Chapter 1
REVIEW QUESTIONS

1. What should be enabled on a computer that has direct connection to the Internet?

A. Router C. Firewall
B. Switch D. VPN

A firewall should be enabled on a computer that has a direct connection to the Internet to protect it from unauthorized access and potential security threats. Firewalls help filter incoming and outgoing network traffic, providing an additional layer of security for the connected computer.

2. True or false. A WAP often provides access to the Internet.

False. A WAP (Wireless Access Point) primarily provides wireless connectivity within a local network but does not directly provide access to the Internet. Internet access is typically provided through a separate device like a router or modem, which may be connected to the WAP to extend the network's wireless coverage.

3. A group of computers are connected in a single location. What is this called?

A. LAN C. VLAN
B. WAN D. VPN

4. A network is connected using high-speed components rated at 1 Gbps.What does the b represent in Gbps? bits

5. Users in the network have to remember an average of five usernames and passwords to access different computers. How can you reduce the number of passwords remembered by users?

A. Change the network to a workgroup C. Create a WAN
B. Change the network to domain D. Create a VPN

To reduce the number of passwords remembered by users, you can change the network to a domain. In a domain-based network, user accounts and authentication are centrally managed by a domain controller. Users have a single set of credentials (username and password) that they use to access resources and devices within the domain. This eliminates the need for users to remember multiple usernames and passwords for different computers, as they can use their domain credentials to access various resources on the network.

6. Define a LAN.

A LAN, or Local Area Network, is a network of interconnected devices and computers within a limited geographical area, such as a home, office, or campus. LANs are designed to facilitate data sharing, resource sharing, and communication among devices located close to each other. Typically, LANs are connected through Ethernet cables or wireless connections like Wi-Fi. They are commonly used in homes and businesses to enable local communication and resource sharing, such as file sharing, printer sharing, and internet access. LANs can vary in size, ranging from small networks in homes to large networks in corporate environments.

7. Define a WAN.

A WAN, or Wide Area Network, is a network that spans a large geographical area, typically a city, country, or even multiple countries. It connects multiple LANs (Local Area Networks) or other WANs and enables data and resource sharing across long distances. WANs are often established using various telecommunication technologies, such as leased lines, satellites, or the Internet, and they are commonly used by organizations to connect remote offices or locations.

8. An employee is able to connect to the employer’s private network over the Internet. What is the employee using?

A. Domain controller C. WAP
B. LAN D. VPN

9. What are two types of remote access servers? (Choose two.)
A. Dial-up C. VPN
B. WAP D. Domain controller

10. True or false. All RFCs are known as standards.
Not all RFCs (Request for Comments) are known as standards. RFCs serve various purposes, including defining standards, providing guidelines, documenting protocols, and more. While some RFCs define standards, others may describe experimental protocols or informational documents. Therefore, not all RFCs are considered standards.

Chapter 2
REVIEW QUESTIONS
1. What type of traffic always goes to all devices in a subnet?
A. Unicast C. Broadcast
B. Multicast D. Allcast

2. True or false. A switch blocks broadcasts. Switches, unlike hubs, block broadcast traffic. They forward data only to the specific device it's intended for, reducing network congestion. Switches operate at the Data Link Layer (Layer 2) of the OSI model and are designed to forward traffic only to the specific device it is intended for based on MAC addresses. This behavior prevents broadcasts from being sent to all devices in a network, which helps reduce unnecessary network traffic and improves network efficiency.

3. What is the difference between a switch and a router?
A. Nothing. They are the same. B. Switches do not pass broadcasts, but routers do.
C. A switch connects devices together, and a router connects subnets together. D. A switch connects subnets together, and a router connects devices together.
Switches operate at the Data Link Layer (Layer 2) of the OSI model and are used to connect devices within the same local network. They forward traffic based on MAC addresses and do not perform routing between different IP subnets. Switches do not pass broadcasts beyond the local network segment. Routers operate at the Network Layer (Layer 3) of the OSI model and are used to connect different IP subnets or networks. They make forwarding decisions based on IP addresses and can route traffic between different subnets. Routers also provide functions like network address translation (NAT) and determine the best path for data to travel between networks.

