrial Ethernet.
- ☐ OT networks use standard Ethernet only.
- ☐ OT networks are primarily used for gaming.
- ☒ OT networks are optimized for real-time transfers.

**Explanation**

OT networks are designed for industrial systems and are optimized for real-time, deterministic data transfers, which is crucial for industrial applications that require precise timing and reliability. This distinguishes them from standard IT data networks, which may not have such stringent requirements for real-time data transfer.

OT networks are used for industrial systems, not for gaming, which is typically associated with IT networks or specialized gaming networks.

While OT networks can use industrial Ethernet, they are not limited to standard Ethernet; they can also use serial data protocols and vendor-developed protocols.

OT networks can indeed use industrial Ethernet, which is optimized for their specific needs.

**References****11.2.2 Industrial Embedded Systems**

q\_iot\_network\_ot\_vs\_standard\_network\_n09.question.fex

## Question 49.

✓ Correct

What is the advantage of using automated builds from templates over master images?

- ☐ Higher security
- ☒ Easier updates
- ☐ Less storage space
- ☐ Faster deployment

**Explanation**

Automated builds from templates allow for easier updates since the template can be modified and then used to provision new instances with the latest configurations, rather than updating a master image directly.

Master images are typically faster than automated builds to deploy since they are pre-configured.

Security benefits depend more on the content of the image or template than the method used.

While templates might use less space than storing multiple images, the primary advantage is the ease of updating.

**References****14.4.1 Infrastructure as Code**

q\_automation\_automated\_builds\_advantage\_n09.question.fex

## Question 50.

✓ Correct

Which of the following is a function of a Cloud Access Security Broker (CASB)?

- ☒ Monitors and audits user and resource activity
- ☐ Increases the speed of cloud services
- ☐ Reduces the cost of cloud storage
- ☐ Directly improves the performance of SD-WAN connections

**Explanation**

Monitoring and auditing user and resource activity is the correct answer. One of the key functions of a CASB is to provide visibility into cloud application usage, monitor user activities, and audit resource accesses. This is crucial for detecting and responding to security threats, ensuring compliance with data protection regulations, and preventing data leaks.

CASBs primarily focus on security aspects rather than enhancing the speed of cloud services. Their role is to enforce security policies between cloud users and cloud applications, which includes monitoring, compliance, and threat protection, but not directly increasing service speeds.

While CASBs can help organizations use cloud services more securely and efficiently, their primary function is not to reduce the cost of cloud storage. They are security tools that manage and protect cloud environments rather than tools designed for cost optimization of storage resources.

CASBs do not directly improve the performance of SD-WAN connections. Their role is to secure access to cloud services by mediating between users and cloud applications, implementing security policies, and providing threat protection. While they may work alongside SD-WAN technologies in a Secure Access Service Edge (SASE) architecture, their primary focus is on security rather than enhancing network performance.

**References****14.4.8 Secure Access Service Edge**

q\_secure\_edge\_casb\_function\_n09.question.fex

## Question 51.

✓ Correct

What is the primary purpose of Wide Area Networks (WAN)?

- ☐ To provide high-speed Internet to households only
- ☐ To connect computers within a single room
- ☐ To connect devices within a single building
- ☒ To support data communications over greater distances than LANs

**Explanation**











WAN technologies are specifically designed to facilitate data communication over large distances, surpassing the capabilities of Local Area Networks (LANs) which are limited to smaller geographical areas like a building or campus.

WANs are designed for much larger geographical areas than a single room, which is typically the domain of Personal Area Networks (PANs).

WANs are used not only to provide Internet to households but also to connect businesses and provide services across cities, countries, and continents.

Connecting devices within a single building is the primary function of LANs, not WANs.

**References**

-  **1.2.1 Open Systems Interconnection Model**
-  **1.2.5 Layer 3 - Network**
-  **1.2.8 OSI Model Summary**
-  **1.3.4 Network Layer Functions**
-  **1.3.6 The Internet**
-  **1.3.7 Binary and Hexadecimal**
-  **1.3.8 Lab: Explore a Single Location in a Lab**
-  **4.1.2 Layer 2 vs. Layer 3 Addressing and Forwarding**
-  **13.1.1 Wide Area Networks and the OSI Model**
-  **14.3.5 Cloud Firewall Security**

q\_wan\_primary\_purpose\_n09.question.fex

## Question 52.

✓ Correct

You manage a network that has multiple internal subnets. You connect a workstation to the 192.168.1.0/24 subnet.

This workstation cannot communicate with any other host on the network. You run **ipconfig /all** and see the following:

```
Ethernet adapter Local Area Connection:  
Connection-specific DNS Suffix. : mydomain.local  
Description . . . . . : Broadcom network adapter  
Physical Address . . . . . : 00-AA-BB-CC-74-EF  
DHCP Enabled. . . . . : No  
Autoconfiguration Enabled . . : Yes  
IPv4 Address. . . . . : 192.168.2.102 (Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway. . . . . : 192.168.1.1  
DNS Servers . . . . . : 192.168.2.20
```










What is the MOST likely cause of the problem?

- ☐ Incorrect default gateway
- ☒ Incorrect IP address
- ☐ Incorrect subnet mask
- ☐ Incorrect DNS server address

**Explanation**

In this example, the IP address assigned to the host is on the wrong subnet. The host address is on the 192.168.2.0/24 subnet, but the other devices are using addresses on the 192.168.1.0 subnet (the scenario states that you're connecting the workstation to this subnet).

**References**

-  **4.4.1 ipconfig**
-  **4.4.2 ifconfig and ip**
-  **4.4.5 Lab: IPv4 Troubleshooting Tools**
-  **4.4.6 Lab: IPv4 Troubleshooting tools for Linux**
-  **4.4.7 Lab: Use IPv4 Test Tools**
-  **6.4.6 Lab: Troubleshoot Address Pool Exhaustion**
-  **6.4.8 Lab: Troubleshoot IP Configuration 1**
-  **6.4.9 Lab: Troubleshoot IP Configuration 2**
-  **6.4.10 Lab: Troubleshoot IP Configuration 3**



## 6.6.1 Client DNS Issues



## 6.6.2 Name Resolution Issues

q\_ipconfig\_incorrect\_address\_scenario\_n09.question.fex

### Question 53.

✓ Correct

What role does virtualization play in cloud computing?

- ☐ It allows for the physical transfer of data between servers.
- ☐ It ensures data security and compliance.
- ☒ It enables provisioning and deprovisioning of resources.
- ☐ It reduces the need for internet connectivity.

#### Explanation

Virtualization is a technology that creates virtual instances of resources, such as servers or storage, from a single physical hardware system. This allows cloud providers to quickly provision and deprovision resources as needed, without manual intervention, making it possible to achieve both scalability and elasticity.

While virtualization can contribute to security by isolating environments, its primary role in cloud computing is not security or compliance.

Virtualization is about creating virtual resources, not physically transferring data between servers.

Virtualization does not impact the need for internet connectivity; it's about resource management within the cloud infrastructure.

#### References



## 14.2.1 Cloud Scalability and Elasticity

q\_cloud\_scale\_virtualization\_n09.question.fex

## Question 54.

✓ Correct

What is the primary purpose of trunking in a network?

- ☐ To connect a computer to the Internet
- ☐ To increase the security of the network
- ☐ To replace wireless connections with wired connections
- ☒ To interconnect multiple switches and build the network fabric

**Explanation**

Trunking is used to connect multiple network switches together, allowing for the creation of a larger network infrastructure. This is essential in environments where a single switch cannot provide enough ports to connect all devices, thereby necessitating the use of multiple switches to form a cohesive network fabric.

Connecting a computer to the Internet is a function of routers and modems, not trunking. Trunking specifically refers to the practice of linking switches to expand the network.

Trunking does not specifically aim to replace wireless connections; it is a method used in wired networks to interconnect switches. Both wired and wireless connections have their own applications and are used based on different criteria.

While trunking can contribute to network security by segregating traffic into VLANs, its primary purpose is not security but rather the expansion and interconnection of the network infrastructure.

**References****5.6.3 Trunking and IEEE 802.1Q**

q\_trunking\_primary\_purpose\_n09.question.fex



## Question 55.

✓ Correct

How does elasticity differ from scalability in cloud computing?

- ☐ Elasticity is about adding more resources, while scalability is about removing resources.
- ☐ Scalability is a technology, while elasticity is a business strategy.
- ☐ Scalability involves using multiple cloud providers, whereas elasticity does not.
- ☒ Elasticity focuses on real-time adjustments, while scalability is about long-term growth.

**Explanation**

Elasticity is the ability of a cloud system to automatically adjust resources in real-time based on fluctuating demand, ensuring optimal performance and cost-efficiency. Scalability, on the other hand, refers to the system's ability to handle increased workloads or users over time in a linear and cost-effective manner. Both concepts are crucial for cloud computing but address different aspects of resource management.

Both elasticity and scalability can involve adding or removing resources, but they differ in their focus and timing (real-time vs. long-term).

Using multiple cloud providers is a strategy related to cloud sourcing or multi-cloud environments, not a distinction between elasticity and scalability.

Both scalability and elasticity are technological capabilities enabled by cloud computing, not a distinction between technology and strategy.

**References****14.2.1 Cloud Scalability and Elasticity**

q\_cloud\_scale\_elasticity\_vs\_scalability\_n09.question.fex

## Question 56.

✓ Correct

An administrator ran a command and determined that the FQDN of a client is forbes.sales.realty.com.

What is the hostname of the client?

- ☐ realty
- ☐ sales
- ☒ forbes
- ☐ com

**Explanation**












A fully qualified domain name (FQDN) consists of the hostname and a domain suffix. In this domain, forbes is the hostname and the domain suffix is sales.realty.com.












A fully qualified domain name (FQDN) consists of the hostname and a domain suffix. In this domain, the suffix .com is the top-level domain.

A fully qualified domain name (FQDN) consists of the hostname and a domain suffix. In this domain, sales is a domain name within the top-level domain .com.

A fully qualified domain name (FQDN) consists of the hostname and a domain suffix. In this domain, realty is a domain name within the top-level domain .com.

**References**

-  **6.5.1 Host Names and Domain Names**
-  **6.5.2 DNS Hierarchy**
-  **6.5.3 Name Resolution Using DNS**
-  **6.5.4 Resource Record Types**
-  **6.5.5 Host Address and Canonical Name Records**
-  **6.5.6 Mail Exchange, Service, and Text Records**
-  **6.5.7 Pointer Records**
-  **6.5.8 DNS Server Configuration**
-  **6.5.9 Internal vs External DNS**
-  **6.5.10 DNS Security**
-  **6.5.11 Lab: Configure DNS Addresses**

-  **6.5.12 Lab: Create Standard DNS Zones**
  -  **6.5.13 Lab: Create Host Records**
  -  **6.5.14 Lab: Create CNAME Records**
  -  **6.5.15 Lab: Troubleshoot DNS Records**
  -  **6.5.16 Configuring DNS Caching on Linux**
  -  **6.6.1 Client DNS Issues**
  -  **6.6.2 Name Resolution Issues**
  -  **6.6.3 nslookup**
  -  **6.6.4 dig**
  -  **6.6.5 Lab: Explore nslookup**
  -  **6.6.6 Lab: Use nslookup**
- q\_dns\_overview\_hostname\_example\_n09.question.fex

## Question 57.

✓ Correct

Why do organizations often choose to use public networks for their WAN services?

- ☒ Because the cost is far less than implementing a private solution
- ☐ Because public networks offer the highest security
- ☐ Because public networks are faster than private networks
- ☐ Because public networks do not require any infrastructure

**Explanation**











Using public networks can significantly reduce costs for organizations compared to the expense of setting up and maintaining a private network infrastructure.

Public networks, being accessible by many entities, typically pose more security challenges than private networks.

The speed of a network depends on various factors, and public networks are not inherently faster than private ones.

Public networks do require infrastructure, but it is owned and maintained by telecommunications companies rather than the organization using the service.

**References**

-  **1.2.1 Open Systems Interconnection Model**
-  **1.2.5 Layer 3 - Network**
-  **1.2.8 OSI Model Summary**
-  **1.3.4 Network Layer Functions**
-  **1.3.6 The Internet**
-  **1.3.7 Binary and Hexadecimal**
-  **1.3.8 Lab: Explore a Single Location in a Lab**
-  **4.1.2 Layer 2 vs. Layer 3 Addressing and Forwarding**
-  **13.1.1 Wide Area Networks and the OSI Model**
-  **14.3.5 Cloud Firewall Security**

q\_wan\_public\_networks\_n09.question.fex

## Question 58.

✓ Correct

At which layer of the OSI model do WANs often use simpler protocols compared to LANs?

- ☐ Transport layer
- ☐ Network layer
- ☒ Data Link layer
- ☐ Physical layer

**Explanation**








The correct answer is the Data Link Layer. At the Data Link layer, WANs often use simpler protocols than LANs due to the point-to-point nature of many WAN connections, which requires less complexity.

The Physical layer describes the media type and interface specifications, not the complexity of protocols.

The Network layer is primarily concerned with addressing and routing, not the complexity of the protocols used.

The Transport layer is responsible for end-to-end communication and data transfer management, not the simplicity or complexity of WAN protocols.

**References**

-  **1.2.1 Open Systems Interconnection Model**
-  **1.2.4 Layer 2 - Data Link**
-  **1.2.8 OSI Model Summary**
-  **1.3.3 Data Link Layer Functions**
-  **1.3.8 Lab: Explore a Single Location in a Lab**
-  **4.1.2 Layer 2 vs. Layer 3 Addressing and Forwarding**
-  **13.1.1 Wide Area Networks and the OSI Model**

q\_wan\_data\_link\_layer\_n09.question.fex

## Question 59.

✓ Correct

Which server is commonly used to maintain source code in software development environments?

- ☐ Email Server
- ☐ Web Server
- ☒ Repository Server
- ☐ FTP Server

**Explanation**

A repository server, such as Git, is used in software development environments to maintain and manage source code. It allows developers to commit changes, track versions, and collaborate effectively.

