2.1.10 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 1/28/2025, 8:21:44 PM • **Time Spent:** 03:57

Score: 100%

Passing Score: 80%

Question 1 ✓ Correct

What is the purpose of a network model?

→ ● Standardize processes at each layer.

○ Provide the logical addressing required to locate your destination node.

○ Used to remotely access application on remote systems.

○ Provide an interface for submitting web requests.

Explanation

The purpose of a network model is to standardize processes at each layer so that the receiving system can make sense of what was sent. This includes data security, addressing, and formatting.

The browser's job is to provide you an interface for submitting web requests.

Telnet is used to either remotely access applications on remote systems or connect to a Cisco device remotely to reconfigure it.

The Internet Protocol (IP) provides the logical addressing required to locate your destination node.

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipoverview_ccna7\q_tcpipoverview_01_ccna7.question.xml

Question 2 ✓ Correct

Which of the following are limitations of the TCP/IP model? (Select two.)

□ Forces modularity in networking features.

□ Does not aid in troubleshooting.

→ ☑ TCP/IP layers are theoretical and do not actually perform real functions.

→ ☑ A particular protocol implementation may not represent every layer.

□ Divides networking tasks into logical layers.

Explanation

You must remember the following limitations of the TCP/IP model:

- TCP/IP layers are theoretical and do not actually perform real functions.
- Industry implementations rarely have a layer-to-layer correspondence with the TCP/IP layers.
- Different protocols within the stack perform different functions, which help send or receive the overall message.
- A particular protocol implementation may not represent every layer (or it may spread across multiple layers).

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipoverview_ccna7\q_tcpipoverview_02_ccna7.question.xml

Question 3.

✓ Correct

Match the layers of the TCP/IP model to the corresponding layers of the OSI model. (Each option may be used more than once.)

Application

✓ Application

Presentation

✓ Application

Session

✓ Application

Transport

✓ Transport

Network

✓ Internet

Data Link

✓ Link

Physical

✓ Link

Explanation

The Application layer (also called the Process-to-Process layer) corresponds to the Session, Presentation, and Application layers of the OSI model.

The Transport layer (also called the Host-to-Host layer) is comparable to the Transport layer of the OSI model and is responsible for error checking and reliable packet delivery. At this layer, the data stream is broken into segments that must be assigned sequence numbers so that the segments can be reassembled correctly on the remote side.

The Internet layer is comparable to the Network layer of the OSI model. It is responsible for moving packets through a network. This involves the addressing of hosts and making routing decisions to identify how the packet traverses the network.

The Link layer corresponds to the functions of the Physical and Data Link layers of the OSI model. It is responsible for describing the physical layout of the network and how messages are formatted on the transmission medium. Sometimes, this layer is divided into the Data Link and Physical layers.

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

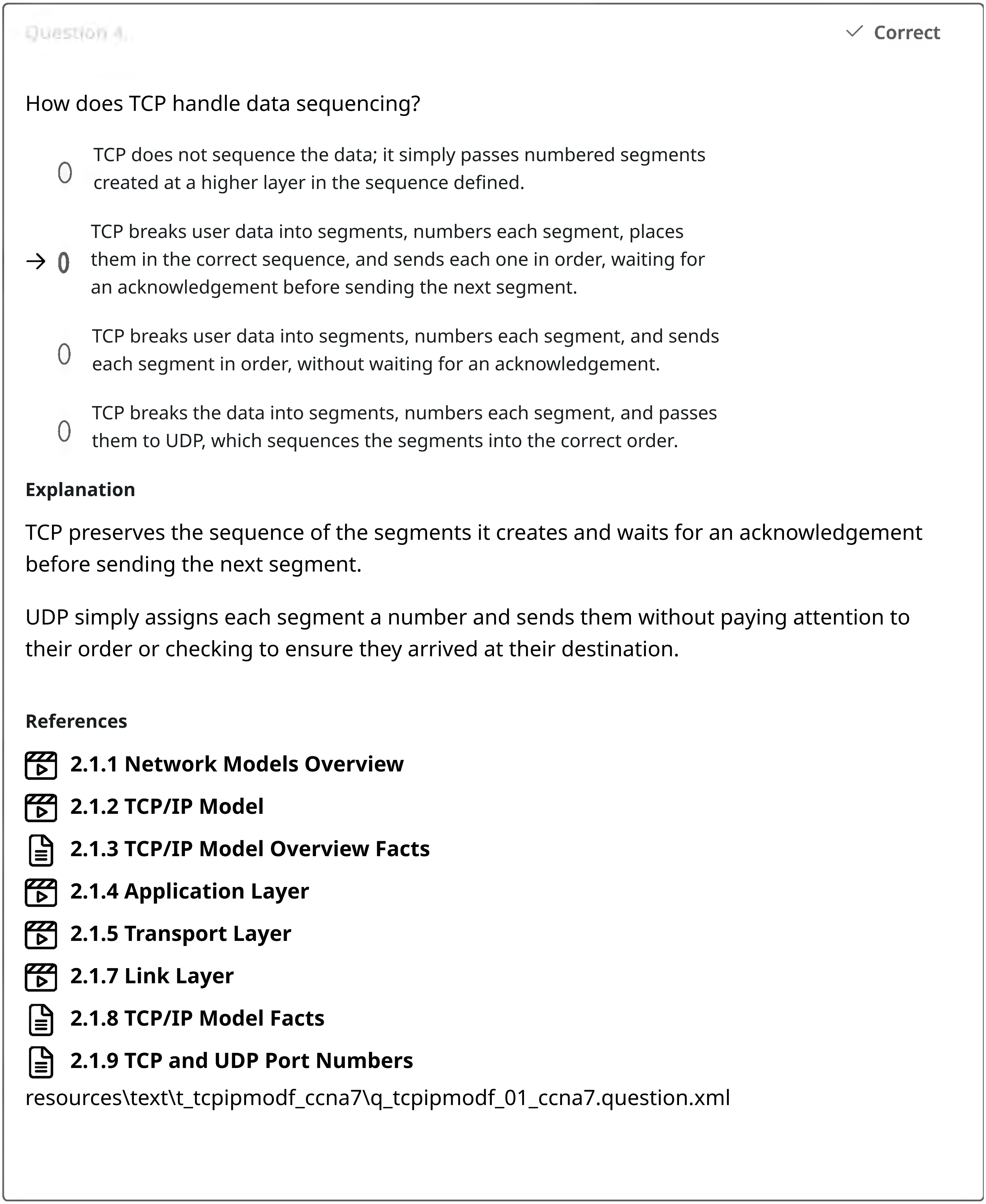
2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipoverview_ccna7\q_tcpipoverview_03_ccna7.question.xml



Question 4.

✓ Correct

How does TCP handle data sequencing?

○ TCP does not sequence the data; it simply passes numbered segments created at a higher layer in the sequence defined.

→ ● TCP breaks user data into segments, numbers each segment, places them in the correct sequence, and sends each one in order, waiting for an acknowledgement before sending the next segment.

○ TCP breaks user data into segments, numbers each segment, and sends each segment in order, without waiting for an acknowledgement.

○ TCP breaks the data into segments, numbers each segment, and passes them to UDP, which sequences the segments into the correct order.

Explanation

TCP preserves the sequence of the segments it creates and waits for an acknowledgement before sending the next segment.

UDP simply assigns each segment a number and sends them without paying attention to their order or checking to ensure they arrived at their destination.

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipmodf_ccna7\q_tcpipmodf_01_ccna7.question.xml

Question 5 ✓ Correct

Which of the following methods helps to detect lost packets? (Select two.)

→ ☑ Sequencing

□ Buffering

→ ☑ Acknowledgements

□ CRC

□ Flow control

Explanation

Lost packets can be detected using sequencing or acknowledgements:

- Sequencing assigns a number to each packet. A missing sequence number in received packets indicates a lost packet.
- The receiving device sends acknowledgements to notify the sending device of received packets. If an acknowledgement is not received by the sending device, it assumes a lost packet and retransmits.

Flow control is the mechanism for controlling how much data is sent at a time. Various mechanisms exist for speeding up or slowing down the data transfer rate.

A Cyclical Redundancy Check (CRC) is a mathematical calculation added to each frame. The CRC detects errors in received frames.

Buffering is a method of holding data that needs to be sent. Buffering can be used in flow control to hold packets that cannot yet be transmitted.

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipmodf_ccna7\q_tcpipmodf_02_ccna7.question.xml

Question 6

✓ Correct

Which of the following lists accurately describes TCP and UDP? (Select two.)

→ ☑ TCP: connection-oriented, reliable, sequenced, high overhead

□ UDP: connection-oriented, reliable, sequenced, high overhead

□ TCP: connection-oriented, reliable, unsequenced, low overhead

□ UDP: connectionless, reliable, sequenced, low overhead

→ ☑ UDP: connectionless, unreliable, unsequenced, low overhead

□ TCP: connectionless, unreliable, unsequenced, low overhead

Explanation

TCP and UDP are both Transport and Host-to-Host level protocols, but they have different characteristics.

TCP characteristics include:

- Connection-oriented
- Reliable
- Sequenced
- High overhead

UDP characteristics include:

- Connectionless
- Unreliable
- Unsequenced
- Low overhead

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipmodf_ccna7\q_tcpipmodf_03_ccna7.question.xml

Question 7

✓ Correct

Match each layer of the TCP/IP model to its functions. (Each layer matches with two functions.)

Is responsible for how messages are electrically transmitted.

✓ Link

Is responsible for forwarding packets through multiple networks.

✓ Internet

Is responsible for describing the physical layout of the network.

✓ Link

Is responsible for error checking and reliable delivery.

✓ Transport

Is not concerned with reliable delivery of information.

✓ Internet

Integrates network functionality into the host operating system.

✓ Application

Provides the capability for services to operate on the network.

✓ Application

Uses ports to enable application-to-application communications between hosts.

✓ Transport

Explanation

The Application layer contains high-level protocols used by processes (applications) running on a host for network communications. The Application layer integrates network functionality into the host operating system and enables network services. The Application layer does not include specific applications that provide services, but rather provides the capability for services to operate on the network.

The Transport layer is responsible for error checking and reliable delivery. The Transport layer also uses ports to enable application-to-application communications between hosts.

The Internet layer is responsible for forwarding packets through multiple networks. This process is called routing. The Internet layer manages the host addressing and routing decisions to identify how packets traverse networks. The Internet layer is not concerned with reliable delivery of information. Instead, it relies on the Transport layer to establish a host-to-host communication channel and ensure information arrives correctly at the destination host.

The Link layer is responsible for describing the physical layout of the network and how messages are electrically transmitted. It is used to move information between hosts by controlling how individual bits are transmitted and received on the network medium.

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipmodf_ccna7\q_tcpipmodf_04_ccna7.question.xml

Question 8 ✓ Correct

An internet server has a single network interface that has been assigned an IP address. The server is running both the FTP and HTTP services. A client computer initiates a session with the HTTP server.

How is the HTTP request from the client routed to the correct service running on the server?

○ IP address

○ Sequence number

→ ● Port or socket number

○ Routing Information Protocol (RIP)

○ Session ID

Explanation

Port or socket numbers are used to identify a service running on the server. For example, FTP uses ports 20 and 21 to send communications to the FTP service running on the server, while port number 80 is used for HTTP.

Sequence numbers are used in packets to make sure that packets can be reassembled in the proper order and identify lost packets. The IP address identifies a network interface. Communication instances within the same service but between different clients (or multiple instances with the same client) are kept separate by session IDs. Routing Information Protocol (RIP) is a routing protocol for routing data through an internetwork.

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_com_port_ccna7\q_com_port_01_ccna7.question.xml

Question 9 ✓ Correct

The TCP/IP protocol stack uses port numbers to determine protocol use. Port usage is regulated by the Internet Corporation for Assigning Names and Numbers (ICANN). Which of the following are characteristics of registered ports? (Select two.)

☐ Has port numbers ranging from 0 to 1023.

→ ☑ Has port numbers ranging from 1024 to 49151.

☐ Assigned for specific protocols and services.

☐ Has port numbers ranging from 49152 to 65535.

→ ☑ Is assigned by ICANN for a network service.