4. True or false. Bridges can connect dissimilar physical topologies.
Bridges can connect dissimilar physical topologies. Bridges are network devices that operate at the Data Link Layer (Layer 2) of the OSI model. They are used to connect and filter traffic between different segments of a network. One of the advantages of bridges is that they can connect segments with different physical layer characteristics, such as Ethernet and Wi-Fi, allowing for greater flexibility in network design. They learn the MAC addresses of devices on each segment and use this information to make forwarding decisions, effectively extending the network while maintaining isolation between segments.

5. A firewall uses _____ to filter both inbound and outbound traffic. Rules

A firewall uses rules to filter both inbound and outbound traffic. These rules define what types of network packets are allowed to pass through the firewall and which ones are blocked, helping to secure a network by controlling access to it. Firewalls can filter traffic based on various criteria, such as IP addresses, port numbers, and the state of the connection, among others.

6. A network-based firewall is a hardware device that provides protection for a net- work. What is a host-based firewall? A host-based firewall is a software-based firewall that runs on individual devices (hosts). It provides protection for a single device rather than an entire network.

7. True or False. A crossover cable is used to connect a computer to a switch.
A crossover cable is typically used to directly connect two computers or two networking devices (e.g., two switches or two routers) without the need for an intermediate device like a switch. When connecting a computer to a switch, a straight-through Ethernet cable is typically used. The switch handles the necessary crossover internally to ensure proper communication between the computer and the switch.

8. Which of the following standards define how twisted-pair cables should be wired?
A. IEEE 802.3 C. Extranet wiring practices
B. RFC 791 D. T568B
The T568B standard defines how twisted-pair cables should be wired, particularly for Ethernet networking. This standard specifies the arrangement of wires within an Ethernet cable, ensuring that each wire is connected to the correct pins on connectors, such as RJ45 connectors. It is one of the two common wiring standards for Ethernet cables, with the other being T568A. These standards ensure that network cables are wired consistently to facilitate proper communication in Ethernet networks.

9. A company wants to host a web server for Internet users.The web server should be placed in _____. Perimeter network
A company that wants to host a web server for Internet users typically places the web server in an area of their network known as the "Demilitarized Zone" or "DMZ." The DMZ is a network segment that is located between the internal trusted network (intranet) and the external untrusted network (Internet).

Placing the web server in the DMZ provides several advantages:

Security: By segregating the web server in the DMZ, it is separated from the internal network where sensitive data and resources are located. This isolation helps protect the internal network from potential threats originating from the Internet.

Controlled Access: The DMZ allows controlled access to the web server from the Internet. Access control lists and security measures can be implemented to permit only authorized traffic to reach the web server.

Redundancy: In some configurations, redundant web servers can be placed in the DMZ to ensure high availability and load balancing for incoming web traffic.

Simplified Configuration: Placing the web server in the DMZ simplifies the configuration of firewalls and security policies, as traffic destined for the web server can be routed through the DMZ.

Overall, the DMZ is a critical component of network security when hosting services, such as web servers, that need to be accessible from the Internet while maintaining a secure separation from the internal network.
the DMZ (Demilitarized Zone) is often referred to as a "perimeter network." The term "perimeter network" emphasizes the idea that it is a network segment located at the perimeter or boundary of an

organization's internal network. This network segment is isolated from the internal network and is designed to provide controlled access to services that need to be exposed to untrusted networks, such as the Internet.

In the context of network security, the DMZ and perimeter network essentially refer to the same concept: a network segment that acts as an intermediary zone between an organization's internal network and external, potentially untrusted networks. It provides an additional layer of security by isolating externally accessible services and resources from the core internal network.

10. What is used to provide access to a company's resources via the Internet to trusted partners?
Extranet
The technology used to provide access to a company's resources via the Internet to trusted partners is often referred to as an "Extranet." An Extranet is a private network that uses the Internet as a connectivity medium to extend a company's network to selected external users, such as business partners, suppliers, or customers. It allows these trusted entities to access specific resources, collaborate, and share information securely over the Internet.

An Extranet typically employs security measures such as firewalls, encryption, access controls, and authentication mechanisms to ensure that only authorized users can access the shared resources. It provides a controlled and secure way for organizations to collaborate and exchange data with external parties without exposing their entire internal network to the public Internet.