FTP servers are used for file transfers and not specifically for maintaining source code.

Email servers manage email communications and are not used for source code management.

Web servers host websites and web applications but do not serve as the central system for source code management.

**References****14.4.3 Source Control**

q\_source\_control\_repository\_server\_n09.question.fex

## Question 60.

✓ Correct

What defines "risk" in the context of computer security?

- ☒ The likelihood and impact of a threat actor exercising a vulnerability
- ☐ A measure of how well a system can resist being compromised
- ☐ The potential for someone or something to exploit a vulnerability and breach security
- ☐ A weakness that could be accidentally triggered or intentionally exploited to cause a security breach

**Explanation**

The correct answer is the likelihood and impact of a threat actor exercising a vulnerability. Risk in computer security is a function of the likelihood of a given threat source exploiting a particular vulnerability and the resulting impact of that event on the organization. It assesses the potential harm that could arise from a breach in security, considering both the probability and the consequences of such an event.

A measure of how well a system can resist being compromised is more related to the concept of resilience or the effectiveness of security measures, not the definition of risk.

The potential for someone or something to exploit a vulnerability and breach security describes "threat," which is the potential for exploitation, not the combined likelihood and impact of such exploitation.

A weakness that could be accidentally triggered or intentionally exploited to cause a security breach describes "vulnerability," which is a specific weakness that could be exploited, not the potential impact and likelihood of such exploitation.

**References**

**9.1.1 Common Security Terminology**



**9.1.2 Security Audits and Assessments**

q\_sec\_concepts\_risk\_n09.question.fex

## Question 61.

✓ Correct

Which factor determines the type of credential a subject can use for authentication?

- ☒ Authentication factor
- ☐ Authorization model
- ☐ Identification process
- ☐ Accounting system

**Explanation**








The correct answer is authentication factor. Authentication factors are criteria used to verify an entity's identity. These can include something the entity knows (password), something the entity has (token), or something the entity is (biometric).

The authorization model determines access rights and permissions, not the type of credentials used for authentication.

The accounting system tracks and records access and actions within the system, unrelated to the determination of authentication credentials.

While identification is the process of recognizing an entity, it does not determine the type of credentials used for authentication.

**References**

-  **10.1.1 Access Control**
-  **10.1.2 Authentication Methods**
-  **10.1.3 Local Authentication**
-  **10.1.4 Single Sign-On and Kerberos**
-  **10.1.8 Remote Authentication**
-  **10.3.4 Scanning for Unsecure Protocols**
-  **13.2.1 Remote Access Considerations**

q\_access\_control\_authentication\_factor\_n09.question.fex



## Question 62.

✓ Correct

What can cause convergence problems in a dynamic routing network?

- ☐ A stable network with no changes
- ☐ The use of static routing protocols
- ☒ A flapping interface
- ☐ Consistent routing information across all routers

**Explanation**

A flapping interface, which frequently changes its state from up to down and back again, can cause convergence problems. This is because each state change can trigger the routers to recalculate routes, leading to instability and inconsistent routing information across the network.

A stable network with no changes would actually facilitate convergence, not cause problems.

Consistent routing information is the goal of convergence, not a cause of its problems.

Static routing protocols do not participate in convergence; they are manually configured and do not adapt to network changes.

**References****5.2.1 Dynamic Routing Protocols**

q\_dyroute\_flapping\_interface\_n09.question.fex

## Question 63.

✓ Correct

What role does a Programmable Logic Controller (PLC) play in an ICS?

- ☐ It acts as a firewall for industrial devices.
- ☐ It serves as a data storage unit for industrial information.
- ☒ It controls industrial machinery and processes.
- ☐ It provides internet access to industrial devices.

**Explanation**

PLCs are embedded programmable controllers that play a crucial role in an ICS by controlling and monitoring industrial machinery and processes. They are linked to actuators and sensors to manage and oversee operations, ensuring efficiency and safety.

Providing internet access is not the primary function of a PLC.

Acting as a firewall is related to network security, not the direct control of machinery.

Serving as a data storage unit is more closely related to the role of a data historian.

**References****11.2.2 Industrial Embedded Systems**

q\_ctrl\_system\_pls\_role\_ics\_n09.question.fex

## Question 64.

✓ Correct

Which example best represents Infrastructure as a Service (IaaS)?

- ☐ Salesforce
- ☐ Google Workspace
- ☐ Microsoft Office 365
- ☒ Amazon Elastic Compute Cloud (EC2)

**Explanation**

Amazon Elastic Compute Cloud (EC2) is a service that provides scalable computing capacity in the Amazon Web Services (AWS) cloud. It allows users to run virtual servers and is a classic example of Infrastructure as a Service (IaaS), providing the raw computing infrastructure over the internet.

Salesforce is an example of Software as a Service (SaaS), offering CRM software over the Internet.

Google Workspace is also an example of SaaS, providing a suite of productivity and collaboration tools.

Microsoft Office 365 is a SaaS offering, providing access to Microsoft's productivity software suite over the Internet.

**References****14.2.3 Cloud Service Models**

q\_cloud\_service\_iaas\_example\_03\_n09.question.fex

## Question 65.

✓ Correct

What is the function of the Request to Send (RTS) and Clear To Send (CTS) mechanism in IEEE 802.11 networks?

- ☐ To increase the transmission speed
- ☐ To assign IP addresses to devices
- ☐ To encrypt data transmissions
- ☒ To further reduce the incidence of collisions

**Explanation**





The Request to Send (RTS) and Clear To Send (CTS) mechanism in IEEE 802.11 networks is used to further reduce the incidence of collisions. By broadcasting an RTS with the source, destination, and time required to transmit, and receiving a CTS in response, other stations are informed not to transmit during that period, thus minimizing the chance of collisions.

RTS and CTS are not used for encrypting data transmissions but for managing access to the medium.

Assigning IP addresses is not the function of RTS and CTS; it is typically handled by other protocols such as DHCP.

The primary goal of RTS and CTS is to manage medium access and reduce collisions, not to directly increase transmission speed.

**References**

-  **12.1.1 IEEE 802.11 Wireless Standards**
-  **12.1.2 IEEE 802.11a and 5GHz Channel Bandwidth**
-  **12.1.4 IEEE 802.11n, MIMO, and Channel Bonding**
-  **12.1.6 Multiuser MIMO and Band Steering**

q\_wireless\_rts\_cts\_function\_n09.question.fex

## Question 66.

✓ Correct

What is the primary advantage of using Time Division Multiplexing (TDM) in T-carrier systems?

- ☐ It encrypts data for secure transmission.
- ☐ It reduces the cost of internet services.
- ☐ It converts analog signals to digital signals.
- ☒ It enables the simultaneous transmission of multiple signals over a single transmission path.

**Explanation**

Time Division Multiplexing (TDM) is a method used in T-carrier systems that enables multiple signals to be transmitted simultaneously over a single transmission path. By assigning each circuit (or channel) a specific time slot, multiple channels can share the same transmission medium (such as a T1 line) without interference, effectively increasing the capacity of the medium.

TDM does not inherently encrypt data; its primary function is to multiplex multiple signals for transmission.

TDM is not about converting signals from analog to digital; it's a multiplexing technique used for digital signals.

While TDM can improve the efficiency of data transmission, its primary advantage is not reducing the cost of internet services but increasing transmission capacity.

**References****13.1.2 Internet Access Types**

q\_wan\_prov\_tdm\_advantage\_n09.question.fex

## Question 67.

✓ Correct

What does the bit rate measure in a wireless network?

- ☐ The efficiency of the network protocol
- ☒ The total amount of data transferred per second
- ☐ The security level of the network
- ☐ The total number of errors in data transmission

**Explanation**

Bit rate is a measure of how much data is transferred over a network in a given second, specifically at the Physical and Data Link layers. It's a crucial metric for understanding the capacity of a wireless connection.

The security level of the network is not quantified by the bit rate but rather by the encryption standards and protocols in use.

The number of errors in data transmission is typically measured by error rates, not bit rate.

The efficiency of the network protocol is related to how well data is transmitted over the network but is not directly measured by the bit rate.

**References****12.4.1 Wireless Performance Assessment**

q\_wifi\_assess\_bit\_rate\_measure\_n09.question.fex

## Question 68.

× Incorrect

What is the primary difference between tagged and untagged ports regarding VLAN tags?

- ☐ Tagged ports strip VLAN tags from incoming frames.
- ☐ Untagged ports can transport traffic for multiple VLANs.
- ☒ Tagged ports add a VLAN tag to all outgoing frames.
- ☐ Untagged ports do not add or remove VLAN tags from frames within the same VLAN.

**Explanation**

Untagged ports, being configured for a single VLAN, do not need to add or remove VLAN tags when forwarding traffic within the same VLAN. The traffic is inherently part of that VLAN.

Tagged ports add a VLAN tag only when necessary, such as when forwarding traffic over a trunk link.

Untagged ports are designed for a single VLAN, not multiple VLANs.

Tagged ports do not strip VLAN tags from incoming frames; they forward frames with the tags to appropriate VLANs.

**References****5.6.4 Tagged and Untagged Ports**

q\_tagged\_vs\_untagged\_ports\_n09.question.fex

## Question 69.

✓ Correct

What does ingress and egress traffic filtering refer to?

- ☐ Monitoring internet usage and bandwidth
- ☐ Encrypting data entering and leaving a network
- ☒ Controlling both inbound and outbound network traffic
- ☐ Filtering both internal and external emails

**Explanation**

The correct answer is to control both inbound and outbound network traffic. Ingress filtering controls incoming traffic to the network, while egress filtering controls outgoing traffic, together ensuring comprehensive traffic management for security purposes.

Ingress and egress filtering apply to all network traffic, not just emails.

The focus is on controlling traffic flow, not encrypting data.

The primary goal is to manage traffic for security reasons, not to monitor usage or bandwidth.

**References**

**1.3.5 Transport and Application Layer and Security Functions**



**5.4.1 Firewall Uses and Types**



**5.4.2 Firewall Selection and Placement**



**10.5.1 Security Rules and ACL Configuration**



**10.5.4 Misconfigured Firewall and ACL Issues**



**10.5.5 Creating Firewall ACLs**



**10.5.7 Lab: Configure a Security Appliance**



**10.5.8 Lab: Configure a Perimeter Firewall**



**14.3.5 Cloud Firewall Security**

q\_firewalls\_ingress\_egress\_n09.question.fex



## Question 70.

✓ Correct

What is a Protocol Data Unit (PDU)?

- ☐ A type of encryption used in data transmission
- ☐ A device that manages data transmission rates
- ☐ A measure of data transmission speed
- ☒ A chunk of data with protocol-specific headers added at each OSI layer

**Explanation**

A Protocol Data Unit (PDU) is the term used to describe the form that data takes at each layer of the OSI model. As data traverses down the layers on the sending node, each layer encapsulates the data by adding its specific headers (and sometimes footers), creating a PDU appropriate for that layer. This process ensures that data can be correctly processed, transmitted, and understood at each stage of its journey.

A PDU is not a device but a structured form of data as it is handled by network protocols.

A PDU refers to the format of data within network protocols, not a measure of speed.

A PDU pertains to the structure of data for protocol processing, not a method of encryption.

**References**

 **1.2.2 Data Encapsulation and Decapsulation**

 **14.4.6 Overlay Networks**

q\_data\_encapsulation\_pdu\_role\_n09.question.fex

## Question 71.

✓ Correct

Which network type is most commonly used in Wi-Fi setups?

- ☐ Ad-hoc network
- ☐ Peer-to-peer network
- ☐ Mesh network
- ☒ Infrastructure network

**Explanation**

The infrastructure network type is the most common Wi-Fi setup, where devices connect through an access point. This setup provides a centralized point for data transmission and allows for greater range and connectivity options compared to other types.

Ad-hoc networks are direct connections between devices without an intermediary access point, less common for general Wi-Fi use.

Mesh networks involve multiple nodes that communicate with each other to spread a network over a large area, not the most common setup for individual Wi-Fi networks.

Peer-to-peer networks involve two devices directly communicating without an intermediary, not the standard for Wi-Fi networks.

**References****12.2.1 Infrastructure Network Type**

q\_wireless\_infra\_infrastructure\_network\_n09.question.fex

## Question 72.

✓ Correct

What is a mandatory model in authorization?

- ☐ A model based on the subject's role
- ☐ A model based on the subject's attributes
- ☒ A model where rights are predetermined by system-enforced rules
- ☐ A model where rights are allocated by the system administrator

**Explanation**

The mandatory access control (MAC) model is characterized by access rights and permissions being predetermined by system-enforced rules, typically based on security classifications and clearances.

A model where rights are allocated by the system administrator more closely aligns with discretionary access control (DAC), where the object owner or system administrator can allocate rights.

Role-based access control (RBAC) assigns permissions based on predefined roles within an organization, not on system-enforced rules.

Attribute-based access control (ABAC) uses policies that evaluate attributes of users, resources, and the environment, differing from the mandatory model's system-enforced rules.

**References****10.1.1 Access Control****10.1.2 Authentication Methods****10.2.2 Privileged Access Management****10.2.5 Lab: Manage Account Policies**

q\_access\_control\_mandatory\_model\_n09.question.fex

## Question 73.

✓ Correct

What does a NAT gateway allow an instance to do?

- ☐ Assign a public IP address to every instance within a subnet.
- ☐ Monitor and log all Internet traffic.
- ☐ Encrypt all outbound and inbound communications.
- ☒ Connect out to the Internet without allowing inbound connections.

**Explanation**

A NAT gateway enables instances in a private subnet to initiate outbound connections to the Internet or other AWS services while preventing inbound connections initiated from the Internet. This setup allows for secure Internet access from instances that do not need to be directly accessible from the Internet.

A NAT gateway does not assign public IP addresses to instances; it allows instances with private IP addresses to access the Internet. Public IP addresses are assigned through other means, such as directly or via an Elastic IP.