Explanation

A registered port:

- Is assigned by ICANN for a network service.
- Has port numbers ranging from 1024 to 49151.

A well-known port is:

- Assigned for specific protocols and services.
- Has port numbers ranging from 0 to 1023.

A dynamic port:

- Is assigned when a network service establishes contact and released when the session ends.
- Allows applications to listen to the assigned port for other incoming requests. Traffic for a protocol can be received through a port other than the port which the protocol is assigned. This requires that the destination application or service is listening for that type of traffic on that port.
- Has port numbers ranging from 49152 to 65535.

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_com_port_ccna7\q_com_port_02_ccna7.question.xml

Question 10 ✓ Correct

Match each TCP and/or UDP ports to the service that uses it.

Dynamic Host Configuration Protocol (DHCP)

✓ UDP ports 67 and 68

Network News Transport Protocol (NNTP)

✓ TCP Port 119

Simple Network Management Protocol (SNMP)

✓ UDP ports 161 and 162

Domain Name System

✓ TCP and UDP port 53

Telnet

✓ TCP and UDP port 23

Trivil File Transfer Protocol (TFTP)

✓ UDP port 69

Explanation

TCP and UDP use port 23 for Telnet

TCP and UDP use port 53 for Domain Name System (DNS)

UDP uses ports 67 and 68 for Dynamic Host Configuration Protocol (DHCP)

UDP uses port 69 for Trivial File Transfer Protocol (TFTP)

TCP uses port 119 for Network News Transport Protocol (NNTP)

UDP uses ports 161 and 162 usually for Simple Network Management Protocol (SNMP)

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_com_port_ccna7\q_com_port_03_ccna7.question.xml

2.2.7 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 1/28/2025, 8:53:14 PM • **Time Spent:** 03:42

Score: 100%

Passing Score: 80%

Question 1

✓ Correct

Put the OSI model layers in order.

Layer 7

✓ Application

Layer 6

✓ Presentation

Layer 5

✓ Session

Layer 4

✓ Transport

Layer 3

✓ Network

Layer 2

✓ Data Link

Layer 1

✓ Physical

Explanation

Layer	Name	Mnemonic (Top-down)	Mnemonic (Bottom-up)
Layer 7	Application	All	Away
Layer 6	Presentation	People	Pizza
Layer 5	Session	Seem	Sausage
Layer 4	Transport	To	Throw
Layer 3	Network	Need	Not
Layer 2	Data Link	Data	Do
Layer 1	Physical	Processing	Please

References

2.2.3 OSI Model Facts

resources\text\t_osimod_ccna7\q_osimod_01_ccna7.question.xml

Question 2 ✓ Correct

Which of the following are limitations of the OSI model? (Select two.)

→ ☑ A particular protocol implementation may not represent every OSI layer.

□ A particular protocol implementation must represent every OSI layer

□ Requires specialization of features at different levels.

→ ☑ OSI layers are theoretical and do not actually perform real functions.

□ OSI layers are not theoretical and actually perform real functions.

Explanation

The following are limitations of the OSI model:

- OSI layers are theoretical and do not actually perform real functions.
- Industry implementations rarely have a layer-to-layer correspondence with the OSI layers.
- Different protocols within the stack perform different functions that help send or receive the overall message.
- A particular protocol implementation may not represent every OSI layer (or may spread across multiple layers).

References

2.2.3 OSI Model Facts

resources\text\t_osimod_ccna7\q_osimod_02_ccna7.question.xml

Question 3: ✓ Correct

Which of the following are functions of the MAC sublayer in the OSI model? (Select two.)

- → ☑ Letting devices on the network have access to the LAN.
- ☐ Mapping hardware addresses to link-layer addresses.
- → ☑ Defining a unique hardware address for each device on the network.
- ☐ Maintaining orderly delivery of frames through sequencing.
- ☐ Creating routing tables based on MAC addresses.

Explanation

The MAC sublayer in the OSI model defines a unique MAC or data-link address for each device on the network. This address is usually assigned by the manufacturer. The MAC sublayer also provides devices with access to the network media.

Mapping hardware addresses to link-layer addresses and creating routing tables based on MAC addresses are not functions of the MAC sublayer.

Maintaining orderly delivery of frames through sequencing occurs at the Logical Link Control layer.

References

2.2.4 OSI Layer Summary

resources\text\t_ositable_ccna7\q_ositable_01_ccna7.question.xml

Question 4

✓ Correct

Which two of the following functions are performed by IP? (Select two.)

□ Creating multicast groups.

□ Delivering IP addresses to hosts.

□ Discovering the MAC address of a host.

→ ☑ Routing datagrams to their destination.

→ ☑ Identifying hosts with the IP address.

Explanation

IP is responsible for moving data through the network. It identifies devices by their IP addresses and routes datagrams based on this address. The other functions listed here are performed by other protocols in the TCP/IP suite.

References

2.2.4 OSI Layer Summary

resources\text\t_ositable_ccna7\q_ositable_02_ccna7.question.xml

Question 5

✓ Correct

A client computer starts to download some files from an FTP server named FTPsvr1. While the first download is in progress, the user opens a second instance of the FTP program and initiates a second download.

What do the server and the client use to keep each download separate?

○ Sequence numbers

○ CRC

○ IP Address

○ Port or socket numbers

→ ● Session ID

Explanation

Communication instances are kept separate by session IDs. Each communication instance is identified with a session ID.

Port or socket numbers are used to identify a service running on the server. For example, FTP uses ports 20 and 21 to send communications to the FTP service running on the server. Both sessions would use the same port number(s) to communicate.

Sequence numbers are used in packets to make sure that packets can be reassembled in the proper order and to identify lost packets.

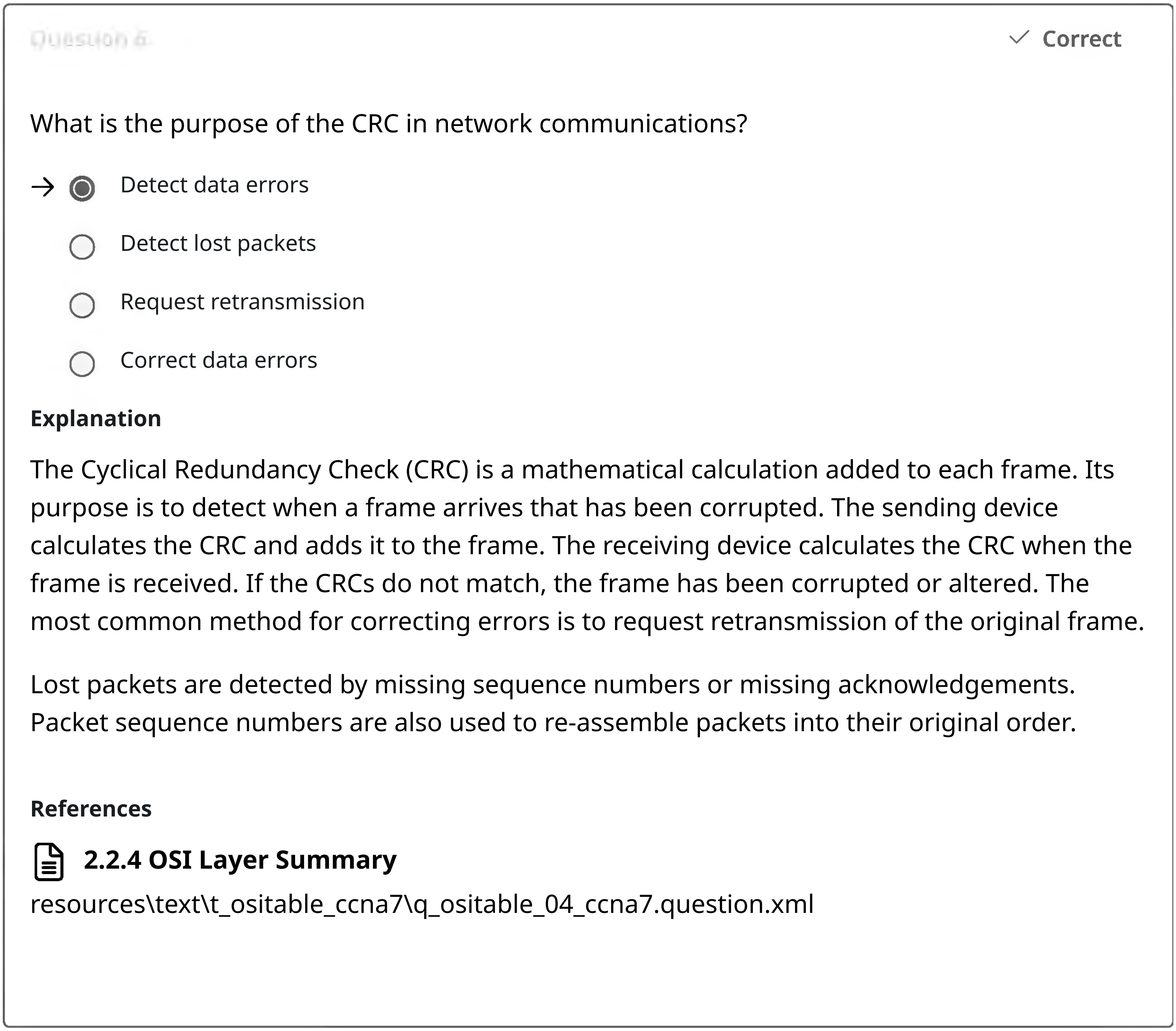
The Cyclical Redundancy Check (CRC) is used in a packet or a frame to identify errors within the packet or the frame.

The IP address identifies a network interface.

References

2.2.4 OSI Layer Summary

resources\text\t_ositable_ccna7\q_ositable_03_ccna7.question.xml



Question 6

✓ Correct

What is the purpose of the CRC in network communications?

→ ● Detect data errors

○ Detect lost packets

○ Request retransmission

○ Correct data errors

Explanation

The Cyclical Redundancy Check (CRC) is a mathematical calculation added to each frame. Its purpose is to detect when a frame arrives that has been corrupted. The sending device calculates the CRC and adds it to the frame. The receiving device calculates the CRC when the frame is received. If the CRCs do not match, the frame has been corrupted or altered. The most common method for correcting errors is to request retransmission of the original frame.

Lost packets are detected by missing sequence numbers or missing acknowledgements. Packet sequence numbers are also used to re-assemble packets into their original order.

References

2.2.4 OSI Layer Summary

resources\text\t_ositable_ccna7\q_ositable_04_ccna7.question.xml

Question 7

✓ Correct

The following items describe the functions performed at various OSI model layers:

1. Logical topology, hardware addresses, media access, framing
2. Logical device identification, path identification, and selection
3. Flow control, reliable data transfer, windowing, segmentation, and sequencing
4. Converting data to 0s and 1s, bit signaling, and synchronization

Which of the following correctly identifies, in order, the layers that perform each of the functions listed here?

○ Network, Transport, Physical, Data Link

○ Network, Data Link, Transport, Physical

○ Transport, Network, Physical, Data Link

→ ● Data Link, Network, Transport, Physical

○ Physical, Transport, Network, Data Link

Explanation

The following OSI model layers correspond to the following functions:

- Data Link: Logical topology, hardware addresses, media access, framing
- Network: Logical device identification, path identification, and selection
- Transport: Flow control, reliable data transfer, windowing, segmentation, and sequencing
- Physical: Converting data to 0s and 1s, bit signaling, and synchronization

References

2.2.4 OSI Layer Summary

resources\text\t_ositable_ccna7\q_ositable_05_ccna7.question.xml

Question 8

✓ Correct

Drag the information type on the left to the appropriate layer of the OSI model that it is associated with on the right.

Network Layer

✓ Packets

Data Link Layer

✓ Frames

Physical Layer

✓ Bits

Transport Layer

✓ Segments

Application Layer

✓ Data

Explanation

Encapsulation is the process of breaking a message into packets, adding control and other information, and transmitting the message through the transmission media. You need to know the following four-step data encapsulation process on the sending system using the OSI model:

- The Application layer prepares the data to be sent through the network.
- The Transport layer breaks the data into pieces called segments adding sequencing and control information.
- The Network layer converts the segments into packets, adding logical network and device addresses.
- The Data Link layer converts the packets into frames, adding physical device addressing information.
- The Physical layer converts the frames into bits for transmission across the transmission media.