Chapter 3
REVIEW QUESTIONS
1. The OSI Model has _____ layers. Seven
The OSI (Open Systems Interconnection) Model has **seven layers**, each serving a specific purpose:

1. **Physical Layer**: This is the lowest layer and deals with the physical medium, such as cables and electrical voltages. It is responsible for transmitting raw binary data over a physical medium.

2. **Data Link Layer**: This layer focuses on data framing, error detection, and MAC (Media Access Control) addressing. It ensures reliable point-to-point communication between devices on the same network.

3. **Network Layer**: The network layer is responsible for routing and forwarding data packets between different networks. It uses logical addressing, such as IP addresses, to determine the best path for data transmission.

4. **Transport Layer**: This layer provides end-to-end communication and error recovery. It ensures that data is reliably delivered between two devices and can use either TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) for this purpose.

5. **Session Layer**: The session layer manages and establishes communication sessions between applications running on different devices. It handles session initiation, maintenance, and termination.

6. **Presentation Layer**: This layer deals with data translation, encryption, and compression. It ensures that data sent from one device can be understood by the receiving device, regardless of their internal representations.

7. **Application Layer**: The top layer, the application layer, provides network services directly to end-users or applications. It includes various protocols for tasks like email (SMTP), web browsing (HTTP), and file transfer (FTP).

2. Write down a mnemonic you use to remember the OSI Model.
Ascending - "Please Do Not Throw Sausage Pizza Away"
Descending - "All People Seem To Need Data Processing"

3. True or false.TCP is a connectionless protocol. Connection-oriented
TCP (Transmission Control Protocol) is not a connectionless protocol; it is a connection-oriented protocol. TCP ensures reliable and ordered delivery of data by establishing a connection between two devices before data transfer begins. It provides features such as acknowledgment of received data, retransmission of lost packets, and flow control to manage the rate of data transmission. These features make TCP suitable for applications that require guaranteed data delivery and in-order arrival, such as web browsing, email, and file transfer.

4. What is a unit of data called at theTransport layer?
A. Packet C. Frame
B. Segment D. Protocol data unit (PDU)
The Transport layer is responsible for ensuring the reliable and orderly transmission of data between two devices on a network.
When data is sent from one device to another, it is divided into smaller units at the Transport layer, and each of these units is referred to as a "Segment."
These segments contain essential information, including source and destination port numbers, sequence numbers, and error-checking information.
The Transport layer takes care of segmenting, numbering, and reassembling these segments to ensure the data arrives intact and in the correct order at its destination.

5. Which of the following could be a valid MAC address for a server named Server 1?
A. Server1 C. A4-BA-DB-FA-60-AD B. 192.168.1.5 D. G4-BA-10B-FA-60-AT
MAC addresses typically consist of six groups of two hexadecimal characters separated by colons or hyphens. Option B follows this format and could be a valid MAC address.

6. IPv4 operates on the _____ layer of the OSI Model. Network layer
IPv4 operates on the Network layer (Layer 3) of the OSI Model. The Network layer is responsible for routing packets of data so that they can travel across networks and reach their intended destinations. IPv4 is one of the key protocols used for addressing and routing data packets in network communications.

7. List the protocols that operate on theTransport layer of the OSI Model.
Transmission Control Protocol (TCP)
User Datagram Protocol (UDP)
Transmission Control Protocol (TCP): TCP is a connection-oriented protocol that provides reliable, error-checked communication. It establishes a connection, acknowledges the receipt of data packets, and retransmits lost packets. TCP is used for applications where data integrity and reliability are critical, such as web browsing, email, and file transfers.

User Datagram Protocol (UDP): UDP is a connectionless protocol that offers minimal error checking and no guarantee of reliable delivery. It is faster than TCP but lacks some of the error recovery features. UDP is used in situations where real-time or low-latency communication is more important than guaranteed delivery, such as in streaming media, online gaming, and some VoIP applications.

8. True or false. Devices that operate on layer 7 of the OSI Model are more intelligent than devices that operate on layer 1.
Layer 7 - Application Layer: This is the top layer of the OSI Model and is closest to the end user. It deals with high-level protocols and represents the interface between the user's application and the network. Devices at this layer understand the data in a format meaningful to the user. Examples include web browsers, email clients, and other applications that interact directly with users. These devices are aware of the content, structure, and purpose of the data being transmitted.