Monitoring and logging Internet traffic is not the primary function of a NAT gateway. While AWS provides monitoring and logging capabilities, these are managed through other services like CloudWatch and VPC Flow Logs.

A NAT gateway does not inherently encrypt traffic; it facilitates outbound Internet access. Encryption of data in transit is typically managed through other means, such as TLS/SSL or VPN connections.

**References****14.3.3 Cloud Gateways****14.3.4 Cloud Connectivity Options**

q\_net\_virtual\_nat\_gateway\_instance\_n09.question.fex

## Question 74.

✓ Correct

Historically, data centers were designed to use the same architecture as which of the following?

- ☐ A retail network
- ☐ A personal home network
- ☐ A small office network
- ☒ An enterprise campus network

**Explanation**

Historically, data centers used the same three-tiered architecture as an enterprise campus network, consisting of core, distribution, and access layer switches. This design is not similar to small office, personal home, or retail networks.

Small office networks typically have simpler network designs that do not match the complexity of historical data center architectures.

Home networks are far simpler and do not require the scalability and security considerations of data center networks.

Retail networks have different priorities and traffic patterns compared to data centers and enterprise campus networks.

**References****14.1.1 Data Center Network Design**

q\_data\_center\_install\_historic\_enterprise\_campus\_n09.question.fex

## Question 75.

✓ Correct

Which of the following attacks aim to recover the encryption key in WEP and original WPA versions?

- ☐ SQL injection attacks
- ☒ Replay attacks
- ☐ Cross-site scripting attacks
- ☐ Phishing attacks

**Explanation**

Replay attacks involve capturing packets transmitted over the network and retransmitting them, possibly with modifications, to gain unauthorized access or recover the encryption key. Both WEP and the original WPA were vulnerable to such attacks.

Phishing attacks target individuals to deceive them into providing sensitive information and are not directly related to recovering encryption keys in wireless networks.

SQL injection attacks target vulnerabilities in web applications that use SQL databases, not wireless encryption keys.

Cross-site scripting attacks are aimed at web applications to execute malicious scripts in users' browsers, not at recovering wireless encryption keys.

**References****12.3.1 Wi-Fi Encryption Standards**

q\_wireless\_encrypt\_replay\_attack\_description\_n09.question.fex

## Question 76.

✓ Correct

Which security device is typically used to enforce rules between network zones?

- ☒ Firewall
- ☐ Access Point
- ☐ Router
- ☐ Switch

**Explanation**

Firewalls are the primary security devices used to enforce policies and rules between different network zones. They control traffic based on predefined security rules, helping to restrict unauthorized access and protect the network from various threats.

Switches are used for connecting devices within the same network segment and do not typically enforce security rules between zones.

Routers are primarily used for routing traffic between different networks but are not specifically designed to enforce security rules between zones.

Access Points provide wireless connectivity and do not enforce security rules between network zones.

**References****11.1.1 Network Security Zones**

q\_net\_zones\_firewall\_enforce\_rules\_n09.question.fex

## Question 77.

✓ Correct

What is a heat map in the context of a wireless survey?

- ☐ A graphical representation of temperature variations in the area
- ☒ A graphical representation of signal strength across an area
- ☐ A map showing the locations of heating vents in relation to APs
- ☐ A security tool to detect unauthorized access

**Explanation**

In the context of a wireless survey, a heat map is a graphical representation that shows the signal strength within a particular area. It typically uses colors to indicate areas of strong signal (greens and yellows) and areas where signal strength drops off (oranges and reds).

It does not represent temperature variations but signal strength.

The map is not related to heating systems but to wireless signal coverage.

While it involves mapping, it's specifically about wireless signal strength, not security breaches.

**References****12.2.3 Wireless Surveys and Heat Maps**

q\_heat\_maps\_heat\_map\_role\_n09.question.fex



## Question 78.

✓ Correct

What role does a Change Advisory Board (CAB) play in change management?

- ☐ It documents the need for change.
- ☒ It approves major or significant changes.
- ☐ It implements the changes directly.
- ☐ It creates the Request for Change (RFC) documents.

**Explanation**

The Change Advisory Board (CAB) is involved in the approval process for major or significant changes, ensuring that these changes are reviewed at an appropriate level and that they align with the organization's goals and risk tolerance.

The need for change is documented in the RFC, not by the CAB.

The CAB does not implement changes directly; it approves them.

RFC documents are created to propose changes, not by the CAB but by those identifying the need for change.

**References****8.1.3 Change Management**

q\_agreements\_cab\_role\_n09.question.fex

## Question 79.

✓ Correct

A company is upgrading its legacy network infrastructure. The existing network is based on 100BASE-TX Fast Ethernet with a mix of hubs and switches. The IT manager wants to improve network performance while maintaining compatibility with older devices that only support 10 Mbps Ethernet interfaces.

What feature should the IT manager ensure the new network devices support to maintain compatibility with older devices?

- ☐ Use of hubs instead of switches
- ☒ Autonegotiation
- ☐ Full-duplex transmissions
- ☐ Higher frequency signaling

**Explanation**







Autonegotiation allows devices to automatically select the highest supported connection parameters, including speed (10 or 100 Mbps) and mode (half or full duplex), ensuring compatibility between devices with different Ethernet capabilities. This feature is crucial for maintaining compatibility with older devices that only support 10 Mbps Ethernet interfaces.

While full-duplex transmissions improve network performance, they do not directly address compatibility with older devices.

Higher frequency signaling is a characteristic of Fast Ethernet but does not specifically ensure compatibility with older devices.

Using hubs would not improve network performance and does not address the compatibility issue. Switches are preferred for their ability to manage collision domains and support full-duplex transmissions.

**References**

-  **2.1.2 Ethernet Standards**
-  **2.1.3 Media Access Control and Collision Domains**
-  **2.1.4 100BASE-TX Fast Ethernet Standards**
-  **2.1.5 Gigabit Ethernet Standards**
-  **2.1.6 Fiber Ethernet Standards**
-  **2.1.8 Lab: Reconnect to an Ethernet Network**



## **2.2.7 Lab: Connect to an Ethernet Network**



## **3.1.2 Modular Transceivers**



## **3.1.5 Ethernet Frame Format**

q\_fast\_autonegotiation\_scenario\_n09.question.fex

## Question 80.

✓ Correct

Which type of firewall can store connection states and use rules to allow established or related traffic?

- ☒ Stateful packet filtering firewall
- ☐ Application layer firewall
- ☐ Web application firewall (WAF)
- ☐ Network layer firewall

**Explanation**










Stateful packet filtering firewalls can track the state of active connections and make decisions based on the context of the traffic, such as allowing packets that are part of an established session. This requires maintaining a state table, which involves more processing power.

Web application firewalls (WAFs) focus on monitoring and blocking HTTP/S traffic to and from a web application, not on connection states.

Network layer firewalls primarily deal with packet filtering based on IP addresses and ports, not connection states.

Application layer firewalls inspect the data within application protocols, not the state of connections.

**References**

-  **1.3.5 Transport and Application Layer and Security Functions**
-  **5.4.1 Firewall Uses and Types**
-  **5.4.2 Firewall Selection and Placement**
-  **10.5.1 Security Rules and ACL Configuration**
-  **10.5.4 Misconfigured Firewall and ACL Issues**
-  **10.5.5 Creating Firewall ACLs**
-  **10.5.7 Lab: Configure a Security Appliance**
-  **10.5.8 Lab: Configure a Perimeter Firewall**
-  **14.3.5 Cloud Firewall Security**

q\_cloud\_firewall\_stateful\_packet\_filtering\_n09.question.fex

## Question 81.

✓ Correct

What is the function of a Customer Edge (CE) router in a WAN?

- ☒ To connect the customer's network to the provider's network
- ☐ To modulate and demodulate signals
- ☐ To increase the bandwidth of the WAN
- ☐ To provide firewall services exclusively

**Explanation**











A Customer Edge (CE) router serves as the interface between the customer's internal network and the service provider's network, facilitating the exchange of data between them.

While a CE router can provide firewall services, its primary function is not limited to security but includes connecting networks.

The primary function of a CE router is to connect networks, not to inherently increase the bandwidth of the WAN. Bandwidth is determined by the service level agreement with the provider and the technology used.

Modulation and demodulation of signals are functions of modems, not routers. Routers, including CE routers, are concerned with directing data packets between networks.

**References**

-  **1.2.1 Open Systems Interconnection Model**
-  **1.2.5 Layer 3 - Network**
-  **1.2.8 OSI Model Summary**
-  **1.3.4 Network Layer Functions**
-  **1.3.6 The Internet**
-  **1.3.7 Binary and Hexadecimal**
-  **1.3.8 Lab: Explore a Single Location in a Lab**
-  **4.1.2 Layer 2 vs. Layer 3 Addressing and Forwarding**
-  **13.1.1 Wide Area Networks and the OSI Model**
-  **14.3.5 Cloud Firewall Security**

q\_wan\_ce\_router\_n09.question.fex

## Question 82.

✓ Correct

What is the primary benefit of a highly elastic cloud system?

- ☒ It can adjust resources in real-time to meet demand.
- ☐ It allows for unlimited storage capacity.
- ☐ It can operate without internet connectivity.
- ☐ It ensures data is automatically backed up.

**Explanation**

The primary benefit of a highly elastic cloud system is its ability to automatically scale resources up or down in real-time as demand changes. This ensures that the system can handle sudden spikes in usage without performance degradation and can also reduce operational costs by deprovisioning resources when demand is low.

Internet connectivity is a requirement for accessing cloud services; elasticity does not change this.

Automatic data backup is an important feature of cloud services but is not directly related to elasticity.

While cloud systems offer scalable storage, elasticity specifically refers to the real-time adjustment of resources, not the provision of unlimited capacity.

**References****14.2.1 Cloud Scalability and Elasticity**

q\_cloud\_scale\_elasticity\_benefit\_n09.question.fex

## Question 83.

✓ Correct

What is a master image in the context of infrastructure as code?

- ☐ A dynamic inventory system
- ☐ A basic template for virtual environments
- ☒ A "gold" copy of a VM or container instance
- ☐ A backup copy of data

**Explanation**

A master image is the "gold" copy of a VM or container instance, with the OS, applications, and patches all installed and configured. It serves as a ready-to-deploy snapshot of a system's desired state.

A backup copy of data refers to data storage practices, not provisioning instances.

Templates are different, as they contain build instructions rather than being a complete, ready-to-use image.

A dynamic inventory system relates to tracking cloud instances, not creating them.

**References****14.4.2 Uses for Infrastructure as Code**

q\_automation\_master\_image\_description\_n09.question.fex



## Question 84.

✓ Correct

A small office/home office (SOHO) network is configured to use the private IP address range of 192.168.1.0/24.

If you are setting up a SOHO router for this network, which of the following IP addresses would be the MOST appropriate for the router?

- ☒ 192.168.1.1
- ☐ 203.0.113.1
- ☐ 192.168.1.255
- ☐ 192.168.2.1

**Explanation**












192.168.1.1 is the correct answer. This IP address is within the specified private IP address range of 192.168.1.0/24 and is commonly used as the default gateway address for devices on the network. It is a suitable choice for the router's IP address, allowing it to manage traffic between the local network and the Internet.

The 192.168.2.1 IP address is not within the specified private IP address range of 192.168.1.0/24. It belongs to a different subnet (192.168.2.0/24), which means it cannot be used for a router within the 192.168.1.0/24 network.

The 192.168.1.255 IP address is the broadcast address for the 192.168.1.0/24 network. It is reserved for broadcasting messages to all hosts within the network and cannot be assigned to any single device, including the router.

The 203.0.113.1 IP address is a public IP address and would not be used for a router within a private network using the 192.168.1.0/24 range. Public IP addresses are used on the WAN (Wide Area Network) side of a router for communication over the Internet, not for internal network addressing.

**References****1.3.1 SOHO Routers****1.3.2 Physical Layer Functions****1.3.3 Data Link Layer Functions****1.3.4 Network Layer Functions****1.3.5 Transport and Application Layer and Security Functions**

-  **1.3.6 The Internet**
  -  **1.3.9 Lab: Create a Home Wireless Network**
  -  **1.3.10 Lab: Create a SOHO Network**
  -  **5.1.1 Routing Tables and Path Selection**
  -  **5.1.4 Packet Forwarding**
  -  **5.1.5 Fragmentation**
  -  **5.1.6 Router Configuration**
  -  **5.1.9 Lab: Install an Enterprise Router**
  -  **10.5.9 Lab: Restrict Telnet and SSH Access**
  -  **10.5.10 Lab: Permit Traffic**
  -  **10.5.11 Lab: Block Source Hosts**
- q\_network\_functions\_router\_address\_n09.question.fex

## Question 85.

✓ Correct

What does an IP scanner do?

- ☐ Edits images
- ☒ Establishes the logical topology of the network
- ☐ Creates spreadsheets
- ☐ Encrypts network traffic

**Explanation**

An IP scanner is used for host discovery, helping to map out the network's logical structure in terms of subnets and routers, aiding in network management and security.

Editing images is a function of software like Adobe Photoshop, not an IP scanner.

Creating spreadsheets is a function of applications like Microsoft Excel.

Encrypting network traffic is related to security protocols, not the function of an IP scanner.

**References****8.2.1 Network Discovery**

q\_ip\_scanner\_logical\_topology\_n09.question.fex

## Question 86.

✓ Correct

What distinguishes a collision domain from a broadcast domain?

- ☒ Collision domains are about physically shared media, and their borders are established by bridges and switches.
- ☐ Broadcast domains require a layer 2 broadcast address to be established.
- ☐ Collision domains can span multiple routers, while broadcast domains are limited to a single switch.
- ☐ Collision domains are established by routers, while broadcast domains are established by switches.