References

2.2.4 OSI Layer Summary

resources\text\t_ositable_ccna7\q_ositable_06_ccna7.question.xml

Question 9 ✓ Correct

Match the TCP/IP protocols with their functions.

Used to send email messages between mail servers.

✓ SMTP

Used to send messages to groups of users.

✓ IGMP

Used to assign IP addresses to hosts.

✓ DHCP

Used to get the MAC address of a host from its IP address.

✓ ARP

Explanation

The Simple Mail Transfer Protocol (SMTP) is used to route electronic mail between mail servers.

Internet Group Membership Protocol (IGMP) is a protocol for defining host groups. All group members can receive broadcast messages intended for the group (called multicasts).

The Dynamic Host Configuration Protocol (DHCP) is used for delivering IP information to connected devices configured to use DHCP or automatic addressing.

The Address Resolution Protocol (ARP) is used to get the MAC address of a host from a known IP address. ARP is used within a subnet to get the MAC address of a device on the same subnet as the requesting device.

The Internet Control Message Protocol (ICMP) works closely with IP to provide error and control information that helps move data packets through the internetwork.

The Simple Network Management Protocol (SNMP) is used to manage networks. SNMP lets network devices exchange configuration and status information. This information can be gathered by management software and used to monitor and manage the network.

References

2.2.6 TCP/IP Protocol Suite Facts

resources\text\t_ipprotocols_ccna7\q_ipprotocols_01_ccna7.question.xml

Question 10

✓ Correct

Match the TCP/IP protocols with their functions.

Group 1

Used to get the IP address of a host from a known MAC address.

✓ RARP

✓ BOOTP

Group 2

Used to transfer files.

✓ FTP

✓ TFTP

Group 3

Used to identify routes through an internetwork.

✓ RIP

✓ OSPF

Explanation

Both BOOTP (Bootstrap Protocol) and RARP (Reverse Address Resolution Protocol) are used to discover the IP address of a device with a known MAC address. BOOTP is an enhancement to RARP, and it is more commonly implemented than RARP. As its name implies, BOOTP is used by computers as they boot to receive an IP address from a BOOTP server. The Address Resolution Protocol (ARP) is used to get the MAC address of a host from a known IP address.

Both the File Transfer Protocol (FTP) and the Trivial File Transfer Protocol (TFTP) are used for transferring files. FTP uses TCP to guarantee delivery, while TFTP uses UDP for fast data transfer. The Hypertext Transfer Protocol (HTTP) is used by web browsers and web servers to exchange files (such as web pages) through the World Wide Web and intranets.

Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) are routing protocols. Routing protocols discover the path through an internetwork and are used to select the best path through an internetwork.

Transmission Control Protocol (TCP) provides connection-oriented services and performs segment sequencing and service addressing. It also performs important error-checking functions and is considered a host-to-host protocol.

References

2.2.6 TCP/IP Protocol Suite Facts

2.3.5 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)

Date: 1/29/2025, 8:57:02 AM • **Time Spent:** 02:54

Score: 100%

Passing Score: 80%

Question 1.

✓ Correct

You need to connect several network devices together using twisted pair Ethernet cables. Assuming Auto-MDIX is *not* enabled on these devices, drag the appropriate type of cabling on the left to each connection type on the right.

Workstation to switch

✓ Straight-through Ethernet cable

Router to switch

✓ Straight-through Ethernet cable

Switch to switch

✓ Crossover Ethernet cable

Workstation to router

✓ Crossover Ethernet cable

Router to router

✓ Crossover Ethernet cable

Explanation

If Auto-MDI/MDIX is not enabled, then you must use a crossover Ethernet cable when connecting the following devices:

- Switch to switch
- Switch to hub
- Hub to hub
- Workstation to router
- Workstation to workstation
- Router to router

Use a straight-through Ethernet cable to connect the following devices:

- Workstation to hub
- Workstation to switch
- Router to hub
- Router to switch

References

2.3.1 Network Design Overview

2.3.2 Cables and Connectors

2.3.3 Twisted Pair Facts

2.3.4 Fiber Optic Facts

2.5.7 Ethernet Standards

2.5.8 Ethernet Standards Facts

resources\text\t_twistedpair_ccna7\q_twistedpair_01_ccna7.question.xml

Question 2 ✓ Correct

You are deploying a new 10GB Ethernet network using Cat 6 cabling.

Which of the following are true concerning this media? (Select two.)

- □ It uses twisted 18- or 16-gauge copper wiring.
- → ☑ PVC insulation surrounds each copper wire.
- □ It supports multi-mode transmissions.
- □ It is completely immune to EMI.
- → ☑ It supports 10 GB Ethernet connections.

Explanation

Cat 6 cabling supports 10-gigabit Ethernet and high-bandwidth broadband communications. It is also backwards-compatible with earlier Ethernet standards, such as 10 Mbps Ethernet. Cat 6 cables have PVC insulation that surrounds each copper wire and often include a solid plastic core that keeps the twisted pairs separated and prevents the cable from being bent too tightly.

Even though Cat 6 cabling uses a very tight twist rate, it is still susceptible to EMI. Only fiber-optic cabling is completely immune to EMI.

Cat 6 cabling typically uses 24-gauge copper wiring.

Multi-mode transmissions are associated with fiber-optic cabling.

References

2.3.1 Network Design Overview

2.3.2 Cables and Connectors

2.3.3 Twisted Pair Facts

2.3.4 Fiber Optic Facts

2.5.7 Ethernet Standards

2.5.8 Ethernet Standards Facts

resources\text\t_twistedpair_ccna7\q_twistedpair_02_ccna7.question.xml

Question 3

✓ Correct

You want to implement an Ethernet network using the 1000BaseT standard using the minimum hardware specifications possible. Which of the following should you include in your plan? (Select two.)

- □ LC connectors
- → ☑ RJ-45 connectors
- □ Cat4 twisted pair cable
- □ Cat5 twisted pair cable
- → ☑ Cat5e twisted pair cable
- □ Multi-mode fiber optic cable

Explanation

1000BaseT runs at 1 Gbps speeds over twisted pair copper cable (the T in the specification stands for twisted pair). 1000BaseT requires Cat5e cable. Use an RJ-45 connector for the cable.

Fiber optic cables use LC, ST, or SC connectors. 100BaseFX, 1000BaseSX, and 1000BaseLX are all standards that use fiber optic.

References

2.3.1 Network Design Overview

2.3.2 Cables and Connectors

2.3.3 Twisted Pair Facts

2.3.4 Fiber Optic Facts

2.5.7 Ethernet Standards

2.5.8 Ethernet Standards Facts

resources\text\t_twistedpair_ccna7\q_twistedpair_03_ccna7.question.xml

Question 4 ✓ Correct

You have a small network with two switches, SwitchA and SwitchB. MDI-X is not enabled on either switch. Each switch has three client computers connected. IP addresses have been assigned to various devices as follows:

WrkA_1, WrkA_2, and WrkA_3 are connected to SwitchA, while WrkB_4, WrkB_5, and WrkB_6 are connected to SwitchB. All of the devices are configured to operate within the same subnet.

You need to connect SwitchA and SwitchB so that workstations connected to SwitchA can communicate with workstations connected to SwitchB. What should you do?

○ Connect SwitchA and SwitchB using a straight-through cable.

○ Connect SwitchA and SwitchB to a router using a straight-through cable on each side.

→ ● Connect SwitchA and SwitchB using a crossover cable.

○ Connect SwitchA and SwitchB to a router using a crossover cable on each side.

Explanation

Because all of the devices on both switches are configured to operate within the same subnet, you can connect both switches directly together. Use a crossover cable when connecting two switches together.

Use a router to connect two switches that are in different subnets. To connect a router to a switch, use a straight-through cable.

References

2.3.1 Network Design Overview

2.3.2 Cables and Connectors

2.3.3 Twisted Pair Facts

2.3.4 Fiber Optic Facts

2.5.7 Ethernet Standards

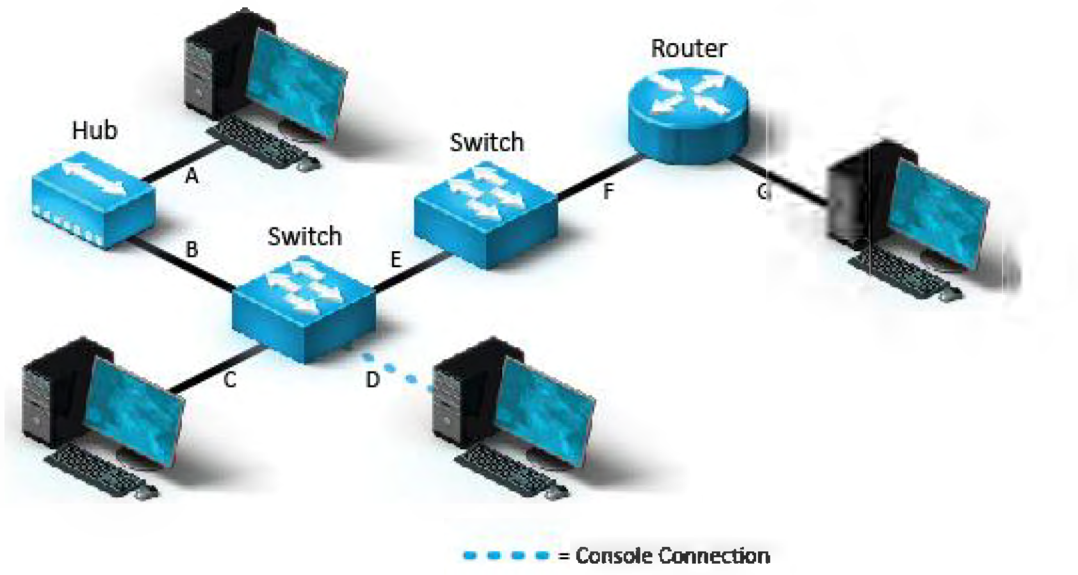
2.5.8 Ethernet Standards Facts

resources\text\t_twistedpair_ccna7\q_twistedpair_04_ccna7.question.xml

[redacted]

✓ Correct

Each connection in the image is labeled A-G. Drag the cable type from the left that you would use to make each connection type.



Connection A

✓ Ethernet straight-through cable

Connection B

✓ Ethernet crossover cable

Connection C

✓ Ethernet straight-through cable

Connection E

✓ Ethernet crossover cable

Connection F

✓ Ethernet straight-through cable

Connection G

✓ Ethernet crossover cable

Explanation

Use a straight-through Ethernet cable to connect a workstation to a hub or a switch.

Use a straight-through Ethernet cable to connect a router to a switch.

Use a crossover Ethernet cable to connect a hub or a switch to another switch.

Use a crossover Ethernet cable to connect a workstation directly to a router.

References

2.3.1 Network Design Overview

2.3.2 Cables and Connectors

2.3.3 Twisted Pair Facts

2.3.4 Fiber Optic Facts

2.5.7 Ethernet Standards

2.5.8 Ethernet Standards Facts

resources\text\t_twistedpair_ccna7\q_twistedpair_05_ccna7.question.xml

Question 6 ✓ Correct

Which pins are used in a Cat 5 Ethernet (100BASE-T) UTP cable?

○ 2, 5, 6, and 9

→ ● 1, 2, 3, and 6

○ 1, 3, 4, and 7

○ 4, 5, 7, and 8

Explanation

Cat 5 Ethernet (100BASE-T) and below (Tx is a pin used for transmitting, and Rx is a pin used for receiving):

- Pin 1: Tx+
- Pin 2: Tx-
- Pin 3: Rx+
- Pin 4: Unused
- Pin 5: Unused
- Pin 6: Rx-
- Pin 7: Unused
- Pin 8: Unused

For Cat 5e (1000BASE-T) and above, all eight pins are used for both transmitting and receiving.