Layer 1 - Physical Layer: This is the lowest layer of the OSI Model and deals with the physical transmission of raw binary data over a physical medium. Devices at this layer, such as network cables and hubs, are concerned with electrical or optical signals, voltage levels, and the physical characteristics of the medium. They do not interpret the data itself.

In summary, Layer 7 devices operate at the application level, understanding the content and meaning of data, while Layer 1 devices are concerned with the physical transmission of raw data. Therefore, Layer 7 devices are considered more intelligent in terms of their ability to process and interpret data in a meaningful way for users.

9. Routers operate on which of the following layers of the OSI Model? Network layer
A. Layer 1 D. Layer 4 B. Layer 2 E. None of the above C. Layer 3
Layer 3 - Network Layer: This layer deals with logical addressing and routing. When data needs to be transmitted between different networks (e.g., from your local network to a server on the internet), it involves routing decisions. Routers are devices specifically designed for this purpose.

10. Proxy servers operate on which of the following layers of the OSI Model? Layer 7 - Application
A. Layer 1 D. Layer 4 B. Layer 2 E. None of the above C. Layer 3
Proxy servers primarily operate at the Application layer (Layer 7) of the OSI Model. Here's an explanation of why they are associated with this layer:

Application Layer (Layer 7): This layer is responsible for end-user services and applications. It deals with the actual user data and the protocols required to display, format, and make it usable for end-users. Proxy servers work at this layer because they act as intermediaries between clients (usually web browsers or other applications) and the servers they want to access.

HTTP Proxy: An HTTP proxy, for example, handles web requests and responses. When a client sends a web request (such as accessing a website), the request is intercepted by the HTTP proxy at the Application layer. The proxy can then evaluate and modify the request, forward it to the destination server on behalf of the client, receive the server's response, and send it back to the client.

Sure, here's a breakdown of each layer of the OSI Model, along with examples of hardware and protocols commonly associated with them:

1. **Physical Layer**:

- Hardware: Cables, network adapters, switches
- Protocols: Ethernet, USB, Bluetooth, RS-232

2. **Data Link Layer**:
- Hardware: Network interface cards (NICs), switches, bridges
- Protocols: Ethernet, Wi-Fi (802.11), IEEE 802.1Q (VLAN tagging)

3. **Network Layer**:
- Hardware: Routers, Layer 3 switches
- Protocols: IP (IPv4 and IPv6), ICMP, ARP

4. **Transport Layer**:
- Hardware: None (primarily a software layer)
- Protocols: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), SCTP (Stream Control Transmission Protocol)

5. **Session Layer**:
- Hardware: None (primarily a software layer)
- Protocols: NetBIOS, PPTP (Point-to-Point Tunneling Protocol)

6. **Presentation Layer**:
- Hardware: None (primarily a software layer)
- Protocols: SSL/TLS (Secure Sockets Layer/Transport Layer Security), ASCII, EBCDIC

7. **Application Layer**:
- Hardware: End-user devices (computers, smartphones)
- Protocols: HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol 3), IMAP (Internet Message Access Protocol)

Chapter 4
REVIEW QUESTIONS

1. Which of the following protocols is considered connection-oriented?

A. UDP C. ARP
B. TCP D. DHCP

TCP is considered a connection-oriented protocol because it establishes a reliable connection between two devices before data exchange, ensuring the delivery of data in the correct order and with error-checking mechanisms.UDP, ARP, and DHCP are not connection-oriented protocols.

2. True or false. UDP traffic accepts the loss of some data.

UDP (User Datagram Protocol) traffic accepts the loss of some data. Unlike TCP (Transmission Control Protocol), which ensures reliable and ordered data delivery by retransmitting lost or corrupted packets, UDP is a connectionless protocol that does not provide such guarantees. It is often used for applications where low overhead and minimal latency are more important than guaranteed delivery, such as real-time audio or video streaming, online gaming, and DNS (Domain Name System) queries. In these cases, a small amount of data loss can be tolerated without significant impact on the user experience.

3. What type of traffic commonly uses UDP? (Choose all that apply.)

A. Streaming audio C. HTTP traffic
B. Streaming video D. Voice over IP
UDP (User Datagram Protocol) is commonly used for real-time and multimedia applications where low latency and minimal delay are critical. This includes streaming audio and video as well as Voice over IP (VoIP) communication. These types of traffic can tolerate some packet loss and are more concerned with maintaining a smooth flow of data and minimizing delays rather than ensuring every packet is delivered.