**Explanation**








Collision domains refer to network segments where data packets can collide due to shared media access. Bridges and switches segment networks into separate collision domains by providing dedicated paths for data packets, thus reducing collisions. Broadcast domains, on the other hand, are defined by routers at layer 3 and determine the reach of broadcast traffic within a network.

Collision domains are not established by routers; they are segmented by bridges and switches. Broadcast domains are defined by routers, not switches.

While broadcast domains involve layer 3 devices and protocols, the requirement for a layer 2 broadcast address is not what distinguishes them from collision domains.

Collision domains are segmented by bridges and switches, not routers, and do not span multiple routers. Broadcast domains can span multiple switches and are limited by routers.

**References**

-  **1.3.3 Data Link Layer Functions**
-  **3.2.1 Hubs**
-  **3.2.3 Switches**
-  **3.2.4 Ethernet Switch Types**
-  **3.2.5 Switch Interface Configuration**
-  **3.2.7 Lab: Install a Switch in the Rack**
-  **3.2.8 Lab: Secure a Switch**

q\_bridges\_collision\_vs\_broadcast\_n09.question.fex

## Question 87.

✓ Correct

At which layer of the OSI model does TLS primarily operate?

- ☒ Session Layer
- ☐ Transport Layer
- ☐ Network Layer
- ☐ Application Layer

**Explanation**





TLS operates at the Session layer of the OSI model, which is responsible for establishing, managing, and terminating connections between applications. By functioning at this layer, TLS provides a secure channel for communication between client and server applications.

The Network layer is responsible for logical addressing and routing, not for securing communications.

Despite its name, TLS operates above the Transport layer, at the Session layer, providing security for the sessions between applications.

The Application layer is where end-user processes communicate. While TLS secures these communications, it operates at the Session layer to do so.

**References**

-  **1.2.1 Open Systems Interconnection Model**
-  **1.2.7 Upper Layers**
-  **1.2.8 OSI Model Summary**
-  **1.3.8 Lab: Explore a Single Location in a Lab**

q\_tls\_osi\_layer\_n09.question.fex

## Question 88.

✓ Correct

What is one solution to mitigate the risk of rogue access points?

- ☐ Decreasing the signal strength of the legitimate access points
- ☒ Using EAP-TLS security for mutual authentication
- ☐ Disabling the network's SSID broadcast
- ☐ Increasing the network's bandwidth

**Explanation**

The correct answer is to use EAP-TLS security for mutual authentication. EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) is a security protocol that provides mutual authentication between the client and the authentication server. By ensuring that both parties authenticate each other, it can mitigate the risk of rogue access points by preventing unauthorized devices from masquerading as legitimate access points.

Disabling the network's SSID broadcast does not prevent unauthorized access points from connecting to the network; it only makes the network name (SSID) invisible to casual observers.

Increasing the network's bandwidth relates to the capacity of the network to transmit data and does not address the security risks posed by rogue access points.

Decreasing the signal strength of legitimate access points could negatively impact network performance for legitimate users without effectively mitigating the risk of rogue access points.

**References****12.3.6 Wireless Network Attacks**

q\_wifi\_atck\_eap-tls\_security\_n09.question.fex

## Question 89.

✓ Correct

Why is Telnet considered to be insecure?

- ☒ It transmits data in plain text.
- ☐ It can only transmit text, not binary files.
- ☐ It uses strong encryption for all communications.
- ☐ It automatically blocks access to port 23.

**Explanation**

Telnet is considered insecure because it transmits all data, including passwords, in plain text. This makes it vulnerable to interception by packet sniffing, where an attacker can easily read the transmitted information.

Telnet does not encrypt its communications at all, which is the primary reason for its insecurity.

The security concerns with Telnet are not related to its ability to transmit text or binary files but to its lack of encryption.

Telnet uses port 23 by default and does not block it. The recommendation is for administrators to block access to port 23 to prevent unauthorized Telnet access.

**References**

**6.1.6 Common TCP and UDP Ports**



**13.3.3 Telnet**

q\_telnet\_insecure\_n09.question.fex

## Question 90.

✓ Correct

What is the advantage of connecting servers to multiple leaf switches in a spine and leaf topology?

- ☐ It allows for direct server-to-server communication.
- ☐ It reduces the cost of the network infrastructure.
- ☒ It provides multipath redundancy.
- ☐ It decreases network latency.

**Explanation**

Connecting servers to multiple leaf switches offers multipath redundancy, ensuring that if one path fails, another can take over, maintaining network reliability and uptime.

The primary advantage is not cost reduction but enhancing network reliability and redundancy.

Direct server-to-server communication is facilitated by the overall topology, not specifically by connecting to multiple leaf switches.

While network latency can be more predictable due to the topology's design, the specific advantage of connecting to multiple leaf switches is to provide redundancy.

**References****14.1.2 Spine and Leaf Topology**

q\_spine\_multiple\_leaf\_switches\_n09.question.fex



## Question 91.

✓ Correct

How is a connection uniquely identified in a TCP/IP network?

- ☐ By the client port and IP address only
- ☒ By the combination of server port and IP address and client port and IP address
- ☐ By the MAC addresses of the communicating devices
- ☐ By the server port and IP address only

**Explanation**

A connection in a TCP/IP network is uniquely identified by the combination of both the server's and client's port numbers and IP addresses, ensuring precise identification of each end of the connection.

By the server port and IP address only or the client port and IP address only are incorrect because both the server and client port and IP addresses are needed to uniquely identify a connection.

MAC addresses identify devices at the Data Link layer, not connections at the Transport layer.

**References**

**6.1.2 Transmission Control Protocol**



**6.1.3 TCP Handshake and Teardown**



**6.1.7 Lab: Explore Three-Way Handshake in Wireshark**

q\_transport\_connection\_identification\_n09.question.fex

## Question 92.

✓ Correct

What is a common implementation of remote network access today?

- ☐ Direct cabled connections
- ☐ Analog modems
- ☐ Physical token exchange
- ☒ Virtual Private Network (VPN)

**Explanation**

VPNs are a common method for implementing remote network access today, allowing secure connections over the Internet by encrypting the data exchanged.

Analog modems are largely outdated for remote access.

Direct cabled connections do not constitute remote access.

Physical token exchange is not a method of remote network access.

**References**

**13.2.2 Tunneling Protocols**



**13.2.8 Lab: Configure a Remote Access VPN**



**13.2.9 Lab: Configure an iPad VPN Connection**



**13.2.10 Lab: Configure a RADIUS Solution**

q\_remote\_access\_vpn\_application\_n09.question.fex

## Question 93.

× Incorrect

What feature does version 2 of HTTP add to enhance its functionality?

- ☒ Increased encryption
- ☐ Faster email transmission
- ☐ Improved FTP support
- ☐ More state-preserving features

**Explanation**

The correct answer is more state-preserving features. HTTP/2 introduces enhancements that allow for more efficient state preservation, improving performance and user experience.

Encryption improvements are more associated with HTTPS rather than a specific version of HTTP.

HTTP/2's improvements do not specifically target email transmission speeds.

HTTP/2 focuses on web traffic, not FTP.

**References****6.1.6 Common TCP and UDP Ports****7.2.1 Hyper Text Transfer Protocol**

q\_http\_state\_preserving\_n09.question.fex

## Question 94.

✓ Correct

You often travel away from the office. While traveling, you would like to use a modem on your laptop computer to connect directly to a server in your office to access needed files.

You want the connection to be as secure as possible. Which type of connection do you need?

- ☐ Internet
- ☒ Remote access
- ☐ Intranet
- ☐ Virtual private network

**Explanation**

Remote access is the correct answer because it specifically refers to the ability to access a computer or a network from a remote location. In the context of the question, using a modem to connect directly to a server in the office for accessing files aligns with the definition of remote access. This type of connection can be secured through various means, such as using secure authentication methods and encryption, to ensure that the data transmitted between the laptop and the office server remains confidential and protected from unauthorized access.

Internet is incorrect because the Internet is a global network that connects millions of private, public, academic, business, and government networks. It is not a specific type of connection for securely accessing files on an office server. While the Internet can be used as the medium over which remote access occurs, by itself, it does not provide the direct and secure connection to an office server that the question implies.

Although a VPN is a technology that creates a secure, encrypted connection over a less secure network, such as the Internet, and could technically be used for the scenario described, it is not the correct answer based on the provided options. The question specifies using a modem to connect directly to a server, which suggests a direct remote access method rather than connecting through a VPN. However, it's important to note that in practice, a VPN is often the preferred method for securely accessing files from a remote location due to its encryption capabilities and ability to secure data transmissions.

An intranet is a private network accessible only to an organization's staff. It is incorrect in this context because the question involves an individual traveling away from the office and needing to access office files remotely. An intranet is typically used within the confines of an organization's physical locations and is not designed for external access without additional configurations or technologies, such as VPN, to securely access the network from outside the organization's premises.

**References****13.2.2 Tunneling Protocols****13.2.8 Lab: Configure a Remote Access VPN****13.2.9 Lab: Configure an iPad VPN Connection****13.2.10 Lab: Configure a RADIUS Solution**

q\_remote\_access\_example\_traveling\_n09.question.fex

## Question 95.

✓ Correct

What is a significant challenge in securing east-west traffic in data centers?

- ☐ The lack of need for security
- ☒ The creation of a severe bottleneck if each transaction passed through a firewall
- ☐ The absence of virtualized security appliances
- ☐ The elimination of north-south traffic

**Explanation**

Securing east-west traffic is challenging because if each server-to-server transaction were to pass through a firewall or other security appliance, it would create a severe bottleneck. This challenge does not stem from a lack of security need, the absence of virtualized security appliances, or the elimination of north-south traffic.

Security is a critical concern for all data center traffic, including east-west.

Virtualized security appliances are increasingly used to address the very challenge of securing east-west traffic without creating bottlenecks.

North-south traffic remains important, and its security is also a concern, but it does not directly relate to the challenge of securing east-west traffic.

**References****14.1.1 Data Center Network Design**

q\_data\_center\_install\_east-west\_challenge\_n09.question.fex

## Question 96.

✓ Correct

At the Network layer, what are IP source and destination addresses used to do?

- ☐ Monitor network traffic and data usage
- ☒ Forward packets to the proper destination
- ☐ Assign specific functions to devices within the network
- ☐ Control access to the network based on device types

**Explanation**

IP source and destination addresses are crucial at the Network layer for routing and forwarding packets to the correct destination. These addresses allow network devices, such as routers, to make decisions about where to send packets next on their journey across the network to reach the intended recipient.

IP addresses are not used to control network access based on device types. Network access control (NAC) systems or other security mechanisms typically handle access control, not IP addressing.

IP addresses identify devices on a network but do not assign functions to those devices. The role or function of a device within a network is determined by its configuration and the services it provides, not its IP address.

IP addresses themselves are not tools for monitoring. While IP addresses can be part of monitoring data to identify sources and destinations of traffic, the actual monitoring of network traffic and data usage is performed by network monitoring tools and software, not by the IP addressing system itself.

**References****4.2.1 IPv4 Address Format**

q\_ipv4\_network\_layer\_n09.question.fex

## Question 97.

✓ Correct

What happens if a Windows host does not receive a response from a DHCP server within a given time frame?

- ☒ It will select an address at random from the APIPA range.
- ☐ It will prompt the user to manually enter an IP address.
- ☐ It will broadcast a request for manual configuration assistance.
- ☐ It will shut down to prevent network conflicts.

**Explanation**

If a Windows host does not receive a DHCP offer within a certain time frame, it will automatically select an IP address from the APIPA range (169.254.1.1 to 169.254.254.254). This allows the host to continue communicating on the local network despite the absence of DHCP server communication.

The host does not shut down; it seeks an alternative method to configure its IP address.

While users can manually enter an IP address, this is not the automatic response when a DHCP server cannot be contacted.

The host does not broadcast for manual configuration assistance; it automatically selects an APIPA address.

**References****4.5.5 IPv6 Link Local Addressing****6.3.1 Automatic Private IP Addressing****6.3.4 Lab: Explore APIPA Addressing****6.3.5 Lab: Explore APIPA Addressing in Network Modeler****6.3.6 Set Up Alternate Addressing**

q\_apipa\_dhcp\_response\_n09.question.fex



## Question 98.

✓ Correct

What is a primary reason for an organization to choose one termination standard (T568A or T568B) over the other and stick with it?

- ☒ To avoid compatibility and connectivity issues between devices
- ☐ To ensure that all cables are the same color
- ☐ To reduce the cost of Ethernet cables
- ☐ To comply with international laws requiring the use of a single standard

**Explanation**

Choosing and consistently using one termination standard within an organization helps avoid compatibility and connectivity issues. Since T568A and T568B have different wiring configurations, mixing them without proper planning can lead to failed connections or network issues. Consistency ensures that all network components are compatible and can communicate effectively.

The choice between T568A and T568B does not affect the color of the cables themselves; it pertains to the wiring configuration within the connectors. Thus, this reason is not relevant to the choice between these standards.

There are no international laws that mandate the exclusive use of either T568A or T568B. The choice between these standards is typically based on organizational policy, regional preferences, or specific project requirements, not legal obligations.

The cost of Ethernet cables is not directly affected by the choice between T568A and T568B standards. Both configurations use the same types of materials and manufacturing processes, so the cost difference, if any, would be negligible and not a primary factor in choosing one standard over the other.

**References****2.3.2 T568A and T568B Termination Standards**

q\_t568a\_t568a\_and\_t568b\_mix\_n09.question.fex

## Question 99.

✓ Correct

What is the primary purpose of link aggregation/NIC teaming?

- ☐ To replace wireless connections with wired connections
- ☐ To increase the cost of network infrastructure
- ☒ To combine multiple network connections into a single logical connection
- ☐ To decrease the network speed

**Explanation**

The correct answer is to combine multiple network connections into a single logical connection. Link aggregation, also known as NIC teaming, is the process of combining two or more network connections into a single logical connection to increase bandwidth and provide redundancy.