References

2.3.1 Network Design Overview

2.3.2 Cables and Connectors

2.3.3 Twisted Pair Facts

2.3.4 Fiber Optic Facts

2.5.7 Ethernet Standards

2.5.8 Ethernet Standards Facts

resources\text\t_twistedpair_ccna7\q_twistedpair_06_ccna7.question.xml

Question 7 ✓ Correct

Match each characteristic on the left with the appropriate fiber optic connector on the right.

MT-RJ

✓ Metal guide pins for alignment

LC

✓ Half the size of other connectors

ST

✓ Bayonet-type connector

SC

✓ Push-on, pull-off connector

Explanation

Each fiber optic connector has the following characteristics:

- The ST connector uses a bayonet-type connector.
- The SC connector uses a separate push-on, pull-off connector with a locking tab for each wire.
- The LC connector is half the size of other fiber optic connectors.
- The MT-RJ connector uses metal guide pins to ensure proper alignment.

References

2.3.1 Network Design Overview

2.3.2 Cables and Connectors

2.3.3 Twisted Pair Facts

🗎 **2.3.4 Fiber Optic Facts**

🎬 **2.5.7 Ethernet Standards**

🗎 **2.5.8 Ethernet Standards Facts**

resources\text\t_cablefiber_ccna7\q_cablefiber_01_cna7.question.xml

Question 8 ✓ Correct

You want to implement an Ethernet network using the 100Base-FX standard and the minimum hardware specifications possible. You need to support distances of up to 1,000 meters without repeaters.

Which of the following should you include in your plan? (Select two.)

- □ Multi-mode fiber optic cable
- □ Cat5e twisted pair cable
- → ☑ SC connectors
- □ Cat5 twisted pair cable
- → ☑ Single-mode fiber optic cable
- □ RJ-45 connectors
- □ Cat4 twisted pair cable

Explanation

100BaseFX uses fiber optic cables with SC, ST, LC, or MT-RJ connectors (SC being the preferred connector). To support distances of up to 2,000 meters without repeaters, use full duplex single-mode cables. Multi-mode cables support distance of up to 412 meters without repeaters.

Twisted pair cables and RJ-45 connectors are used with 100BaseTX, 100BaseT4, and 1000BaseT Ethernet. Maximum distances are up to 100 meters when using twisted pair.

References

2.3.1 Network Design Overview

2.3.2 Cables and Connectors

2.3.3 Twisted Pair Facts

2.3.4 Fiber Optic Facts

2.5.7 Ethernet Standards

2.5.8 Ethernet Standards Facts

resources\text\t_cablefiber_ccna7\q_cablefiber_02_cna7.question.xml

Question 9 ✓ Correct

Which of the following are features of multimode fiber cable? (Select three.)

→ ☑ Supports only limited distance cable lengths

☐ Has a core diameter around 10 microns

→ ☑ Transfers data through the core using multiple light rays

☐ Supports cable lengths that extend a great distance

☐ Typically used for connecting networks between buildings

→ ☑ Has a core diameter around 50 to 100 microns

☐ Transfers data through the core using a single light ray

Explanation

Multimode fiber cable:

- Transfers data through the core using multiple light rays
- Has a core diameter around 50 to 100 microns
- Supports only limited distance cable lengths

Single-mode fiber cable:

- Transfers data through the core using a single light ray (the ray is also called a mode)
- Supports a large amount of data
- Has a core diameter around 10 microns
- Supports cable lengths that extend a great distance

References

2.3.1 Network Design Overview

2.3.2 Cables and Connectors

2.3.3 Twisted Pair Facts

2.3.4 Fiber Optic Facts

2.5.7 Ethernet Standards

2.5.8 Ethernet Standards Facts

resources\text\t_cablefiber_ccna7\q_cablefiber_03_cna7.question.xml

Question 11 ✓ Correct

Which fiber optic cable requires the exposed fiber tip to be polished as part of the assembly process?

○ RJ-45 connectors

○ Pre-polished connectors

○ Only plastic core fiber connectors

→ ● Field terminated epoxy connectors

Explanation

If a connector requires epoxy during termination in the field, the ends must be polished.

Pre-polished connectors do not require polishing during field termination.

RJ-45 is a copper wire connector and does not work with fiber-optic cables.

The connector type is what determines requirements for polishing, not the core material.

References

2.3.1 Network Design Overview

2.3.2 Cables and Connectors

2.3.3 Twisted Pair Facts

2.3.4 Fiber Optic Facts

2.5.7 Ethernet Standards

2.5.8 Ethernet Standards Facts

resources\text\t_cablefiber_ccna7\q_cablefiber_04_cna7.question.xml

2.4.6 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)

Date: 1/29/2025, 11:35:07 AM • **Time Spent:** 03:18

Score: 100%

Passing Score: 80%

Question 1 ✓ Correct

Drag the information type on the left to the appropriate layer of the TCP/IP model it is associated with on the right.

Transport Layer

✓ Segments

Link Layer

✓ Frames

Application Layer

✓ Data

Internet Layer

✓ Packets

Explanation

Encapsulation is the process of breaking a message into packets, adding control and other information, and transmitting the message through the transmission media. You need to know the following four-step data encapsulation process on the sending system using the TCP/IP model:

- The Application layer prepares the data to be sent through the network.
- The Transport layer breaks the data into pieces called segments, adding sequencing and control information.
- The Internet layer converts the segments into packets, adding logical network and device addresses.
- The Link layer converts the packets into frames, adding physical device addressing information. It also converts the frames into bits for transmission across the transmission media.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_tcpipsdu_ccna7\q_tcpipsdu_01_ccna7.question.xml

Question 2 ✓ Correct

The process of breaking a message into packets, adding control information and other information, and then transmitting the message through the transmission medium is known as __________?

○ Transformation

→ ● Encapsulation

○ Sequencing

○ Segmentation

Explanation

Encapsulation is the process of breaking a message into packets, adding control and other information, and then transmitting the message through the transmission medium.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

📄 **4.3.3 Subnet Design Facts**

🎬 **4.4.1 Route Summarization Overview**

🎬 **4.4.2 Route Summarization Network Design**

📄 **4.4.3 Route Summarization Facts**

🖥 **4.4.4 Configure Route Summarization**

📄 **4.4.5 Route Summarization Command List**

🖥 **6.2.3 Set Up Static Routing**

🎬 **6.4.1 IPv4 Routing Overview**

🎬 **6.4.2 Routing Troubleshooting Tools**

🖥 **6.4.3 Use Ping and Traceroute**

🎬 **6.4.4 Host Configuration Issues**

🎬 **6.4.5 Router Configuration Issues**

🖥 **6.4.6 Use Show Commands on the Router**

📄 **6.4.7 Troubleshooting IPv4 Routing Facts**

📄 **6.5.5 IP Troubleshooting Utility Facts**

📄 **6.5.6 IP Troubleshooting Facts**

resources\text\t_tcpipsdu_ccna7\q_tcpipsdu_02_ccna7.question.xml

Question 3. ✓ Correct

Match the TCP/IP layers with their function.

Breaks the data into pieces.

✓ Transport

Prepares the data to be sent.

✓ Application

Adds physical addesses.

✓ Link

Adds logical addresses.

✓ Internet

Explanation

1. The Application layer prepares the data to be sent through the network.
2. The Transport layer breaks the data into pieces called segments, adding sequencing and control information.
3. The Internet layer converts the segments into packets, adding logical network and device addresses.
4. The Link layer converts the packets into frames, adding physical device addressing information and a frame check sequence footer for error detection. It also converts the frames into bits (0s and 1s) for transmission across the transmission media.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

- 🎬 **4.1.3 IP Addresses**
- 🎬 **4.1.4 IP Address Format**
- 🎬 **4.1.5 IP Address Classes**
- 📄 **4.1.6 IP Address Class Facts**
- 🎬 **4.1.7 Public vs. Private IP Addresses**
- 📄 **4.1.8 Public and Private IP Address Facts**
- 🎬 **4.2.1 Subnets**
- 📄 **4.2.2 Subnet Facts**
- 🎬 **4.2.3 Subnet Math**
- 📄 **4.2.4 Subnet Math Facts**
- 🎬 **4.2.5 Variable Length Subnet Masking (VLSM)**
- 📄 **4.2.6 VLSM Facts**
- 📄 **4.2.7 Subnet Operations Facts**
- 🎬 **4.3.1 Subnet Design**
- 🖥 **4.3.2 Configure Subnets**
- 📄 **4.3.3 Subnet Design Facts**
- 🎬 **4.4.1 Route Summarization Overview**
- 🎬 **4.4.2 Route Summarization Network Design**
- 📄 **4.4.3 Route Summarization Facts**
- 🖥 **4.4.4 Configure Route Summarization**
- 📄 **4.4.5 Route Summarization Command List**
- 🖥 **6.2.3 Set Up Static Routing**
- 🎬 **6.4.1 IPv4 Routing Overview**
- 🎬 **6.4.2 Routing Troubleshooting Tools**
- 🖥 **6.4.3 Use Ping and Traceroute**
- 🎬 **6.4.4 Host Configuration Issues**
- 🎬 **6.4.5 Router Configuration Issues**
- 🖥 **6.4.6 Use Show Commands on the Router**
- 📄 **6.4.7 Troubleshooting IPv4 Routing Facts**
- 📄 **6.5.5 IP Troubleshooting Utility Facts**

6.5.6 IP Troubleshooting Facts

resources\text\t_tcpipsdu_ccna7\q_tcpipsdu_03_ccna7.question.xml

Question 4 ✓ Correct

What is the purpose of a frame check sequence (FCS) footer?

○ Control information

○ Holds segment data

○ Contains logical network addresses

→ ● Checksum error detection

Explanation

The Link layer converts the packets into frames, adding physical device addressing information and a frame check sequence footer for error detection. It also converts the frames into bits (0s and 1s) for transmission across the transmission media.

Control information is added at the Transport layer.

The Transport layer breaks the data into pieces called segments.

The Internet layer converts the segments into packets, adding logical network and device addresses.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_tcpipsdu_ccna7\q_tcpipsdu_04_ccna7.question.xml

Question 5

✓ Correct

What term does the OSI model use that is different from the TCP/IP model uses to refer to frame, packet, and segment?

→ ● Protocol data unit (PDU)

○ Session

○ IEEE Ethernet standard

○ Presentation

Explanation

The OSI model uses the term protocol data unit (PDU) instead of the terms frame, packet and segment.

Presentation and session are layers 5 and 6 of the OSI model respectively and do not correspond to the use of frame, packet, and segment in the TCP/IP model.