4. What is used to resolve an IP address to a MAC address?
A. DNS C. ARP
B. TCP D. ICMP
ARP (Address Resolution Protocol) is used to resolve an IP address to a MAC (Media Access Control) address within a local network. It helps devices on the same network identify each other's hardware addresses, enabling data to be properly delivered at the data link layer. ARP is an essential part of local network communication.

5. List three commonly used protocols for email.
SMTP (Simple Mail Transfer Protocol): SMTP is used for sending outgoing email messages from a client to a server or between email servers. It handles the routing and delivery of email messages.

POP3 (Post Office Protocol version 3): POP3 is used by email clients to retrieve email messages from a mail server. It allows users to download messages to their local devices, usually removing them from the server.

IMAP (Internet Message Access Protocol): IMAP is another protocol for retrieving email messages from a mail server. Unlike POP3, IMAP allows users to view, organize, and manage their email messages on the server, which can be accessed from multiple devices.

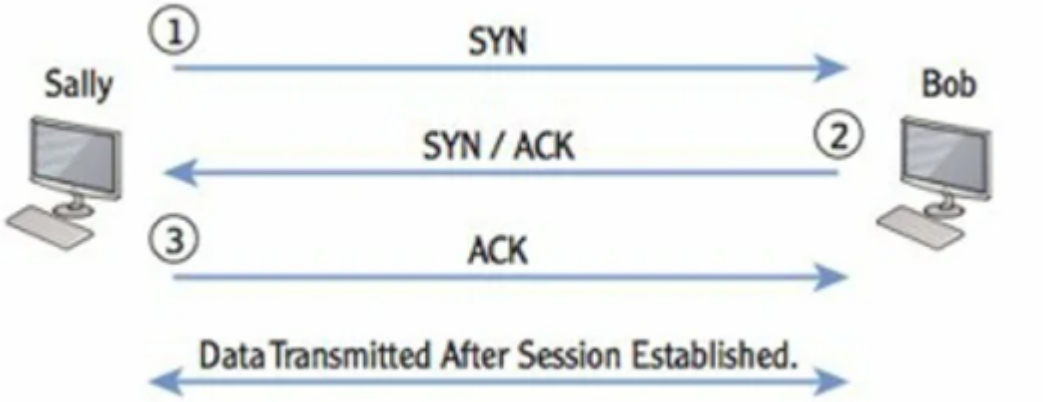
6. L2TP is one of many tunneling protocols used for VPNs. What is used to encrypt L2TP traffic?
L2TP (Layer 2 Tunneling Protocol) itself does not provide encryption. Instead, it is often used in conjunction with IPsec (Internet Protocol Security) to encrypt the traffic passing through the VPN tunnel. IPsec provides the encryption and security features needed to protect data transmitted over the VPN connection.

7. The _____ protocol is used to manage multicast transmissions. Internet Group Multicast Protocol (IGMP)
IGMP is used to manage multicast transmissions in a network. It allows hosts to join or leave multicast groups and informs routers about the multicast group memberships of hosts on their attached networks.

8. What port is used by RDS
A. 389
B. 636
C. 1701
D. 3389

9. What port is used by LDAP?
A. 25
B. 389
C. 1723
D. 3389

10. What port is used by Kerberos?
A. 25 B. 80
C. 88 D. 443



Port	TCP or UDP	Protocol	Comments
20, 21	TCP	FTP	File Transfer Protocol.
22	TCP	SSH	Secure Shell.
23	TCP	Telnet	Can be secured with SSH.
25	TCP	SMTP	Simple Mail Transfer Protocol. Used to send email.
110	TCP	POP3	Post Office Protocol. Used to receive email.

143	TCP	IMAP4	Internet Message Access Protocol. Used when email stored on server.
80	TCP	HTTP	Hypertext Transfer Protocol. Used for web pages.
443	TCP	HTTPS	Secure HTTPS. Commonly uses SSL for security.
53	TCP/UDP	DNS	Domain Name Service. Used to resolve names to IP addresses.
88	TCP	Kerberos	Primary authentication protocol used by Active Directory.
389	TCP	LDAP	Lightweight Directory Access Protocol (LDAP). Language used to communicate with Active Directory.
636	TCP	SLDAP	Secure LDAP. Uses SSL or TLS to encrypt LDAP communications.
161, 162	UDP	SNMP	Simple Network Management Protocol. Used to manage network devices such as routers and switches.
3389	TCP	Remote Desktop Services	Remote Desktop Services are used for remote assistance and remote desktops in a Microsoft network.
1723	TCP	PPTP	Point-to-Point Tunneling Protocol. Used in VPNs.
1701	UDP	L2TP	Layer 2 Tunneling Protocol. Used in VPNs.