Link aggregation/NIC teaming is used to increase the network speed by combining multiple network connections, not to decrease it.

The purpose of link aggregation/NIC teaming is to combine multiple wired network connections for increased bandwidth and redundancy, not to replace wireless connections with wired ones.

While implementing link aggregation/NIC teaming might involve some initial costs for additional hardware, its primary purpose is to enhance network performance and reliability, not to increase overall infrastructure costs.

**References****3.3.1 Link Aggregation and NIC Teaming****3.3.6 Lab: Configure Port Aggregation**

q\_lag\_primary\_purpose\_n09.question.fex

## Question 100.

✓ Correct

Why is Infrastructure as Code important for cloud technologies?

- ☐ It simplifies the physical maintenance of cloud servers.
- ☒ It encourages the use of scripted approaches to provisioning.
- ☐ It reduces the bandwidth required for cloud services.
- ☐ It enables manual configurations to be more reliable.

**Explanation**

IaC is crucial for cloud technologies because it leverages scripted, automated approaches for provisioning and managing cloud resources. This ensures faster, more reliable, and consistent deployments compared to manual configurations.

IaC deals with virtual rather than physical aspects of cloud servers.

IaC aims to replace manual configurations with automation for reliability.

IaC's importance lies in automation and efficiency, not in reducing bandwidth usage.

**References****14.4.1 Infrastructure as Code**

q\_iac\_cloud\_technology\_n09.question.fex

## Question 101.

✓ Correct

What method does IEEE 802.11 use to cope with contention?

- ☐ Time Division Multiple Access (TDMA)
- ☐ Code Division Multiple Access (CDMA)
- ☐ Frequency Division Multiple Access (FDMA)
- ☒ Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

**Explanation**





IEEE 802.11 uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to manage contention. This method allows devices to avoid collisions by checking the channel before transmitting and using acknowledgments and retransmissions to ensure successful communication.

TDMA is a method that divides the channel into different time slots, not used in IEEE 802.11.

FDMA divides the frequency band into multiple channels, which is not the contention method used in IEEE 802.11.

CDMA allows multiple signals to occupy the same channel simultaneously, which is different from the collision avoidance strategy of CSMA/CA.

**References**

-  **12.1.1 IEEE 802.11 Wireless Standards**
-  **12.1.2 IEEE 802.11a and 5GHz Channel Bandwidth**
-  **12.1.4 IEEE 802.11n, MIMO, and Channel Bonding**
-  **12.1.6 Multiuser MIMO and Band Steering**

q\_wireless\_contention\_n09.question.fex

## Question 102.

✓ Correct

Your organization is planning to host a conference at its headquarters, expecting a large number of guests who will require internet access. To accommodate this, you need to decide which network security zone to connect the guests' devices to.

Which of the following zones would be MOST appropriate for this purpose?

- ☐ Private client network
- ☐ Public server network
- ☒ Guest
- ☐ Private server administrative networks

**Explanation**

The correct answer is Guest. The guest zone is specifically designed to accommodate unmanaged devices, providing them with internet access while imposing certain restrictions and monitoring to maintain network security. This zone is typically untrusted, meaning it is isolated from the organization's critical internal resources to prevent unauthorized access. Connecting guests to this zone ensures that they have the access they need without compromising the security of the organization's more sensitive or critical network zones.

Private server administrative networks are highly secure zones intended for critical servers and infrastructure, subject to strict security policies and continuous monitoring. Allowing guest access to this zone would pose a significant security risk.

The private client network is designed for devices that require access to both the organization's internal resources and public networks. While it has security policies and monitoring in place, it is meant for trusted devices and not suitable for unmanaged guest devices.

The public server network is for devices that are fully managed by the organization but accept connections from unmanaged public clients. It is not intended to provide general internet access to guests and could expose critical services to unnecessary risk.

**References****12.3.5 Bring Your Own Device Issues****12.3.8 Lab: Create a Guest Network for BYOD**

q\_net\_zones\_guest\_scenario\_n09.question.fex

## Question 103.

✓ Correct

What role does the access point (AP) play in enterprise authentication?

- ☐ It generates the master key (MK).
- ☐ It serves as the authentication server.
- ☒ It forwards authentication data to an AAA server.
- ☐ It directly authenticates user credentials.

**Explanation**

In enterprise authentication, the access point acts as an intermediary that forwards the credentials of the supplicant (wireless client) to an AAA (Authentication, Authorization, and Accounting) server for validation. This process ensures that the authentication data is securely handled and validated by a dedicated server.

The master key (MK) is transmitted by the AAA server to the supplicant, not generated by the AP.

The AP does not serve as the authentication server; this role is fulfilled by the AAA server.

The AP does not directly authenticate user credentials; it forwards them to the AAA server for authentication.

**References****12.2.8 Lab: Design an Indoor Wireless Network****12.2.9 Lab: Design an Outdoor Wireless Network****12.2.10 Lab: Implement an Enterprise Wireless Network****12.3.10 Lab: Secure a Home Wireless Network**

q\_wifi\_ent\_ap\_role\_n09.question.fex

## Question 104.

✓ Correct

What is the role of the Gateway/next hop parameter in a routing table?

- ☐ It specifies the final destination of the packet.
- ☐ It identifies the router's physical location.
- ☐ It determines the speed at which the packet is forwarded.
- ☒ It indicates the next router or gateway along the path to the destination.

**Explanation**

The Gateway/next hop parameter is crucial for indicating the immediate next stop (router or gateway) a packet should be forwarded to on its journey towards the final destination. It helps in making hop-by-hop decisions to efficiently route the packet.

The final destination of the packet is determined by the Destination parameter, not the Gateway/next hop, which only indicates the next immediate stop.

The Gateway/next hop parameter does not provide information about the physical location of routers; it simply points to the next device in the path.

The forwarding speed of packets is influenced by the network's bandwidth and the router's processing capabilities, not the Gateway/next hop parameter.

**References****1.3.1 SOHO Routers****1.3.2 Physical Layer Functions****1.3.3 Data Link Layer Functions****1.3.4 Network Layer Functions****1.3.5 Transport and Application Layer and Security Functions****1.3.6 The Internet****1.3.9 Lab: Create a Home Wireless Network****1.3.10 Lab: Create a SOHO Network****5.1.1 Routing Tables and Path Selection****5.1.4 Packet Forwarding****5.1.5 Fragmentation**



### **5.1.6 Router Configuration**



### **5.1.9 Lab: Install an Enterprise Router**



### **10.5.9 Lab: Restrict Telnet and SSH Access**



### **10.5.10 Lab: Permit Traffic**



### **10.5.11 Lab: Block Source Hosts**

q\_route\_table\_gateway\_parameter\_n09.question.fex



## Question 105.

✓ Correct

What is an implicit deny in firewall configuration?

- ☐ A rule that explicitly allows all traffic
- ☒ A default behavior to block traffic that does not match any rule
- ☐ A rule that only denies traffic from specific countries
- ☐ A temporary rule that denies access during peak hours

**Explanation**










The implicit deny principle is a fundamental security measure in firewall configurations. It ensures that any traffic not explicitly allowed by the defined rules is automatically denied. This default blocking stance helps prevent unauthorized access by ensuring that only traffic that has been explicitly permitted can pass through the firewall.

A rule that explicitly allows all traffic is the opposite of implicit deny, as it would permit all traffic by default, which is not secure.

Implicit deny is not a temporary measure nor is it based on time-of-day conditions; it is a constant default behavior.

Implicit deny applies to all traffic that does not match any rule, not just traffic from specific geographic locations.

**References**

-  **1.3.5 Transport and Application Layer and Security Functions**
-  **5.4.1 Firewall Uses and Types**
-  **5.4.2 Firewall Selection and Placement**
-  **10.5.1 Security Rules and ACL Configuration**
-  **10.5.4 Misconfigured Firewall and ACL Issues**
-  **10.5.5 Creating Firewall ACLs**
-  **10.5.7 Lab: Configure a Security Appliance**
-  **10.5.8 Lab: Configure a Perimeter Firewall**
-  **14.3.5 Cloud Firewall Security**

q\_acl\_implicit\_deny\_n09.question.fex

Question 106.

✓ Correct

What is the role of a modem in a WAN?

- ☒ To perform modulation and demodulation of data
- ☐ To serve as a firewall and provide security
- ☐ To connect multiple LANs within an organization
- ☐ To increase the speed of the internet connection

### Explanation







Modems modulate digital signals from a computer into analog signals for transmission over telephone lines or other media and demodulate incoming analog signals back into digital form.

The primary function of a modem is not to increase internet speed but to convert signals for transmission over different types of media.

Connecting multiple LANs is typically the role of routers or switches, not modems.

While some modems may have built-in security features, their primary role is not to serve as a firewall.

### References

-  **1.2.1 Open Systems Interconnection Model**
-  **1.2.3 Layer 1 - Physical**
-  **1.2.8 OSI Model Summary**
-  **1.3.2 Physical Layer Functions**
-  **1.3.8 Lab: Explore a Single Location in a Lab**
-  **13.1.1 Wide Area Networks and the OSI Model**

q\_wan\_modem\_role\_n09.question.fex

## Question 107.

✓ Correct

What is the primary purpose of using the **show mac address-table** command in troubleshooting network issues?

- ☐ To display the routing table of a switch
- ☐ To reset the MAC address table on the switch
- ☒ To identify the MAC addresses associated with a particular switch port
- ☐ To list the IP addresses assigned to all devices on the network

**Explanation**

The **show mac address-table** command is used to display the MAC address table of a switch, which includes the MAC addresses learned by each port. This is particularly useful in troubleshooting to identify which devices (via their MAC addresses) are connected to which ports on the switch. This can help in isolating issues to specific devices or segments of the network.

The routing table, which contains information about network paths and destinations, is typically viewed with commands like **show ip route** in routers or Layer 3 switches. The **show mac address-table** command specifically displays the MAC address table, not the routing table.

The **show mac address-table** command displays MAC addresses, not IP addresses. To view IP addresses, you would typically look at the DHCP server's lease table or use a command like **show ip arp** on a router or Layer 3 switch to see the IP-to-MAC address mappings.

The **show mac address-table** command is used for viewing the current state of the MAC address table and does not perform any actions such as resetting the table. Resetting or clearing the MAC address table would involve a different command, such as **clear mac address-table dynamic**.

**References****3.4.3 Switch Show Commands****3.4.5 MAC Address Table****3.4.8 Lab: Troubleshoot Disabled Ports**

q\_mac\_table\_show\_mac\_purpose\_n09.question.fex

## Question 108.

✓ Correct

What makes TACACS+ different from RADIUS?

- ☐ TACACS+ uses UDP for communication.
- ☒ TACACS+ separates AAA functions.
- ☐ TACACS+ combines AAA in a single process.
- ☐ TACACS+ is less secure than RADIUS.

**Explanation**

TACACS+ provides more flexibility and security by separating the authentication, authorization, and accounting (AAA) functions, allowing for more granular control and auditing capabilities.

TACACS+ uses TCP, not UDP, for communication.

TACACS+ specifically separates the AAA functions, unlike RADIUS.

TACACS+ is designed to offer more security features, not less.

**References****10.1.8 Remote Authentication****10.3.4 Scanning for Unsecure Protocols****12.3.3 Enterprise Authentication****13.2.1 Remote Access Considerations****13.2.10 Lab: Configure a RADIUS Solution**

q\_remote\_access\_tacacs\_vs\_radius\_n09.question.fex

## Question 109.

✓ Correct

What distinguishes an external threat actor from an internal threat actor?

- ☐ The type of malware they use
- ☐ The geographical location of the actor
- ☒ Whether they have authorized access to the system
- ☐ The sophistication of the attack

**Explanation**






The key difference between external and internal threat actors is whether they have authorized access to the target system. External threat actors do not have such access and must find ways to infiltrate the system, often using malware or social engineering. In contrast, internal threat actors already have some level of authorized access due to their role within or relationship to the organization.

The type of malware used can vary among all threat actors and does not define whether they are internal or external.

The geographical location of the actor is irrelevant to their classification as internal or external.

The sophistication of the attack can vary widely among both internal and external actors and is not a distinguishing factor.

**References**

-  **9.1.1 Common Security Terminology**
  -  **9.1.5 Vulnerability and Exploit Types**
  -  **9.2.1 Threat Types and Assessment**
  -  **9.3.5 Using SMAC to Spoof MAC Addresses**
  -  **9.3.8 Lab: Spoof MAC Addresses with SMAC**
- q\_threat\_types\_external\_vs\_internal\_n09.question.fex

## Question 110.

✓ Correct

What is Electromagnetic Interference (EMI) and how can it be detected?

- ☐ EMI is a type of signal boost provided by certain appliances, detectable through standard Wi-Fi analysis.
- ☐ EMI is interference from devices working in different frequency bands and can be ignored.
- ☒ EMI is interference from a powerful source in the same frequency band.
- ☐ EMI is an enhancement of the Wi-Fi signal that can be detected with a Wi-Fi adapter.

**Explanation**

Electromagnetic Interference (EMI) occurs when a powerful radio or electromagnetic source operating in the same frequency band as the Wi-Fi network introduces noise or interference. It can be detected using a spectrum analyzer, a device equipped with a special radio receiver that can identify and locate the source of interference.

EMI does not enhance Wi-Fi signals; it interferes with them. Wi-Fi adapters are not suitable for detecting EMI since they filter out non-Wi-Fi signals.

EMI is specifically interference from sources working in the same frequency band, not different ones, and it cannot be simply ignored as it affects network performance.

EMI is not a signal boost but interference, and it requires a spectrum analyzer for detection, not standard Wi-Fi analysis tools.

**References****12.4.3 Channel Overlap Issues****12.4.4 Interference Issues****12.4.7 Lab: Explore Wireless Network Problems****12.4.9 Lab: Optimize a Wireless Network**

q\_interference\_emi\_role\_n09.question.fex

## Question 111.

✓ Correct

Your company has recently expanded its operations and opened a new branch office. As the IT manager, you are tasked with setting up the network infrastructure for this new location. The office will connect to the company's main data center via the Internet for access to centralized resources.