IEEE Ethernet standard refers to the standard that defines Ethernet.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

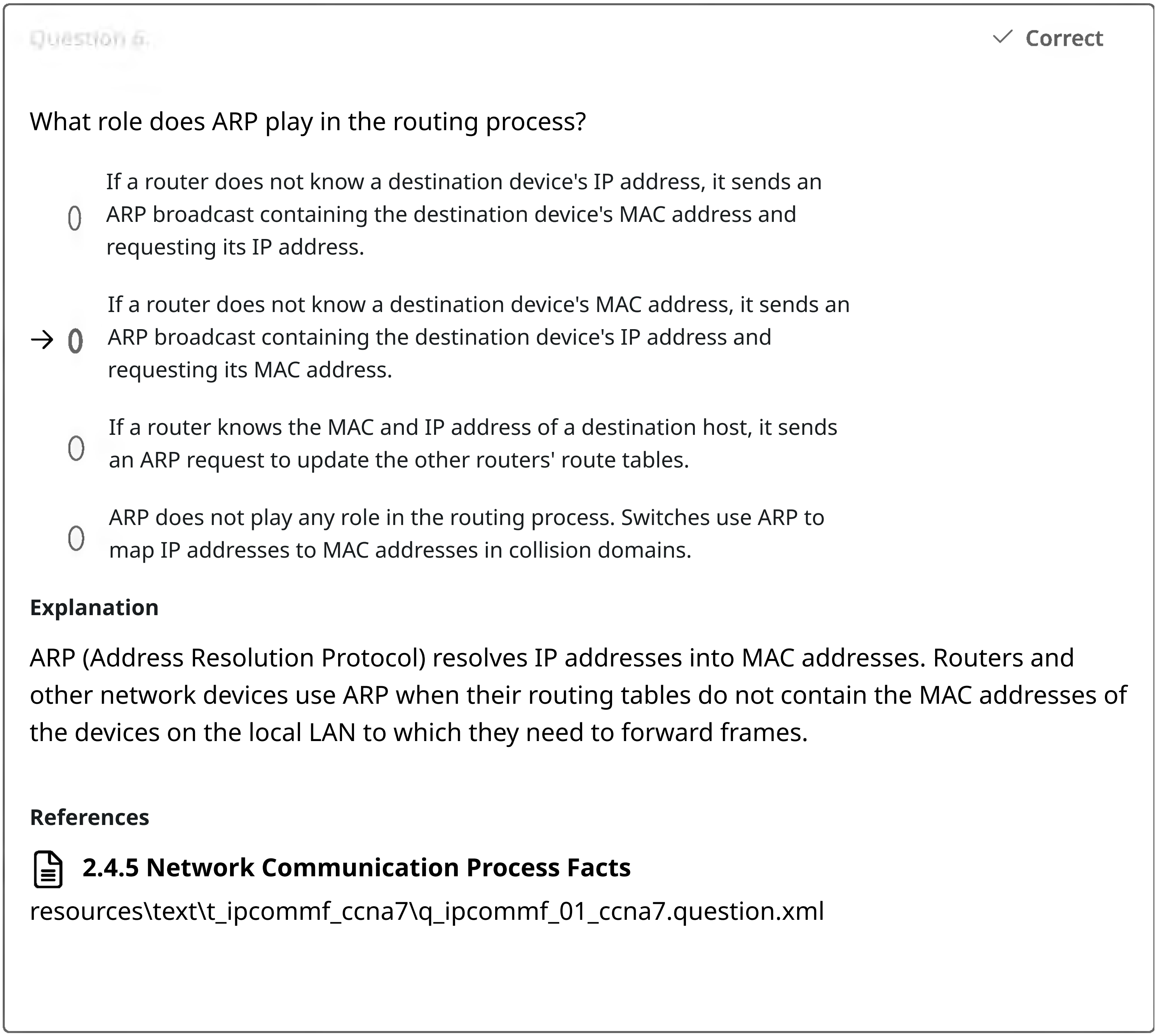
6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_tcpipsdu_ccna7\q_tcpipsdu_05_ccna7.question.xml



Question 6.

✓ Correct

What role does ARP play in the routing process?

○ If a router does not know a destination device's IP address, it sends an ARP broadcast containing the destination device's MAC address and requesting its IP address.

→ ○ If a router does not know a destination device's MAC address, it sends an ARP broadcast containing the destination device's IP address and requesting its MAC address.

○ If a router knows the MAC and IP address of a destination host, it sends an ARP request to update the other routers' route tables.

○ ARP does not play any role in the routing process. Switches use ARP to map IP addresses to MAC addresses in collision domains.

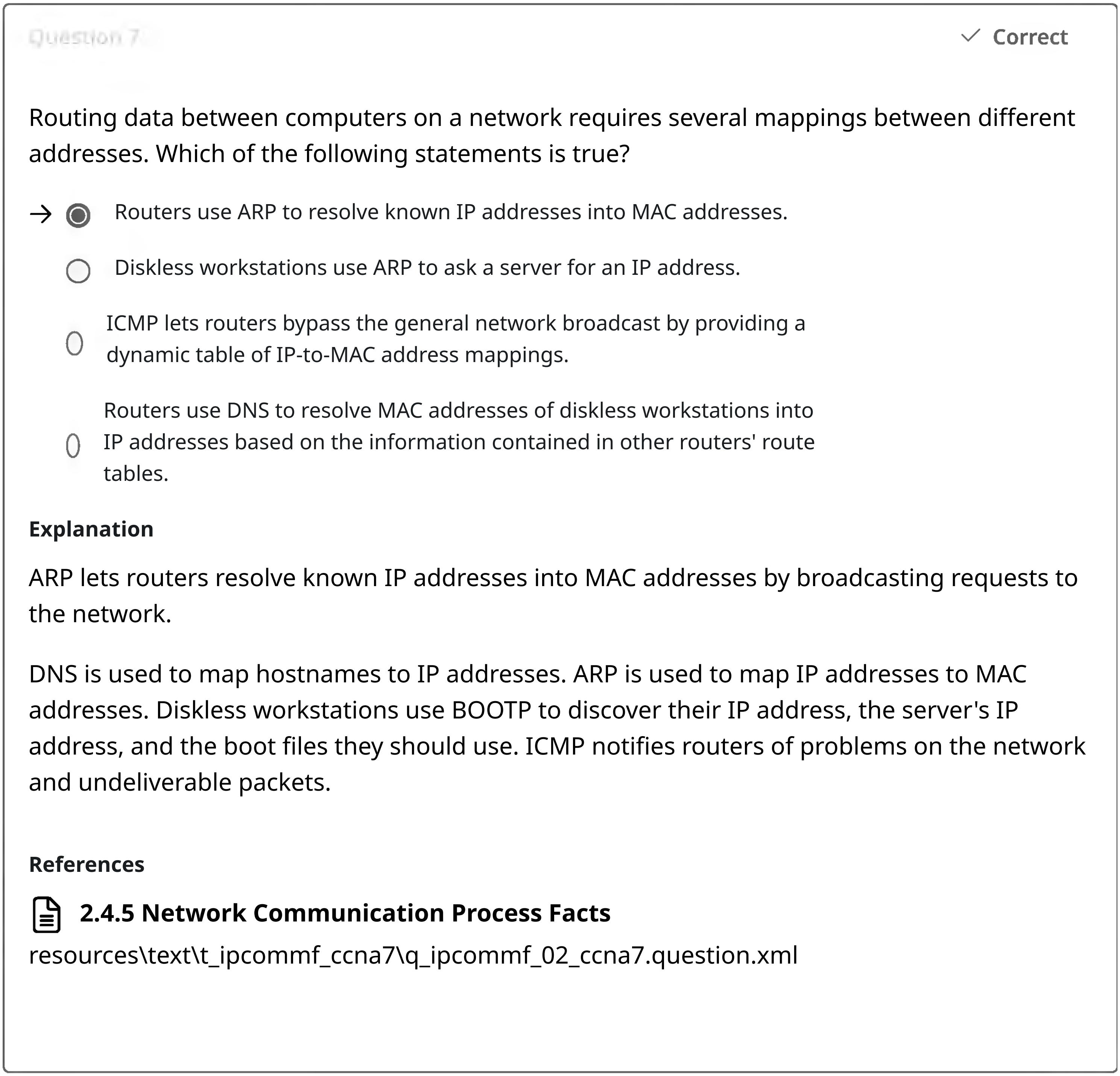
Explanation

ARP (Address Resolution Protocol) resolves IP addresses into MAC addresses. Routers and other network devices use ARP when their routing tables do not contain the MAC addresses of the devices on the local LAN to which they need to forward frames.

References

2.4.5 Network Communication Process Facts

resources\text\t_ipcommf_ccna7\q_ipcommf_01_ccna7.question.xml



Question 7 ✓ Correct

Routing data between computers on a network requires several mappings between different addresses. Which of the following statements is true?

→ ● Routers use ARP to resolve known IP addresses into MAC addresses.

○ Diskless workstations use ARP to ask a server for an IP address.

○ ICMP lets routers bypass the general network broadcast by providing a dynamic table of IP-to-MAC address mappings.

○ Routers use DNS to resolve MAC addresses of diskless workstations into IP addresses based on the information contained in other routers' route tables.

Explanation

ARP lets routers resolve known IP addresses into MAC addresses by broadcasting requests to the network.

DNS is used to map hostnames to IP addresses. ARP is used to map IP addresses to MAC addresses. Diskless workstations use BOOTP to discover their IP address, the server's IP address, and the boot files they should use. ICMP notifies routers of problems on the network and undeliverable packets.

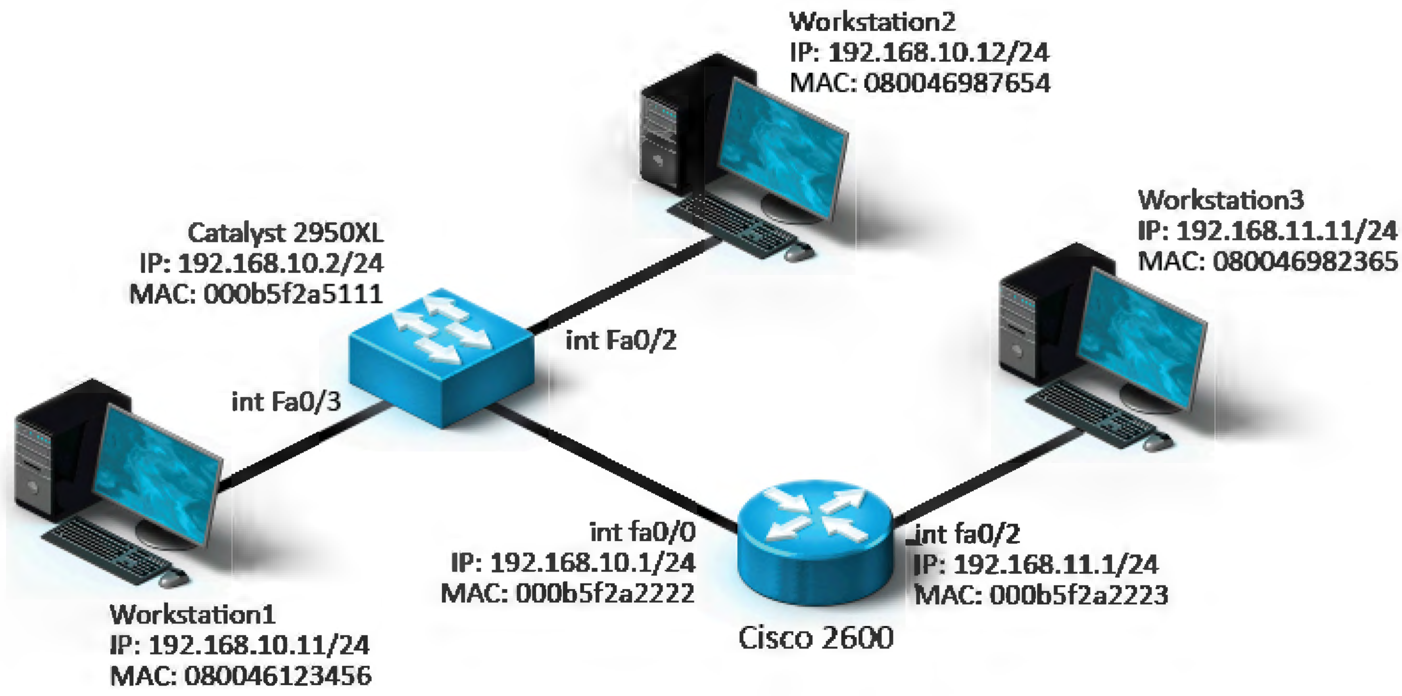
References

2.4.5 Network Communication Process Facts

resources\text\t_ipcommf_ccna7\q_ipcommf_02_ccna7.question.xml

✓ Correct

Workstation2 needs to send data to Workstation3. Identify the Layer 2 and Layer 3 addresses Workstation2 will use to send the data by dragging the corresponding address from the list on the left to its location on the right.



Layer 2 source address

✓ 080046987654

Layer 3 source address

✓ 192.168.10.12

Layer 2 destination address

✓ 000b5f2a2222

Layer 3 destination address

✓ 192.168.11.11

Explanation

Workstation2 uses the following addresses to send the data:

- The source Layer 2 address is its own MAC address, 080046987654.
- The source Layer 3 address is its own IP address, 192.168.10.12.
- The destination Layer 2 address is the MAC address of the default gateway router, 000b5f2a2222. The MAC address is the address of the interface connected to the same subnet as Workstation2.
- The destination Layer 3 address is the IP address of the destination device (Workstation3), 192.168.11.11.