Chapter 5
REVIEW QUESTIONS

1. Which of the following addresses is a valid IPv4 address?

A. 192.168.1.256 C. 2001:0000:4137:9e76:3c2b:05ad:3f57:fe98
B. 10.1.25.2 D. 2001:0000:4137:9g76:3c2b:05zd:3x57:gh98

2. What class is the following IP address: 192.168.1.5?

A. Class A C. Class C
B. Class B D. Class D

Class A IP addresses typically start with a number between 1 and 126. Example: 10.0.0.1
Class B IP addresses usually start with a number between 128 and 191. Example: 172.16.0.1

Class C IP addresses commonly start with a number between 192 and 223. Example: 192.168.0.1
Class D IP addresses are reserved for multicast groups and typically start with a number between 224 and 239.
So, in this case, the IP address 192.168.1.5 is in Class C. Remember, Class C IP addresses are often used for local area networks (LANs) and are ideal for small to medium-sized networks.

3. True or false.The following two classful IP addresses have the same network ID: 192.168.1.5 and 192.168.2.6
The network ID is determined by the first three segments of the IP address in classful IP addressing. Since the third segment is different in 192.168.1.5 and 192.168.2.6, they belong to different network IDs.

In classful addressing, the network ID is determined by the address class (A, B, C), and the first few segments of the IP address, typically the first three segments in the case of Class C addresses.
IP Address: 192.168.1.5

Network ID: 192.168.1.0
Host ID: 0.0.0.5
IP Address: 192.168.2.6

Network ID: 192.168.2.0
Host ID: 0.0.0.6
As you can see, the network IDs are different because they are determined by the first three segments, and in this case, the third segment is different. The host IDs are unique to each device within the respective network.

4. True or false.The following two classful IP addresses have the same network ID: 10.80.4.2 and 10.81.15.2
The two classful IP addresses, 10.80.4.2 and 10.81.15.2, have different network IDs. The network ID is determined by the first segment of the IP address, and in this case, the first segments are 10 and 10, but the second segments are different (80 and 81). So, they belong to different networks.

6. What is the subnet mask for the following IP address: 192.168.1.5 /26?
A. 192.168.1.5 C. 255.255.255.192
B. 255.255.255.0 D. 255.255.255.240

The subnet mask for the IP address 192.168.1.5/26 is 255.255.255.192.

Here's a memory trick to help you remember this:

In a /26 subnet, there are 6 bits reserved for the network part of the IP address, leaving 2 bits for the host part. To find the subnet mask, you can write it in binary form: 11111111.11111111.11111111.11000000. Each "1" represents a bit in the subnet mask, and each "0" represents a bit in the host part.

Now, let's convert this binary mask to decimal:

The first three octets (24 bits) are all "1," so they are 255 in decimal.
The last octet has two "1" bits and six "0" bits, which is equivalent to 128 + 64 = 192.
So, the subnet mask is 255.255.255.192.

7. Which of the following IP addresses is in one of the reserved IP address ranges defined by RFC 1918?
A. 10.80.256.1 C. 192.169.4.5
B. 172.17.34.14 D. 224.17.2.5

8. How many hosts are supported in subnet with a network ID of 192.168.1.128 /26?
A. 30 C. 62
B. 32 D. 64
To determine how many hosts are supported in a subnet with a network ID of 192.168.1.128/26, we need to calculate the number of host addresses within that subnet.

A /26 subnet has 64 IP addresses. This is because a /26 subnet has 6 bits available for host addresses (32 - 26 = 6). With 6 bits, you can represent 2^6 = 64 unique combinations.

However, in any given subnet, two IP addresses are reserved: one for the network address (192.168.1.128 in this case) and one for the broadcast address (192.168.1.191 in this case).