You need to select a router that will manage the traffic between the branch office's local area network (LAN) and the wide area network (WAN) internet access efficiently.

Which type of router would be most suitable for this purpose?

- ☐ Wireless router
- ☒ Edge router
- ☐ Virtual router
- ☐ Core router

**Explanation**

An edge router is the most suitable choice for managing traffic between a branch office's LAN and the WAN internet access. It is specifically designed to serve as the boundary between internal networks and external networks, handling data entering and exiting the network. This makes it ideal for connecting the branch office to the company's main data center over the internet.

Core routers are used within the backbone of the Internet or within large enterprise networks to route traffic within the network core. They are not designed for direct connection to external networks, making them less suitable for the described scenario.

While a wireless router provides Wi-Fi connectivity, its primary function is not to manage traffic between a LAN and WAN. In a business environment, especially for connecting a branch office to a main data center, a more robust solution like an edge router is needed.

Virtual routers can be used in various scenarios, including as part of a virtualized network infrastructure. However, for the specific task of managing traffic between a branch office's LAN and the WAN with a physical connection, a physical edge router is more appropriate. Virtual routers are more suited for environments where routing capabilities need to be dynamically adjusted or where physical space and hardware are limited.

**References****5.3.1 Edge Routers**

q\_edge\_route\_example\_scenario\_n09.question.fex

Question 112.

✓ Correct

How do CDN servers ensure that the content they deliver is current?

- ☐ By deleting outdated content
- ☐ By only serving static content that doesn't change
- ☒ By replicating content to remain current with each other
- ☐ By requiring manual updates from the content owner

### Explanation

CDN servers replicate content among themselves to ensure that all nodes in the network have the latest version of the content. This replication process helps in maintaining consistency and delivering up-to-date content to users.

Simply deleting outdated content does not ensure that the remaining content is current. The key is the replication process among CDN servers.

While content owners may update their content, CDN servers automatically replicate these updates across the network. This process does not primarily rely on manual updates from the content owner.

CDNs serve both static and dynamic content. The ability to keep content current is not limited to static content; it also applies to dynamic content through various caching and replication strategies.

### References



#### 14.2.4 Content Delivery Networks

q\_content\_deliver\_delivery\_current\_n09.question.fex



## Question 113.

× Incorrect

What mode in SNMP v3 does not encrypt packets?

- ☐ authPriv
- ☐ privAuth
- ☐ authNoPriv
- ☒ noAuthNoPriv

**Explanation**







The correct answer is authNoPriv. In SNMP v3, the authNoPriv mode requires authentication but does not encrypt packets, providing a level of security without encryption.

authPriv mode in SNMP v3 provides both authentication and encryption, ensuring secure communication between agents and monitors, contrary to authNoPriv which lacks encryption.

noAuthNoPriv mode offers neither authentication nor encryption, making it the least secure configuration in SNMP v3, suitable only for environments where security is not a concern.

privAuth is not a valid mode within SNMP v3's security model, which categorizes security levels as noAuthNoPriv, authNoPriv, and authPriv, focusing on the presence of authentication and encryption.

**References**

-  **8.2.1 Network Discovery**
-  **8.3.1 SNMP Agents and Monitors**
-  **8.3.2 SNMP Security**
-  **8.3.3 Configuring an SNMP System on a Router**
-  **8.3.4 Monitoring a Switch with SNMP**
-  **8.3.5 Configuring SNMP Trap**

q\_snmp\_authnopriv\_n09.question.fex

## Question 114.

✓ Correct

What does the "confidentiality" aspect of the CIA Triad ensure?

- ☐ Confidentiality ensures that the system can continue to operate effectively even under attack.
- ☐ Confidentiality ensures that data is available and accessible to anyone who needs it.
- ☒ Confidentiality ensures that certain information is only accessible to those who are authorized to view it.
- ☐ Confidentiality ensures that data is stored and transferred without any unauthorized modifications.

**Explanation**

The confidentiality aspect of the CIA Triad focuses on protecting sensitive information from unauthorized access and disclosure. It ensures that data is only available to individuals who have the necessary permissions to access it, thereby safeguarding personal and business information from potential breaches and misuse.

Confidentiality is about restricting access to information, not making it universally available. The aspect of the CIA Triad that deals with making information accessible to authorized users is "Availability," not "Confidentiality."

Confidentiality ensures that data is stored and transferred without any unauthorized modifications is incorrect because it describes the principle of "Integrity" within the CIA Triad, not "Confidentiality." Integrity is concerned with maintaining the accuracy and reliability of data by ensuring that it is not altered in an unauthorized manner during storage, transfer, or processing.

Confidentiality ensures that the system can continue to operate effectively even under attack is incorrect as it relates to the principle of "Availability" within the CIA Triad, which focuses on ensuring that data and systems are accessible to authorized users, especially during adverse conditions. "Confidentiality" specifically deals with protecting information from unauthorized access, not maintaining system operations under attack.

**References****9.1.1 Common Security Terminology**

q\_sec\_concepts\_confidentiality\_n09.question.fex

Question 115.

✕ Incorrect

What makes smart devices vulnerable to standard attacks?

- ☐ Their inability to connect to the Internet
- ☒ The use of proprietary operating systems
- ☐ The lack of integrated peripherals
- ☐ Their compute, storage, and network functions

### Explanation

Smart devices are effectively running mini-computers with compute, storage, and network capabilities. These functions make them vulnerable to some of the standard attacks associated with web applications and network functions, such as malware, hacking, and unauthorized access.

The ability to connect to the Internet is actually what exposes smart devices to potential attacks, not an inability.

Many smart devices use common operating systems like Linux or Android, not proprietary ones, which means they share vulnerabilities known in those systems.

Integrated peripherals, such as cameras or microphones, could indeed be compromised, but their presence is not what primarily makes smart devices vulnerable; it's the compute, storage, and network functions.

### References

**11.2.1 IoT Devices****11.2.3 IoT Networks****11.2.4 IoT Network Security****11.2.5 Lab: Scan for IoT Devices**

q\_iot\_smart\_device\_vulnerability\_n09.question.fex

## Question 116.

× Incorrect

Which of the following is a valid IPv6 address compression?

- ☒ 2001:db8::abc::def0:1234
- ☐ 2001:db8:0000:0000:0abc:0000:def0:1234
- ☐ 2001:db8:0abc::def0:1234
- ☐ 2001:db8::abc:0:def0:1234

**Explanation**

The 2001:db8::abc:0:def0:1234 address correctly uses the double colon (::) to compress consecutive 16-bit blocks of zeros only once, adhering to the rules of IPv6 address notation.

2001:db8::abc::def0:1234 is incorrect because it uses double colon compression more than once, which violates the rule that it can only be used once to avoid ambiguity.

2001:db8:0000:0000:0abc:0000:def0:1234 is incorrect in this context because it is fully expanded and does not demonstrate compression.

2001:db8:0abc::def0:1234 is incorrect because it suggests an incorrect structure by misplacing the compression, potentially leading to confusion about the original address structure.

**References****4.5.2 IPv6 Address Format**

q\_ipv6\_format\_valid\_compression\_n09.question.fex

## Question 117.

✓ Correct

What is typically indicated when a host can ping a server by its IP address but not by its name?

- ☐ Faulty network cable
- ☒ Incorrect DNS configuration
- ☐ Incorrect subnet mask configuration
- ☐ The server is offline.

**Explanation**














When a host can ping a server by its IP address but not by its name, it indicates an issue with DNS configuration. DNS is responsible for translating human-readable domain names into IP addresses. If DNS is not correctly configured, the host cannot resolve the name to an IP address, though direct IP connectivity remains unaffected.

The server being offline would prevent both name and IP address pinging.

An incorrect subnet mask would affect all network communications, not just name resolution.

A faulty network cable would prevent any form of communication, including pinging by IP address.

**References**

-  **6.5.1 Host Names and Domain Names**
-  **6.5.2 DNS Hierarchy**
-  **6.5.3 Name Resolution Using DNS**
-  **6.5.4 Resource Record Types**
-  **6.5.5 Host Address and Canonical Name Records**
-  **6.5.6 Mail Exchange, Service, and Text Records**
-  **6.5.7 Pointer Records**
-  **6.5.8 DNS Server Configuration**
-  **6.5.9 Internal vs External DNS**
-  **6.5.10 DNS Security**
-  **6.5.11 Lab: Configure DNS Addresses**
-  **6.5.12 Lab: Create Standard DNS Zones**
-  **6.5.13 Lab: Create Host Records**

**6.5.14 Lab: Create CNAME Records****6.5.15 Lab: Troubleshoot DNS Records****6.5.16 Configuring DNS Caching on Linux****6.6.1 Client DNS Issues****6.6.2 Name Resolution Issues****6.6.3 nslookup****6.6.4 dig****6.6.5 Lab: Explore nslookup****6.6.6 Lab: Use nslookup**

q\_trouble\_dns\_ping\_ip\_address\_n09.question.fex

## Question 118.

✓ Correct

What standards are most wireless LANs based on?

- ☐ Wi-Fi 5
- ☒ 802.11
- ☐ MU-MIMO
- ☐ Cellular radio

**Explanation**

Most wireless LANs (WLANs) are based on the IEEE 802.11 standards which define the physical layer media by which data encodes into a radio carrier signal by using a modulation scheme.

Wi-Fi 5 works only in the 5 GHz band although it can use the 2.4 GHz band for legacy standards (802.11g/n) in mixed mode.

Multiuser MIMO (MU-MIMO) is the use of spatial multiplexing to connect multiple MU-MIMO-capable stations simultaneously, providing the stations are not on the same directional path.

Cellular radio is mobile telephony standards divided into 2G (GSM; up to about 14 Kbps), 2.5G (GPRS, HSCSD, and EDGE; up to about 48 Kbps), and 3G (WCDMA; up to about 2 Mbps).

**References****12.1.1 IEEE 802.11 Wireless Standards****12.1.2 IEEE 802.11a and 5GHz Channel Bandwidth****12.1.4 IEEE 802.11n, MIMO, and Channel Bonding****12.1.6 Multiuser MIMO and Band Steering**

q\_wireless\_802\_11\_n09.question.fex

## Question 119.

✓ Correct

What is the difference between an Internet gateway and a NAT gateway in terms of directionality?

- ☐ An Internet gateway is one-way, while a NAT gateway is two-way.
- ☒ An Internet gateway is two-way, while a NAT gateway is one-way.
- ☐ Both gateways are two-way.
- ☐ Both gateways are one-way.

**Explanation**

An Internet gateway allows two-way communication, enabling instances to send and receive data over the Internet. A NAT gateway, on the other hand, only allows one-way (outbound) communication, meaning instances can send data out but cannot receive data initiated from the Internet.

An Internet gateway is one-way, while a NAT gateway is two-way is the opposite of the correct relationship. An Internet gateway supports two-way communication, while a NAT gateway supports only outbound communication.

Both gateways are one-way is incorrect because an Internet gateway supports two-way communication.

Both gateways are two-way is incorrect because a NAT gateway only supports outbound (one-way) communication.

**References****14.3.3 Cloud Gateways**

q\_net\_virtual\_internet\_vs\_nat\_gateway\_n09.question.fex



## Question 120.

× Incorrect

Which cloud service model allows businesses to rent IT resources such as servers and storage on an as-needed basis?

- ☐ PaaS
- ☐ DaaS
- ☐ IaaS
- ☒ SaaS

**Explanation**

Infrastructure as a Service (IaaS) provides virtualized computing resources over the Internet. It allows businesses to rent IT infrastructure (servers, virtual machines, storage, networks, and operating systems) on a pay-as-you-go basis from a cloud provider.

Software as a Service (SaaS) delivers software applications over the Internet, on a subscription basis, not IT infrastructure.

Platform as a Service (PaaS) offers hardware and software tools over the Internet, mainly for application development, not just raw IT infrastructure.

DaaS (Desktop as a Service) provides virtual desktops to users over the Internet, which is not the same as offering IT infrastructure components.

**References****14.2.3 Cloud Service Models**

q\_cloud\_service\_iaas\_example\_02\_n09.question.fex

## Question 121.

✓ Correct

What is a legitimate reason for a client to disassociate but not deauthenticate from an AP?

- ☒ The client is roaming in an extended service area.
- ☐ The client is updating its firmware.
- ☐ The client is performing a security scan.
- ☐ The client is shutting down.

**Explanation**

When a client roams from one AP to another within the same network, it may disassociate from the current AP without deauthenticating because it intends to maintain its authentication status with the network as it moves to another AP.

Shutting down would typically lead to both disassociation and deauthentication.

Performing a security scan is unrelated to the association status with an AP.

Firmware updates do not require maintaining an association with a specific AP.

**References****12.4.5 Roaming and Client Disassociation Issues**

q\_client\_dis\_disassociate\_not\_deauthorize\_n09.question.fex

## Question 122.

✓ Correct

Which process allows hosts using private IP addresses to access the Internet?

- ☐ Domain Name System (DNS)
- ☐ Internet Protocol Security (IPsec)
- ☐ Dynamic Host Configuration Protocol (DHCP)
- ☒ Network Address Translation (NAT)

**Explanation**

NAT translates private IP addresses to a public IP address for Internet communication, allowing multiple devices on a local network to share a single or a few public IP addresses. This process enables private-addressed hosts to access the Internet.

DHCP is used for automatically assigning IP addresses to devices on a network, not for enabling Internet access for private addresses.

DNS translates domain names to IP addresses, facilitating user-friendly Internet browsing. It does not enable Internet access for private IP addresses.

IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a data stream. It is not related to enabling Internet access for private addresses.

**References****4.3.2 Public vs Private Addressing**

q\_priv\_address\_nat\_process\_n09.question.fex

## Question 123.

✓ Correct

What does "protect mode" do when a switch port enters a violation state?