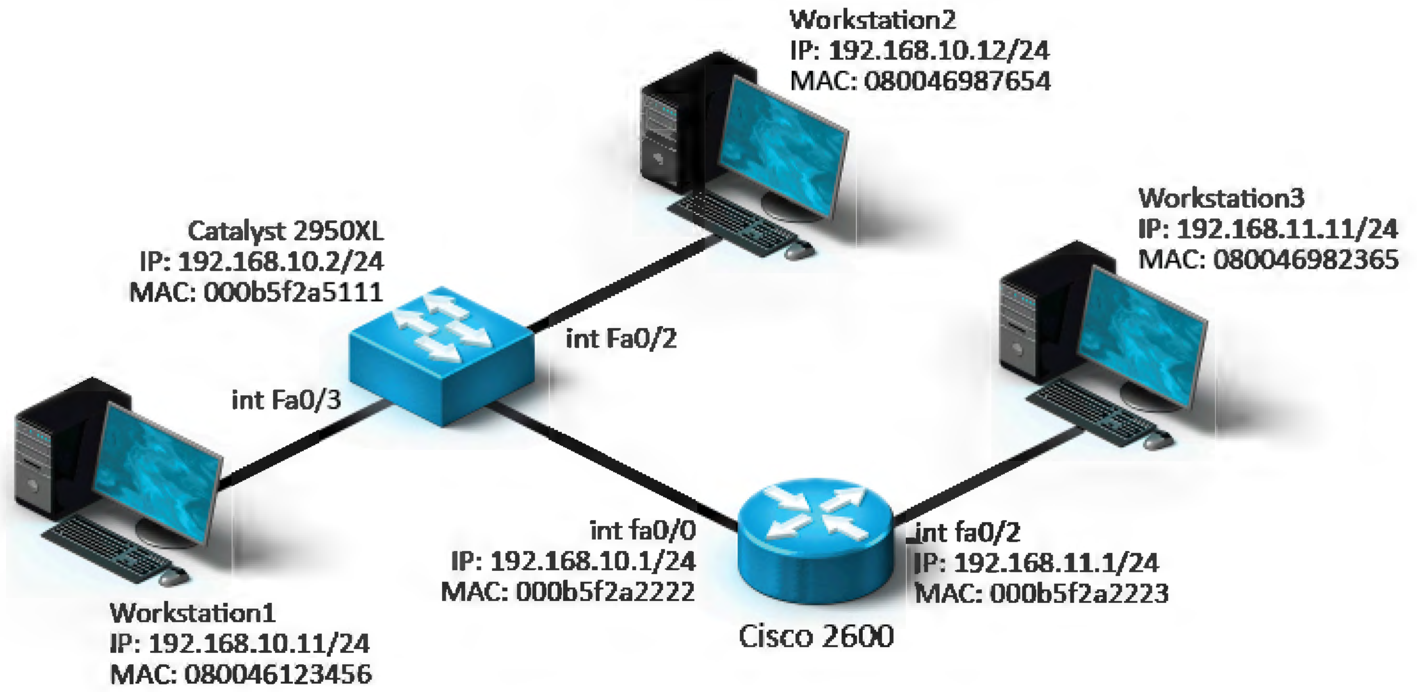
References

2.4.5 Network Communication Process Facts

resources\text\t_ipcommf_ccna7\q_ipcommf_03_ccna7.question.xml

✓ Correct

Workstation3 has started communicating with Workstation2. It sends a frame to the default gateway. Identify the Layer 2 and Layer 3 addresses used by the Cisco 2600 router to forward the data to Workstation2 by dragging the corresponding address from the list on the left to its location on the right.



Layer 2 source address

✓ 000b5f2a2222

Layer 3 source address

✓ 192.168.11.11

Layer 2 destination address

✓ 080046987654

Layer 3 destination address

✓ 192.168.10.12

Explanation

The Cisco 2600 router is the default gateway. When it receives a frame from Workstation3, it examines the Layer 3 address in the packet to locate the destination device. Then it creates a new frame and modifies the source and destination Layer 2 addresses (MAC addresses) as follows:

- The source Layer 2 address is its own MAC address on the same segment as the destination device, 000b5f2a222.
- The destination Layer 2 address is the MAC address of the destination device, 080046987654.

The source and destination Layer 3 addresses (IP addresses) do not change.

- The source IP address is the IP address of Workstation3 is 192.168.11.11.
- The destination IP address is the IP address of Workstation2 is 192.168.10.12.

References

2.4.5 Network Communication Process Facts

resources\text\t_ipcommf_ccna7\q_ipcommf_04_ccna7.question.xml

Question 10 ✓ Correct

During network transmission, data is transferred to various routers, which forward the data to the appropriate network. If the source and destination network addresses reside on the same network, which protocol is used to determine the MAC address of the destination IP address?

○ HTTP get

○ TCP

→ ● ARP

○ UDP

Explanation

The Address Resolution Protocol (ARP) is used to determine the host's MAC address using the destination IP address.

An HTTP get requests web page information from a web server.

UDP and TCP are both Transport layer protocols.

References

2.4.5 Network Communication Process Facts

resources\text\t_ipcommf_ccna7\q_ipcommf_05_ccna7.question.xml

2.5.9 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 1/30/2025, 11:14:50 AM • **Time Spent:** 02:00

Score: 100%

Passing Score: 80%

Question 1

✓ Correct

Which of the following are true about Gigabit Ethernet? (Select two.)

→ ☑ Uses CSMA/CD

□ Uses CSMA/CA

□ Requires fiber optic

□ Uses polling

→ ☑ Can use both copper and fiber optic

Explanation

Gigabit Ethernet is very similar to Fast Ethernet. It uses Carrier Sense, Multiple Access/Collision Detection as the media access method. It can use both copper and fiber optic cables.

References

2.5.2 Network Access (CSMA/Cx)

2.5.3 Ethernet Architecture Facts

6.2.1 Static vs. Dynamic Routing

6.2.2 Static vs. Dynamic Routing Comparison

10.1.1 WAN Overview

10.1.2 WAN Type Facts

resources\text\t_etharchitecture_ccna7\q_etharchitecture_01_ccna7.question.xml

Question 2 ✓ Correct

What is the *backoff* on an Ethernet network?

○ A signal that a collision has occurred.

○ A way to identify the maximum size of a data segment within a packet.

○ A process that prevents collisions from occurring.

→ ○ The random amount of time a device waits before retransmitting after a collision.

Explanation

When a collision occurs on an Ethernet network, sending devices wait a random amount of time before retransmitting. This is called the backoff. Transmitting devices use a jam signal to indicate that a collision has occurred. The backoff cannot completely prevent collisions, although it does help to prevent multiple consecutive collisions.

References

2.5.2 Network Access (CSMA/Cx)

2.5.3 Ethernet Architecture Facts

6.2.1 Static vs. Dynamic Routing

6.2.2 Static vs. Dynamic Routing Comparison

10.1.1 WAN Overview

10.1.2 WAN Type Facts

resources\text\t_etharchitecture_ccna7\q_etharchitecture_02_ccna7.question.xml

Question 3 ✓ Correct

Which of the following mechanisms are used on Ethernet networks to control access to the transmission medium? (Select two.)

□ Token

□ Collision avoidance

□ Request to send/clear to send (RTS/CTS)

→ ☑ Backoff

→ ☑ Collision detection

□ Polling

Explanation

Ethernet networks use Carrier Sense, Multiple Access/Collision Detection (CSMA/CD) for controlling access to the transmission medium. A device first listens to the transmission medium to see if it is free. If it is, it starts to transmit. When a collision occurs, the device that detected the collision sends a jam signal. Any device that was trying to send waits a random period of time (called a backoff) before attempting to retransmit.

Collision avoidance is used on wireless networks. Collision avoidance uses Request to send/clear to send (RTS/CTS) messages to determine when to use the transmission medium.

A token is used on token ring networks; only the device with the token is able to transmit. Polling is a media access control method that uses a central device that regularly grants permission to other devices to use the transmission medium.

References

2.5.2 Network Access (CSMA/Cx)

2.5.3 Ethernet Architecture Facts

6.2.1 Static vs. Dynamic Routing

6.2.2 Static vs. Dynamic Routing Comparison

10.1.1 WAN Overview

10.1.2 WAN Type Facts

resources\text\t_etharchitecture_ccna7\q_etharchitecture_03_ccna7.question.xml

Question 4..

✓ Correct

What is the first thing that happens when a collision occurs on an Ethernet network?

○ A device that wants to send data sends a request to send (RTS) message.

○ All devices wait a random amount of time before trying to retransmit.

→ ● The device that detected the collision transmits a jam signal.

○ All devices that were sending data transmit a clear to send (CTS) message.

○ Devices listen to the medium before trying to retransmit.

Explanation

When a collision occurs on an Ethernet network:

1. The device that detected the collision transmits a jam signal.
2. All devices wait a random period of time before attempting to retransmit.
3. After the time interval has expired, a device will listen to the transmission medium, then transmit if it is free.

Collision avoidance uses Request to send/clear to send (RTS/CTS) messages to determine when to use the transmission medium.

References

- **2.5.2 Network Access (CSMA/Cx)**
- **2.5.3 Ethernet Architecture Facts**
- **6.2.1 Static vs. Dynamic Routing**
- **6.2.2 Static vs. Dynamic Routing Comparison**
- **10.1.1 WAN Overview**
- **10.1.2 WAN Type Facts**

resources\text\t_etharchitecture_ccna7\q_etharchitecture_04_ccna7.question.xml

Question 5 ✓ Correct

Which of the following is true of CSMA/CD? (Select two.)

→ ☑ A device with data to send first listens to the transmission medium to determine whether it is free.

☐ After a collision, sending devices run the same algorithm before sending their messages again.

☐ Only devices with information to send have access to the transmission media.

→ ☑ If collisions are detected, an interrupt jam signal is broadcast to stop all transmissions.

☐ Two devices can transmit at the same time without collisions occurring.

Explanation

CSMA/CD has the following characteristics:

1. Because all devices have equal access to the transmission media (multiple access), a device with data to send first listens to the transmission medium to determine whether it is free (carrier sense).
2. If the transmission medium is not free, the device waits a random time and listens again. When the transmission medium is free, the device transmits its message.
3. If two devices transmit at the same time, a collision occurs. The sending devices detect the collision and sends a jam signal.
4. Both devices wait a random length of time before attempting to resend the original message. This is called a backoff.

References

2.5.2 Network Access (CSMA/Cx)

2.5.3 Ethernet Architecture Facts

6.2.1 Static vs. Dynamic Routing

6.2.2 Static vs. Dynamic Routing Comparison

10.1.1 WAN Overview

10.1.2 WAN Type Facts

resources\text\t_etharchitecture_ccna7\q_etharchitecture_05_ccna7.question.xml

Question 6.

✓ Correct

Which two of the following statements accurately describe full-duplex Ethernet? (Select two.)

☐ It uses 75% of the available bandwidth for actual signal transmission.

☐ It uses built-in loopback and collision detection.

→ ☑ It uses direct point-to-point connections between the sender and receiver.

→ ☑ It is collision-free.

☐ It multiplexes signals along the same wire for higher transmission speeds.

Explanation

Full-duplex Ethernet uses dedicated point-to-point connections and separate circuits for sending and receiving data, so there can be no collisions. Because it is collision-free, it can use 100% of the available bandwidth for data transmission.

Half-duplex Ethernet uses a single cable for both sending and receiving, so it must be able to detect and recover from collisions. Due to possible collisions, transmission speeds and available bandwidth are reduced.

References

2.5.4 Half and Full Duplex Facts

11.7.1 Troubleshoot Switches

11.7.2 Interface Status Troubleshooting Facts

11.7.3 VLAN and Trunking Troubleshooting Facts

resources\text\t_duplex_ccna7\q_duplex_01_ccna7.question.xml

Question 7 ✓ Correct

Which two of the following statements accurately describe half-duplex Ethernet? (Select two.)

→ ☑ It uses collision detection and recovery.

□ It uses direct point-to-point connections between the sender and receiver.

□ It does not require collision detection.

→ ☑ It sends both signals along the same wire.

□ It lets you use 100% of the available bandwidth for data transmission.

Explanation

Half-duplex Ethernet uses a single cable for both sending and receiving, so it must be able to detect and recover from collisions. Because of possible collisions, it can use only 50-60% of the available bandwidth for data transmission. Devices with collision detection turned on require half-duplex.