So, to calculate the number of usable host addresses:

64 (total addresses) - 2 (reserved addresses) = 62 usable host addresses.

So the answer is C. 62 hosts are supported in this subnet.

To remember this, you can think of the 2 addresses reserved for network and broadcast, leaving 62 addresses for hosts in a /26 subnet.

9. True or false.The following two classless IP addresses have the same network ID: 192.168.1.105 /26 and 192.168.1.136 /26.
In IPv4, a subnet mask specifies the network portion of an IP address. The /26 subnet mask means the first 26 bits are dedicated to the network, and the remaining 6 bits are for host addresses.

For the two IP addresses, 192.168.1.105 /26 and 192.168.1.136 /26, they both share the same first 26 bits, which is 192.168.1. Their host portions (the last 6 bits) are different: 105 in binary is 01101001, and 136 in binary is 10001000.

Since the network portion is the same and the subnet mask is identical (/26), these two IP addresses belong to the same subnet and therefore have the same network ID.

This is why it's true that these classless IP addresses have the same network ID.

10. A computer is unable to communicate with other computers on the network.You use ipconfig and see the following information: IP address: 169.254.5.7 Subnet mask: 255.255.0.0 Default gateway: blank
DNS server: blank
A. A DHCP server can’t be reached.
B. The default gateway needs to be manually configured.
C. The DNS server IP address needs to be manually configured.
D. None of the above.

This situation is indicative of an APIPA (Automatic Private IP Addressing) address. When a computer can't obtain an IP address from a DHCP server, it will assign itself an address in the range of 169.254.0.1 to 169.254.255.254. Since the IP address is in this range and the default gateway and DNS server fields are blank, it suggests that the computer couldn't reach a DHCP server to obtain a valid IP address, gateway, and DNS information.

Chapter 6
REVIEW QUESTIONS

1. Which of the following addresses is a valid IPv6 address?
A. 192.168.1.256 C. 2001:0000:4137:9e76:3c2b:05ad:3f57:fe98 B. 10.1.25.2 D. 2001:0000:4137:9g76:3c2b:05zd:3x57:gh98
IPv6 addresses are represented using hexadecimal characters and colons as separators. The provided address follows the correct format for an IPv6 address.

2. You need to manually assign an IPv6 address to a client computer for use within a private network. Which one of the following addresses should you use?
A. 0000::a123:4567:89ab:cdef D. fe80:: a123:4567:89ab:cdef B. 2001:0001::fcde:ba98:7654 E. fd00:: a123:4567:89ab:cdef C. 2001:0000: fcde:ba98:7654
The prefix "fd00" is reserved for ULA, and the rest of the address can be used for your private network. This ensures uniqueness within your private network and is not routable on the public internet.

3. Which of the following features is built into IPv6 to provide extra security?
A. Teredo tunneling C. Unique local addresses
B. Global addresses D. IPSec
IPSec (Internet Protocol Security) is built into IPv6 to provide extra security. It offers features like authentication, encryption, and data integrity to protect communication over IPv6 networks. Teredo tunneling, global addresses, and unique local addresses are not security features but rather address assignment and routing mechanisms in IPv6.

4. True or false. An IPv6 address with a prefix of fd is a link-local address.
An IPv6 address with a prefix of fd is typically a unique local address (ULA) and not a link-local address. Link-local addresses usually start with fe80. Unique local addresses (ULAs) are meant for local communications within a single site and are not automatically generated, unlike link-local addresses.

5. What IPv6 to IPv4 technology uses tunneling to encapsulate an IPv6 packet within an IPv4 packet?
The IPv6 to IPv4 technology that uses tunneling to encapsulate an IPv6 packet within an IPv4 packet is "6to4 tunneling." This allows IPv6 traffic to be transmitted over an IPv4 network, helping in the transition from IPv4 to IPv6.

6. You need to assign IPv6 addresses to hosts on a private network.You should use _____ addresses.
You should use "Unique Local Addresses" (ULA) for assigning IPv6 addresses to hosts on a private network. ULAs are designed for local communication within an organization and are not globally routable, making them suitable for private networks.

7. What IPv6 protocol is used to identify routers on the same network?
A. Network Discovery C. IGMP

B. Teredo **D. Anycast**

8. IPv4 addresses use public address on the Internet. IPv6 uses ___global__ addresses on the Internet.