- ☐ It disables the port and sends alerts.
- ☒ It drops frames from the invalid source address but keeps the interface open.
- ☐ It encrypts traffic from the invalid source address.
- ☐ It reroutes traffic from the invalid source address to a quarantine VLAN.

**Explanation**

The correct answer is that it drops frames from the invalid source address but keeps the interface open. Protect mode allows the port to continue operating for authorized traffic while blocking frames from unauthorized sources, providing a balance between security and network functionality.

It disables the port and sends alerts is incorrect because this describes the shutdown mode, not protect mode.

It encrypts traffic from the invalid source address is incorrect because protect mode involves dropping unauthorized frames, not encrypting them.

It reroutes traffic from the invalid source address to a quarantine VLAN is incorrect because protect mode specifically drops frames rather than rerouting traffic.

**References**

 **10.4.1 Network Access Control and Port Security**

 **10.4.2 Lab: Secure Access to a Switch**

 **10.4.3 Lab: Secure Access to a Switch 2**

 **10.4.4 Lab: Disable Switch Ports - GUI**

 **10.4.6 Port Guards**

 **10.4.7 Lab: Harden a Switch**

 **10.4.8 Port Mirroring**

q\_port\_security\_protect\_mode\_n09.question.fex

## Question 124.

✓ Correct

Which organizations have created categories of cable standards for twisted pair to simplify the selection of a suitable quality cable?

- ☒ ANSI and TIA/EIA
- ☐ ITU and ETSI
- ☐ IEEE and IETF
- ☐ ISO and IEC

**Explanation**

The American National Standards Institute (ANSI) and the Telecommunications Industry Association (TIA)/Electronic Industries Alliance (EIA) are responsible for creating categories of cable standards for twisted pair cables. This simplifies the process of selecting a suitable quality cable for telecommunications purposes.

IEEE and IETF are organizations involved in setting standards for various technologies, but they are not the ones responsible for creating categories of cable standards for twisted pair cables.

ISO and IEC maintain similar standards but are not the primary organizations mentioned in the document for creating categories of cable standards for twisted pair cables.

ITU and ETSI are involved in telecommunications and standardization but are not the organizations mentioned in the document for this specific task.

**References****2.2.3 Cat Cable Standards**

q\_cat\_ansi\_tia\_eia\_n09.question.fex

## Question 125.

✓ Correct

What is meant by cloud elasticity?

- ☐ The process of moving data from one cloud provider to another
- ☒ The ability for a cloud system to adjust resources in real-time
- ☐ The use of multiple cloud providers to ensure data redundancy
- ☐ The ability to add more storage to the cloud system as needed

**Explanation**

Cloud elasticity refers to the system's ability to scale resources up or down automatically and in real-time as demand changes. This ensures that the system can handle sudden increases in demand without loss of service or performance and can also reduce resources to save costs when demand is low.

Adding more storage is a part of scalability but does not fully capture the concept of elasticity, which includes real-time adjustments for both increasing and decreasing demand.

Moving data between cloud providers is related to cloud migration, not elasticity.

Using multiple cloud providers for redundancy is a strategy for achieving high availability and disaster recovery, not elasticity.

**References****14.2.1 Cloud Scalability and Elasticity**

q\_cloud\_scale\_elasticity\_description\_n09.question.fex

## Question 126.

✓ Correct

You are a network administrator tasked with setting up a Wi-Fi network in a large office building. The building has multiple floors with thick concrete walls and several electronic devices that could cause interference. Your primary goal is to ensure high data rates and minimal interference for the office's Wi-Fi network.

Given this scenario, which frequency band and configuration would be the most appropriate for your Wi-Fi network?

- ☐ Use the 2.4 GHz band because it has better penetration through solid surfaces.
- ☒ Use the 5 GHz band because it supports higher data rates and has more individual channels.
- ☐ Use the 2.4 GHz band because it is less congested and supports more individual channels.
- ☐ Use the 5 GHz band but limit the power output to comply with regulatory constraints.

**Explanation**

The 5 GHz band supports higher data rates and has more individual channels, which reduces the risk of interference. Although it is less effective at penetrating solid surfaces, the higher data rates and reduced congestion make it more suitable for an office environment where high performance is required, as in this scenario.

While it is true that the 2.4 GHz band has better penetration through solid surfaces, it is often congested with other Wi-Fi networks and other types of wireless technology, such as Bluetooth®. This congestion can lead to increased interference and lower data rates, which is not ideal for a high-performance office network.

The 2.4 GHz band is actually more congested and supports fewer individual channels compared to the 5 GHz band. Therefore, it is not the best choice for minimizing interference and maximizing data rates.

While it is true that regulatory constraints may limit the power output of devices using the 5 GHz band, this answer does not address the primary benefits of the 5 GHz band, which are higher data rates and more individual channels. Limiting power output is a regulatory requirement but not a primary factor in choosing the 5 GHz band for this scenario.

**References**

**12.1.2 IEEE 802.11a and 5GHz Channel Bandwidth**

q\_5ghz\_802\_11a\_example\_n09.question.fex

Question 127.

✓ Correct

What is the purpose of using a hot aisle/cold aisle layout in a data center?

- ☐ To enhance physical security of the servers
- ☐ To increase the density of servers in a rack
- ☒ To maximize cooling efficiency
- ☐ To simplify cable management

**Explanation**

A hot aisle/cold aisle layout is designed to maximize cooling efficiency by ensuring that hot air expelled from exhaust vents does not mix with the cool air drawn in through intake vents. This layout helps in maintaining optimal operating temperatures for the equipment.

Increasing the density of servers in a rack is related to how many units can be fitted into a given space, not cooling.

Enhancing physical security of the servers is achieved through other means, such as lockable doors.

Simplifying cable management is not the primary purpose of a hot aisle/cold aisle layout, though it may indirectly affect it.

**References****2.5.1 Rack Systems****2.5.2 Humidity and Temperature**

q\_rack\_diagram\_hot\_cold\_aisle\_n09.question.fex



## Question 128.

✓ Correct

How is a user's biometric data used in a biometric lock system?

- ☐ It is stored on the user's badge.
- ☒ It is recorded and stored on an authentication server.
- ☐ It is sent to a remote server for storage.
- ☐ It is deleted immediately after each use for privacy reasons.

**Explanation**

In a biometric lock system, a user's biometric data is recorded as a template and stored on an authentication server. When the user attempts to gain access, their biometric is scanned and compared to the stored template for authentication.

Sending biometric data to a remote server for storage is not the standard practice for biometric lock systems, which typically store templates on a dedicated authentication server.

Storing biometric data on the user's badge is not secure or practical for biometric lock systems, which rely on authentication servers.

Deleting biometric data immediately after each use would negate the purpose of having a biometric lock system, which needs to store templates for comparison.

**References****11.3.1 Locks****11.3.4 Lab: Implement Physical Security**

q\_badges\_biometric\_data\_n09.question.fex

## Question 129.

✓ Correct

What is the role of a beacon frame in a WLAN?

- ☐ To directly connect client devices to the Internet
- ☒ To advertise the WLAN
- ☐ To suppress the SSID broadcast
- ☐ To encrypt data transmissions between the AP and client devices

**Explanation**

Beacon frames are special management frames broadcast by the AP to advertise the WLAN's presence. They contain information such as the SSID/ESSID, BSSID, supported data rates, signaling, and encryption/authentication requirements, making it easier for client devices to discover and connect to the network.

Beacon frames advertise the network; they do not encrypt data transmissions.

Beacon frames do not provide direct internet connections; they advertise the network to potential clients.

Beacon frames are used for broadcasting the SSID, not suppressing it.

**References****12.2.4 Wireless Roaming**

q\_wifi\_bridge\_beacon\_frame\_role\_n09.question.fex

## Question 130.

✓ Correct

What does the **show startup-config** command display?

- ☐ The list of errors logged by the switch
- ☐ The switch's temporary configuration
- ☒ The switch's configuration upon the next reboot
- ☐ The switch's current operational status

**Explanation**

The **show startup-config** command is used to display the switch's configuration that will be used upon the next reboot. This is important for verifying changes that are saved but not yet applied.

The switch's temporary configuration is typically referred to as the running configuration, not the startup configuration.

The switch's current operational status is typically shown with commands like **show system status**, not **show startup-config**.

The list of errors logged by the switch can be viewed with commands like **show logging**, not **show startup-config**.

**References****3.4.3 Switch Show Commands**

q\_int\_config\_show\_startup-config\_n09.question.fex

## Question 131.

✓ Correct

What is the primary purpose of ARP poisoning in an on-path attack?

- ☒ To redirect traffic through the attacker.
- ☐ To encrypt all data packets on the network.
- ☐ To increase the efficiency of the ARP protocol.
- ☐ To physically damage the network infrastructure.

**Explanation**

The correct answer is to redirect traffic through the attacker, allowing them to intercept or modify it. ARP poisoning manipulates the ARP cache so that traffic intended for a specific host is misdirected to the attacker instead. This enables the attacker to intercept, monitor, or alter the traffic, which is the primary goal of such an attack.

ARP poisoning is a malicious activity aimed at compromising network security, not improving protocol efficiency.

ARP poisoning does not involve encryption; it involves deceiving network devices about the true MAC address associated with an IP address.

ARP poisoning is a software-based attack that affects network traffic flow and data integrity, not the physical infrastructure of the network.

**References**

 **9.3.3 Poison ARP**

 **9.3.7 Lab: Poison ARP and Analyze with Wireshark**

q\_path\_attack\_arp\_poisoning\_on-path\_n09.question.fex

## Question 132.

✓ Correct

What does IPv6 use to replace the Options field found in IPv4 headers?

- ☐ Hop Limit
- ☒ Extension headers
- ☐ Traffic Class
- ☐ Flow Label

**Explanation**

In IPv6, the Options field from IPv4 headers is replaced by extension headers. These headers provide a flexible method to extend the protocol and support features like fragmentation and reassembly, security (IPSec), and source routing.

Traffic Class is used in IPv6 for QoS purposes but does not replace the Options field.

Hop Limit replaces the TTL field from IPv4, not the Options field.

Flow Label is used for identifying packet flows in IPv6 and does not replace the Options field.

**References****4.5.1 IPv4 vs IPv6**

q\_ipv4\_ipv6\_option\_field\_replace\_n09.question.fex

## Question 133.

✓ Correct

What is the purpose of installing cages around racks in data centers?

- ☐ To enhance the visual appeal of the data center
- ☒ To restrict access by technicians to their own equipment
- ☐ To improve air circulation around the equipment
- ☐ To reduce the risk of electrical interference

**Explanation**

Installing cages around racks in data centers is a security measure that ensures technicians can only physically access the racks containing their own company's servers and appliances. This prevents unauthorized access to equipment owned by other companies, enhancing security within a shared or colocation data center environment.

Improving air circulation around the equipment is important for preventing overheating, but it is not the primary purpose of installing cages. Data center design, including the layout and cooling systems, primarily addresses air circulation.

Reducing the risk of electrical interference is a concern in data center design, but cages around racks are not intended for this purpose. Electrical interference is typically managed through proper cabling, grounding, and equipment design.

Enhancing the visual appeal of the data center may be a consideration in its overall design, but the primary purpose of installing cages around racks is to provide security and control access, not to improve aesthetics.

**References****11.3.1 Locks**

q\_badges\_cage\_purpose\_n09.question.fex

## Question 134.

✓ Correct

What is the role of virtualized security appliances in modern data centers?

- ☒ To monitor traffic as it passes between servers
- ☐ To replace physical servers
- ☐ To store physical documents securely
- ☐ To manage employee workspaces

**Explanation**

Virtualized security appliances play a crucial role in modern data centers by monitoring traffic as it passes between servers, helping to secure east-west traffic without creating bottlenecks. They do not replace physical servers, store documents, or manage workspaces.

Virtualized security appliances are focused on security, not on replacing the core computing resources.

Virtualized security appliances are concerned with digital data security, not physical document storage.

The role of virtualized security appliances is in network security, not in workspace management.

**References****14.1.1 Data Center Network Design**

q\_data\_center\_install\_virtualized\_appliances\_n09.question.fex

## Question 135.

✓ Correct

Which of the following BEST describes the method an attacker might use to make an evil twin access point more appealing to unsuspecting users?

- ☐ Decreasing the signal strength of the evil twin access point
- ☐ Encrypting the connection to the evil twin access point with an outdated encryption method
- ☒ Configuring the evil twin access point with a similar or identical SSID to a legitimate access point
- ☐ Naming the evil twin access point with a completely unrelated SSID

**Explanation**

An evil twin access point is designed to mimic a legitimate access point to deceive users into connecting to it. By configuring the evil twin with a similar or identical SSID (Service Set Identifier) to that of a legitimate access point, attackers make it difficult for users to distinguish between the two. This similarity can trick users into connecting to the evil twin, believing it to be the legitimate network, thereby exposing their devices to potential attacks or data interception.

Decreasing the signal strength of the evil twin access point would make it less appealing to users. Users are more likely to connect to access points with stronger signals, believing them to provide better connectivity.

Naming the evil twin access point with a completely unrelated SSID would not make it appealing or convincing as a legitimate access point. Users are less likely to connect to unfamiliar networks, especially when they are looking for a specific, known network.

Encrypting the connection to the evil twin access point with an outdated encryption method would not necessarily make it more appealing. While encryption might give a sense of security, the use of an outdated method does not contribute to the evil twin's appeal in mimicking a legitimate access point. Users typically do not check the encryption method before connecting; they are more influenced by the SSID and signal strength.

**References****12.3.6 Wireless Network Attacks**

q\_wifi\_atck\_evil\_twin\_appealing\_n09.question.fex



## Question 136.

✓ Correct

Which protocol is typically used for remote configuration of network appliances?

- ☐ HTTP
- ☐ SNMP
- ☒ SSH
- ☐ FTP

**Explanation**

Secure Shell (SSH) is commonly used for the remote configuration of network appliances, especially those that are headless (lacking a video monitor or input devices). SSH provides a secure channel over an unsecured network, enabling secure command execution and configuration changes on remote devices.