Full-duplex Ethernet uses dedicated point-to-point connections and separate circuits for sending and receiving data, so there can be no collisions. Because it is collision free, it can use 100% of the available bandwidth for data transmission.

References

2.5.4 Half and Full Duplex Facts

11.7.1 Troubleshoot Switches

11.7.2 Interface Status Troubleshooting Facts

11.7.3 VLAN and Trunking Troubleshooting Facts

resources\text\t_duplex_ccna7\q_duplex_02_ccna7.question.xml

Question 8

✓ Correct

Match each Ethernet frame component with its description.

A set of alternating ones and zeros terminated by two ones (11).

✓ Preamble

Information that needs to be transmitted from one host to the other.

✓ Packet

Verifies that the frame contents arrived uncorrupted.

✓ Frame Check Sequence

Identifies the receiving host's MAC address.

✓ Destination address

Junk data required to make 64 bytes.

✓ Pad

Identifies the sending host's MAC address.

✓ Source address

Specifies the Network/Internet layer protocol being used.

✓ Type

Explanation

The preamble is a set of alternating ones and zeros terminated by two ones (11), which mark it as a frame.

The destination address identifies the receiving host's MAC address.

The source address identifies the sending host's MAC address.

The type field is two bytes and specifies the Network/Internet layer protocol being used.

The packet or data contains the information that needs to be transmitted from one host to the other.

Ethernet frames are 64 to 1518 bytes in size. If the frame is smaller than 64 bytes, the sending NIC places junk data in the pad to make it the required 64 bytes.

The FCS helps verify that the frame contents have arrived uncorrupted using a cyclic redundancy check (CRC), which is a mathematical calculation performed on the frame.

References

2.5.6 Ethernet Frame Format Facts

resources\text\t_frameformat_ccna7\q_frameformat_01_ccna7.question.xml

Question 9 ✓ Correct

What is the maximum cable length for UTP Ethernet T implementations?

○ 10 kilometers

→ ● 100 meters

○ 40 kilometers

○ 300 meters

Explanation

The maximum cable length for UTP Ethernet T implementations is 100 meters for all standards.

References

2.3.1 Network Design Overview

2.3.2 Cables and Connectors

2.3.3 Twisted Pair Facts

2.3.4 Fiber Optic Facts

2.5.7 Ethernet Standards

2.5.8 Ethernet Standards Facts

resources\text\t_ethernetstandards_ccna7\q_ethernetstandards_01_ccna7.question.xml

Question 10

✓ Correct

As specified in the Ethernet standards, what is the maximum number of hosts supported on a single subnet?

○ 254

○ 100

○ 512

→ ● 1024

Explanation

Ethernet standards support a maximum of 1024 hosts on a single subnet.

References

2.3.1 Network Design Overview

2.3.2 Cables and Connectors

2.3.3 Twisted Pair Facts

2.3.4 Fiber Optic Facts

2.5.7 Ethernet Standards

2.5.8 Ethernet Standards Facts

resources\text\t_ethernetstandards_ccna7\q_ethernetstandards_02_ccna7.question.xml

2.6.8 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 2/2/2025, 12:38:00 PM • **Time Spent:** 01:47

Score: 100%

Passing Score: 80%

Question 1

✓ Correct

Which of the following statements are true about bridges? (Select two.)

- □ Bridges connect two networks that use different protocols.
- → ☑ Bridges connect two network segments with the same network address.
- □ Bridges give each segment guaranteed bandwidth.
- → ☑ Bridges convert one type of transmission medium into another.
- □ Bridges maintain a database of routes through a network.

Explanation

A bridge connects two segments within the same subnet. Bridges learn which side a host resides on by copying the MAC address of the source device and placing it into the MAC address table. The port number that the frame entered is also recorded in the table and associated with the source MAC address.

Another function of a bridge is to convert one type of transmission medium into another. A common example of this is a wireless bridge, which converts wired transmissions into wireless transmissions and vice versa.

Routers maintain a database of routes through a network.

Gateways connect two networks that use different protocols.

References

2.6.1 Switches

2.6.2 LAN Connectivity Device Facts

resources\text\t_lanswitch_ccna7\q_lanswitch_01_ccna7.question.xml

Question 2 ✓ Correct

At which layer of the OSI model do network switches operate that do not support routing?

○ Transport

→ ● Data Link

○ Physical

○ Network

Explanation

Switches manipulate Ethernet frames at the Data Link layer of the OSI Model. Some switches, such as a Layer 3 switches, also work at the Network layer.

Network hubs operate at the physical layer of the OSI model. Devices such as routers and multi-layer switches operate at layers higher than the Data Link layer in the OSI model.

References

2.6.1 Switches

2.6.2 LAN Connectivity Device Facts

resources\text\t_lanswitch_ccna7\q_lanswitch_02_ccna7.question.xml

Question 3 ✓ Correct

Which of the following accurately describe how switches and hubs work? (Select two.)

→ ☑ Switches use the hardware address in the frame to send frames only to the port where the device is attached.

□ A switch uses the logical addresses in a packet to send it through the correct port to all VLANs defined on that port.

□ A switch simply receives signals and regenerates them.

□ A hub uses the hardware address in the frame to forward it to the hosts on the VLAN that corresponds to that address.

→ ☑ A hub repeats frames to all ports, regardless of the destination address.

Explanation

It is important to remember that a hub simply receives signals and regenerates them, sending them to all connected devices.

A switch sends data only to the switch port connected to the device for which the data is addressed.

References

2.6.1 Switches

2.6.2 LAN Connectivity Device Facts

resources\text\t_lanswitch_ccna7\q_lanswitch_03_ccna7.question.xml

Question 4

✓ Correct

You want to prevent collisions on your network by creating separate collision domains and defining virtual LANs. Which of the following devices should you choose?

○ Bridge

○ Active hub

→ ● Switch

○ Router

Explanation

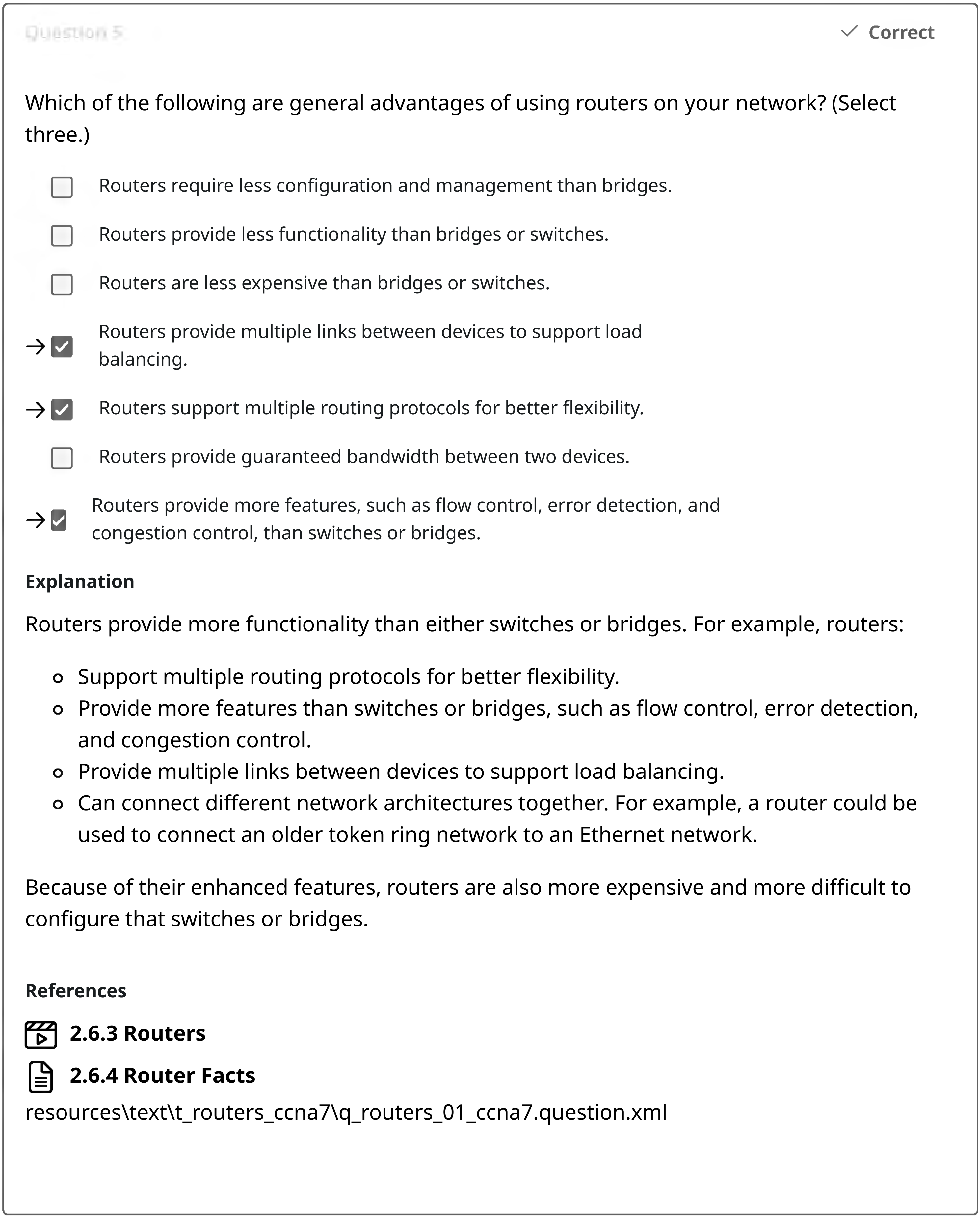
Use a switch to create additional collision domains on a LAN. A switch can be used to define virtual LANs within the switch itself, which a router can't do.

References

2.6.1 Switches

2.6.2 LAN Connectivity Device Facts

resources\text\t_lanswitch_ccna7\q_lanswitch_04_ccna7.question.xml



Question 5

✓ Correct

Which of the following are general advantages of using routers on your network? (Select three.)

- ☐ Routers require less configuration and management than bridges.
- ☐ Routers provide less functionality than bridges or switches.
- ☐ Routers are less expensive than bridges or switches.
- → ☑ Routers provide multiple links between devices to support load balancing.
- → ☑ Routers support multiple routing protocols for better flexibility.
- ☐ Routers provide guaranteed bandwidth between two devices.
- → ☑ Routers provide more features, such as flow control, error detection, and congestion control, than switches or bridges.

Explanation

Routers provide more functionality than either switches or bridges. For example, routers:

- Support multiple routing protocols for better flexibility.
- Provide more features than switches or bridges, such as flow control, error detection, and congestion control.
- Provide multiple links between devices to support load balancing.
- Can connect different network architectures together. For example, a router could be used to connect an older token ring network to an Ethernet network.

Because of their enhanced features, routers are also more expensive and more difficult to configure that switches or bridges.

References

2.6.3 Routers

2.6.4 Router Facts

resources\text\t_routers_ccna7\q_routers_01_ccna7.question.xml

Question 6 ✓ Correct

You have been put in charge of connecting two company networks that were previously separated.

You need to connect a 100BaseTx Ethernet network with an older token ring network. Most traffic will be localized within each network, with only a little traffic crossing between networks. Both networks are using the TCP/IP protocol suite.

Which connectivity device would be the best choice in this situation?

○ Bridge

○ Hub

○ Switch

→ ● Router

Explanation

You should use a router to connect the networks.

Because each network uses a different architecture (and has a different network address and different device addressing scheme), you cannot use a bridge or a switch. A gateway is not needed because both networks are using the same protocol.

References

2.6.3 Routers

2.6.4 Router Facts

resources\text\t_routers_ccna7\q_routers_02_ccna7.question.xml

Question 7 ✓ Correct

You are asked to design a LAN segmentation solution for Company AGH. They have three workgroups separated with VLANs: Accounting, Sales, and Service. Most network traffic is localized within the individual workgroups, but some traffic crosses between each group. Company AGH is especially concerned about the security of information within the Accounting department.

Which segmentation device meets the functionality requirements and provides the simplest, most economical administration?