HTTP is widely used for web browsing and can be used for configuration purposes, but it is not specifically designed for secure remote configuration like SSH.

FTP is used for transferring files between systems but does not provide a secure method for configuring network appliances.

SNMP is used for managing and monitoring network devices but is not typically used for direct configuration tasks.

**References**

 **6.1.6 Common TCP and UDP Ports**

 **13.3.1 Remote Host Access**

 **13.3.2 Secure Shell**

q\_ssh\_emulate\_remote\_config\_ssh\_n09.question.fex

## Question 137.

× Incorrect

What is the effect of suppressing SSID broadcast in a WLAN?

- ☐ It increases the beacon frame broadcast interval.
- ☐ It requires users to manually configure the network connection.
- ☐ It automatically encrypts all data transmissions.
- ☒ It makes the network invisible to all client devices.

**Explanation**

Suppressing SSID broadcast means the network name is not openly advertised. As a result, users must manually enter the network's SSID to connect, as their devices will not automatically detect and display the network in the list of available networks.

The network is not entirely invisible, as determined devices can still detect it.

SSID suppression affects network discovery, not the encryption of data transmissions.

SSID broadcast settings do not directly affect the beacon frame broadcast interval.

**References****12.2.4 Wireless Roaming**

q\_wifi\_bridge\_ssid\_suppress\_n09.question.fex

## Question 138.

✓ Correct

What is the primary purpose of analyzing access point association times for client devices?

- ☒ To identify issues with roaming
- ☐ To assess the security level of the wireless network
- ☐ To determine the optimal placement for new access points
- ☐ To calculate the total data usage of each client

**Explanation**

The correct answer is to identify issues with roaming. Analyzing the association times of client devices with access points can reveal how quickly and effectively clients are able to roam within the network. Long association times or frequent reassociations can indicate problems with roaming configurations, such as insufficient overlap between AP coverage areas or issues with client support for roaming standards. This analysis helps in diagnosing and addressing roaming issues to ensure a seamless wireless experience.

While the placement of access points is crucial for network design, analyzing association times specifically targets roaming performance rather than initial AP placement.

Association times do not directly relate to data usage. Data usage analysis would require different metrics, such as the amount of data transmitted and received by each client.

The security level of the wireless network is assessed through other means, such as encryption standards and authentication methods, rather than through association times, which focus on connectivity and roaming performance.

**References****12.4.5 Roaming and Client Disassociation Issues**

q\_client\_dis\_access\_point\_times\_n09.question.fex

## Question 139.

× Incorrect

Which protocol is known for operating at the Network layer of the OSI model to authenticate hosts and encrypt packets?

- ☐ PPP
- ☐ GRE
- ☐ IPSec
- ☒ TLS

**Explanation**

IPSec operates at the Network layer (Layer 3) and is designed to secure IP communications through authenticating and encrypting each IP packet in a data stream. IPSec is widely used in VPNs for securing Internet communication.

PPP operates at the Data Link layer and does not inherently encrypt or authenticate packets.

GRE operates at the Network layer but does not provide authentication or encryption.

TLS operates at a higher layer, the Session layer, and is not designed to work at the Network layer like IPsec.

**References****4.5.7 IPv4 and IPv6 Transition Mechanisms****4.5.9 Lab: Configure an IPv6 Address****13.2.2 Tunneling Protocols**

q\_tunneling\_protocols\_ipsec\_network\_layer\_n09.question.fex

## Question 140.

✓ Correct

What is the benefit of using virtual appliances in a cloud environment?

- ☐ They eliminate the need for any network security.
- ☐ They are only compatible with proprietary operating systems.
- ☒ They can emulate the functions of dedicated hardware appliances.
- ☐ They require dedicated hardware.

**Explanation**

Virtual appliances in a cloud environment can emulate the functions of dedicated hardware appliances, such as routers or firewalls, without the need for physical hardware, offering flexibility and scalability.

One of the main benefits of virtual appliances is that they do not require dedicated hardware.

Virtual appliances do not eliminate the need for network security; they must still be secured like any other network component.

Virtual appliances are designed to be compatible with standard operating systems and computing platforms, not just proprietary ones.

**References****14.3.1 Cloud Instances**

q\_cloud\_sec\_appliance\_advantage\_n09.question.fex

## Question 141.

✓ Correct

What feature allows a security camera to survey a large room and pick out individual faces?

- ☐ Narrow focal length
- ☐ Fixed positioning
- ☐ Coaxial cabling
- ☒ Pan-Tilt-Zoom (PTZ) controls

**Explanation**

The correct answer is Pan-Tilt-Zoom (PTZ) controls. PTZ controls allow a camera to pan (move horizontally), tilt (move vertically), and zoom in on specific areas or subjects. This capability is essential for surveying large rooms and picking out individual faces, providing flexibility and detailed surveillance that fixed cameras cannot offer.

Fixed positioning limits a camera to one viewpoint, making it inadequate for surveying large rooms effectively.

A narrow focal length is suitable for capturing images through a fixed, narrow view, not for flexible, detailed surveillance of large areas.

Coaxial cabling is a method of connecting cameras to a network or multiplexer, not a feature that enhances a camera's ability to survey large areas.

**References****11.3.2 Cameras****11.3.4 Lab: Implement Physical Security**

q\_detect\_device\_ptz\_controls\_n09.question.fex

## Question 142.

✓ Correct

How has the concept of the network edge changed due to the erosion of the perimeter security model?

- ☐ It has become more focused on the physical location of the network.
- ☐ It has become synonymous with the firewall.
- ☐ It has been eliminated entirely.
- ☒ It has expanded to include access switches and wireless access points.

**Explanation**








As the traditional perimeter security model has become less effective, the concept of the network edge, or perimeter, has expanded. It now includes not just the boundary between the private and public networks but also internal components like access switches and wireless access points, which were previously considered "internal."

The change in the network edge concept is not about focusing more on physical location but expanding what is considered the edge.

While firewalls are part of the network edge, the concept has expanded beyond just the firewall to include other components.

The concept of the network edge has not been eliminated but rather expanded to adapt to new security challenges.

**References**

-  **1.3.3 Data Link Layer Functions**
-  **3.2.1 Hubs**
-  **3.2.3 Switches**
-  **3.2.4 Ethernet Switch Types**
-  **3.2.5 Switch Interface Configuration**
-  **3.2.7 Lab: Install a Switch in the Rack**
-  **3.2.8 Lab: Secure a Switch**

q\_defense\_depth\_network\_edge\_change\_n09.question.fex

## Question 143.

✓ Correct

What does the Version field in the IPv4 header indicate?

- ☐ The type of payload encapsulated in the packet
- ☒ The version of Internet Protocol in use
- ☐ The total packet size
- ☐ The size of the header

**Explanation**

The Version field in the IPv4 header specifically indicates the version of the Internet Protocol that is being used, which in this case is 4. This is crucial for ensuring that the packet is processed correctly according to the appropriate IP standards.

The type of payload is indicated by the Protocol field, not the Version field.

The size of the header is indicated by the Length fields, not the Version field.

The total packet size is also indicated by the Length fields, not the Version field.

**References****4.1.1 IPv4 Datagram Header**

q\_ipv4\_header\_version\_purpose\_n09.question.fex



## Question 144.

✓ Correct

What is the purpose of a Business Impact Analysis (BIA) in continuity planning?

- ☐ To evaluate the effectiveness of sales strategies
- ☐ To identify the most profitable business areas
- ☒ To identify risk disruption for primary business functions
- ☐ To assess the impact of new hires on the business

**Explanation**

A BIA is conducted to understand which business functions are critical (mission essential and primary) and to assess the risks and impacts that would arise if the organization is unable to fulfill these functions due to a disruption.

Identifying profitable business areas is a strategic business decision, not the focus of a BIA, which is concerned with continuity planning.

Assessing the impact of new hires is related to human resources management, not the objective of a BIA.

Evaluating sales strategies is a marketing function and not the purpose of conducting a BIA in continuity planning.

**References****7.4.1 Disaster Recovery Concepts**

q\_availability\_bia\_role\_n09.question.fex

## Question 145.

✓ Correct

What is a reverse proxy used for?

- ☒ Managing inbound traffic
- ☐ Directly connecting clients to the Internet
- ☐ Managing outbound traffic
- ☐ Storing data permanently

**Explanation**

A reverse proxy is used for managing inbound traffic, acting as an intermediary for requests from the Internet to internal servers. It can provide additional security, load balancing, and caching services.

Managing outbound traffic is the role of a forward proxy.

Directly connecting clients to the Internet is not the purpose of a reverse proxy.

Storing data permanently is not a function of a reverse proxy; it may cache data temporarily to improve performance.

**References****10.5.2 Proxy Servers**

q\_proxy\_reverse\_role\_n09.question.fex

## Question 146.

× Incorrect

A network engineer is assigned to locate and acquire a data communications network controlled by a single organization.

What is the name for this type of network?

- ☐ Enterprise WAN
- ☐ T-Carrier
- ☐ WAN
- ☒ Digital Subscriber Line

**Explanation**











The term enterprise WAN describes a WAN operated and controlled by a single organization.

Wide area network (WAN) technologies support data communications over greater distances than LANs. Long-distance communications usually involve the use of public networks. Public networks are owned by telecommunications (telco) companies and provide WAN services to businesses and households.

The T-carrier system was developed by the telecommunications provider Bell Labs. This system allows a user to place multiple calls on a single cable.

Digital subscriber line (DSL) is a technology for transferring data over voice-grade telephone lines, often referred to as the local loop.

**References**

-  **1.2.1 Open Systems Interconnection Model**
-  **1.2.5 Layer 3 - Network**
-  **1.2.8 OSI Model Summary**
-  **1.3.4 Network Layer Functions**
-  **1.3.6 The Internet**
-  **1.3.7 Binary and Hexadecimal**
-  **1.3.8 Lab: Explore a Single Location in a Lab**
-  **4.1.2 Layer 2 vs. Layer 3 Addressing and Forwarding**
-  **13.1.1 Wide Area Networks and the OSI Model**
-  **14.3.5 Cloud Firewall Security**

q\_wan\_enterprise\_description\_n09.question.fex

Question 147.

✓ Correct

Consider the following IP addresses:

1. 124.77.8.5
2. 131.11.0.9
3. 190.66.250.10
4. 196.5.89.44

Which of the following represents (in order) the IP address class of each listed IP address?

- ☐ Class B, Class B, Class C, Class D
- ☐ Class A, Class B, Class C, Class C
- ☐ Class B, Class B, Class C, Class C
- ☒ Class A, Class B, Class B, Class C
- ☐ Class B, Class C, Class C, Class D

### Explanation

The IP addresses listed are of the following classes: Class A, Class B, Class B, Class C. You can identify the IP address class by memorizing the range of values for the first octet.

- 0-126 = Class A
- 128-191 = Class B
- 192-223 = Class C
- 223-239 = Class D
- 240-255 = Class E

### References



#### 4.3.1 Classful Addressing

q\_class\_addr\_class\_order\_n09.question.fex

## Question 148.

× Incorrect

What is the function of the Protocol field in the IPv4 header?

- ☐ Indicates the size of the header
- ☐ Specifies the total packet size
- ☐ Specifies the type of data encapsulated in the payload
- ☒ Indicates the version of Internet Protocol in use

**Explanation**

The Protocol field in the IPv4 header specifies the type of data encapsulated in the payload, allowing the receiving host to know how to process it. This is crucial for the correct interpretation and handling of the data by the destination.

The version of Internet Protocol in use is indicated by the Version field.

The size of the header is indicated by the Length fields.

The total packet size is also indicated by the Length fields, not the Protocol field.

**References****4.1.1 IPv4 Datagram Header**

q\_ipv4\_header\_protocol\_purpose\_n09.question.fex

## Question 149.

✓ Correct

What is the primary purpose of authorization in network systems?

- ☒ To allocate rights and permissions
- ☐ To monitor network traffic
- ☐ To encrypt data
- ☐ To authenticate user identities

**Explanation**

Authorization occurs after authentication and is the process of allocating specific rights and permissions to a user account on networks, computers, and data. It determines what users can and cannot do within a system, such as accessing certain files or executing commands.

Authentication is the process of verifying the identity of a user or device, a prerequisite to authorization but serves a different purpose.

Encryption is a method of converting information or data into a code to prevent unauthorized access, which is not directly related to the allocation of rights and permissions.

Monitoring network traffic is a part of network management and security but does not directly involve the allocation of rights and permissions to user accounts.

**References****10.1.1 Access Control****10.1.2 Authentication Methods****10.2.2 Privileged Access Management****10.2.5 Lab: Manage Account Policies**

q\_rbac\_authorization\_primary\_purpose\_n09.question.fex

## Question 150.

✓ Correct

What is the role of Router Advertisements (RAs) in the IPv6 address configuration process?

- ☒ To inform hosts of network prefixes and autoconfiguration options
- ☐ To encrypt data packets sent between hosts and routers
- ☐ To request an IP address from a DHCPv6 server
- ☐ To assign static IP addresses to devices

**Explanation**

Router Advertisements (RAs) are sent by routers to inform hosts on the network about available network prefixes and autoconfiguration options (stateless or stateful). This information is crucial for hosts to configure their IPv6 addresses properly.

RAs do not request IP addresses; they provide information necessary for address configuration.

RAs are not involved in encrypting data packets; they are used for network configuration.

RAs do not assign static IP addresses; they provide information for automatic configuration.

**References**

**4.5.5 IPv6 Link Local Addressing**



**6.3.1 Automatic Private IP Addressing**



**6.3.4 Lab: Explore APIPA Addressing**



**6.3.5 Lab: Explore APIPA Addressing in Network Modeler**



**6.3.6 Set Up Alternate Addressing**

q\_apipa6\_ra\_role\_n09.question.fex