→ ● Router

○ Hub

○ Bridge

○ Switch

Explanation

Select a router to meet the needs specified in this scenario. The need to keep the Accounting workgroup's traffic secure calls for segmenting them into their own subnet. The router would keep their internal traffic from getting out to the rest of the network.

While a Layer 3, or multilayer, switch can also be used to meet these needs, the switch listed here is not specified as a Layer 3 switch, so it is assumed to be a Layer 2 switch, which would not be able to route traffic from one network to another. You can configure virtual LANs (VLANs) for each workgroup on a switch to segment the network, but a router would be required for data to cross between the workgroups. A switch and router used in combination is another solution, but that would not meet the requirement to be the most economical and simple solution. In addition, routers enforce security better than bridges or hubs.

References

2.6.3 Routers

2.6.4 Router Facts

resources\text\t_routers_ccna7\q_routers_03_ccna7.question.xml

Question 8

✓ Correct

Which of the following describes the function of a dedicated wireless access point on a network?

○ On a network, a wireless access point only acts as a router that connects the wireless network to the wired network.

○ On a network, a wireless access point only acts as a hub that connects to both the wireless and wired networks.

○ On a network, a wireless access point only acts as a switch that forwards traffic from the wireless network to the wired network.

→ ○ On a network, a wireless access point only acts as a bridge between the wireless segment and the wired segment on the same subnet.

Explanation

On a network, a wireless access point only acts as a bridge between the wireless segment and the wired segment on the same subnet. The function of a bridge is to connect two segments of the same subnet. On an enterprise network, the wired segment and the wireless segment need to be on the same subnet, so the wireless access point acts as a bridge between these two segments.

References

2.6.6 Network Appliances

2.6.7 Network Appliance Facts

resources\text\t_netappliances_ccna7\q_netappliances_01_ccna7.question.xml

Question 9 ✓ Correct

Which is the primary role of a firewall?

○ To protect network users from accessing dangerous or questionable web pages. The firewall does this using a website blacklist.

○ To detect and block messages that contain viruses and worms that could infect the network or workstations.

○ To protect users from phishing, botnets, and other types of social networking and social media attacks.

→ ○ To protect networks and workstations by allowing or denying network traffic. The firewall does this using a configured set of rules.

Explanation

A firewall is a software-based or hardware-based network security system that allows or denies network traffic. The firewall does this using a configured set of rules.

References

2.6.6 Network Appliances

2.6.7 Network Appliance Facts

resources\text\t_netappliances_ccna7\q_netappliances_02_ccna7.question.xml

Question 10 ✓ Correct

Match the firewall types on the left with the characteristics shown on the right. (Firewall types may be used more than once.)

Usually a software firewall

✓ Host-based firewall

Most robust and secure firewall

✓ Network-based firewall

Considered a hardware firewall

✓ Network-based firewall

Installed on a single computer

✓ Host-based firewall

Installed on the edge of a network

✓ Network-based firewall

Less robust and less customizable

✓ Host-based firewall

Explanation

Network-based firewalls are installed on the edge of a private network or network segment.

- Most network-based firewalls are considered hardware firewalls, even though they use a combination of hardware and software to protect the network from internet attacks.
- Network-based firewalls are more expensive and require more configuration than other types of firewalls, but they are much more robust and secure.

Host-based firewalls are installed on a single computer in a network. Almost all host-based firewalls are software firewalls.

- A host-based firewall can be used to protect a computer when no network-based firewall exists (such as when connected to a public network).
- Host-based firewalls are less expensive and easier to use than network-based firewalls, but they don't offer the same level of protection or customization.

References

2.6.6 Network Appliances

2.6.7 Network Appliance Facts

resources\text\t_netappliances_ccna7\q_netappliances_03_ccna7.question.xml

3.1.8 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 1/31/2025, 6:07:30 AM • **Time Spent:** 06:06

Score: 100%

Passing Score: 80%

Question 1 ✓ Correct

You are a field technician for a large company. You have been sent to a remote site to troubleshoot a downed router. When you arrive at the remote site, how will you connect your laptop to the router?

○ Connect the laptop's COM/USB port to the router's Ethernet port using a straight-through cable.

○ Connect the laptop's COM/USB port to the router's console port using a crossover cable.

→ ○ Connect the laptop's COM/USB port to the router's console port using a rollover cable.

○ Connect the laptop's COM/USB port to the router's console port using a straight-through cable.

Explanation

You can connect a PC directly to a router using a RJ-45-to-DB-9 female DTE rollover cable or an RJ-45 to USB rollover cable.

References

2.1.9 TCP and UDP Port Numbers

2.2.5 Network Applications

3.1.1 Device Access

3.1.2 Device Connection Facts

13.8.4 Set Up Secure Remote Access

resources\text\t_cabtyp_ccna7\q_cabtyp_01_ccna7.question.xml

Question 2

✓ Correct

You want to make a console connection to a router using the serial port on a PC. Select the necessary components to make the console connection. Select only the necessary components.

Components

✓ Rollover cable

✓ Console port

✓ Terminal emulation program

Explanation

To make a console connection, connect the router's console port to the PC's serial port with a rollover cable, and then run a terminal emulation program (such as HyperTerminal) on the PC to make the connection.

To connect to a router with a Telnet session connect the router to a PC or to the network using the Ethernet port and an Ethernet cable. The router interface must be assigned an IP address.

References

2.1.9 TCP and UDP Port Numbers

2.2.5 Network Applications

3.1.1 Device Access

3.1.2 Device Connection Facts

13.8.4 Set Up Secure Remote Access

resources\text\t_cabtyp_ccna7\q_cabtyp_02_ccna7.question.xml

Question 3.

✓ Correct

Match the memory types with the information they store.

Stores the running-configuration file, routing tables, and ARP tables.

✓ RAM

Stores the startup-configuration file.

✓ NVRAM

Stores the Cisco IOS software.

✓ FLASH

Stores POST and the boot loader software.

✓ ROM

Explanation

RAM stores the running-configuration file, routing tables, and ARP tables.

FLASH stores the Cisco IOS software.

ROM stores POST and the boot loader software.

NVRAM stores the startup-configuration file.

References

3.1.7 Manage IOS Files Facts

resources\text\t_ios_files_ccna7\q_ios_files_01_ccna7.question.xml

Question 4 ✓ Correct

You have issued the following command and received the response as shown.

```
Router#sh start
%%Non-volatile configuration memory has not been set up or has
bad checksum
```

Which of the following is a reason for this response?

○ The command was issued from user EXEC mode but needs to be issued from privileged EXEC mode instead.

○ RAM memory contains no configuration file.

○ The router issues a bad checksum because a file on the TFTP server is also named startup-config.

→ ● No configuration file has been saved to NVRAM.

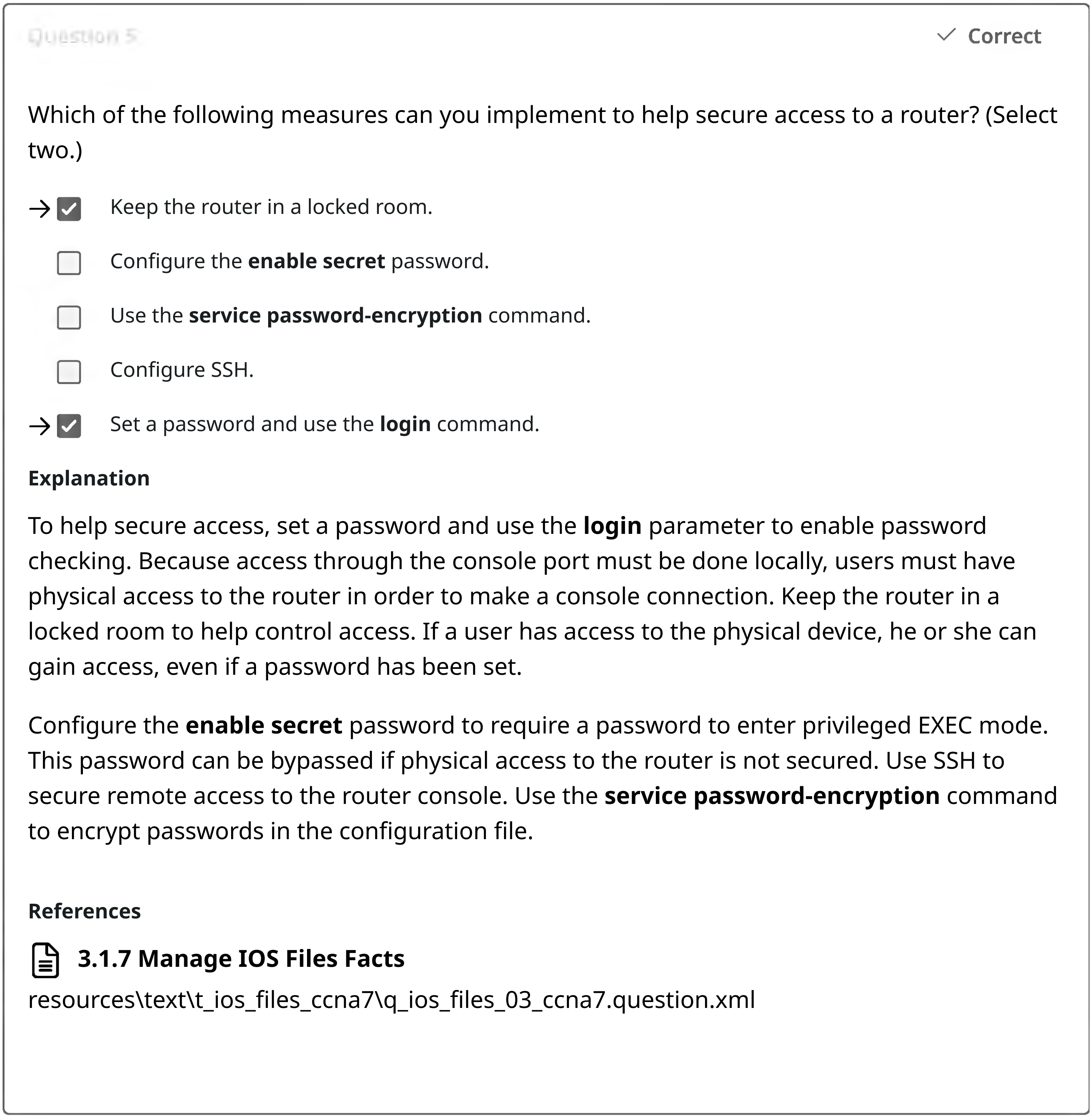
Explanation

This message is shown if no configuration file are saved to NVRAM.

References

3.1.7 Manage IOS Files Facts

resources\text\t_ios_files_ccna7\q_ios_files_02_ccna7.question.xml



Question 5

✓ Correct

Which of the following measures can you implement to help secure access to a router? (Select two.)

→ ☑ Keep the router in a locked room.

□ Configure the **enable secret** password.

□ Use the **service password-encryption** command.

□ Configure SSH.

→ ☑ Set a password and use the **login** command.

Explanation

To help secure access, set a password and use the **login** parameter to enable password checking. Because access through the console port must be done locally, users must have physical access to the router in order to make a console connection. Keep the router in a locked room to help control access. If a user has access to the physical device, he or she can gain access, even if a password has been set.

Configure the **enable secret** password to require a password to enter privileged EXEC mode. This password can be bypassed if physical access to the router is not secured. Use SSH to secure remote access to the router console. Use the **service password-encryption** command to encrypt passwords in the configuration file.

References

3.1.7 Manage IOS Files Facts

resources\text\t_ios_files_ccna7\q_ios_files_03_ccna7.question.xml

Question 6.

✓ Correct

Put the boot sequence process items in order.

1

✓ Power-on self-test checks hardware.

2

✓ Boot loader software is loaded.

3

✓ IOS is loaded.

4

✓ Startup-config is loaded.

Explanation

After a successful power-on-self-test, the device copies the boot loader software, which is sometimes called a bootstrap, from the ROM into RAM and executes it. The bootstrap program initializes the CPU and enables other boot functions. It also determines which IOS image should be used and when to load it.

As the IOS loads from flash memory, the boot loader software turns control of the system over to the operating system.

Then the IOS locates the startup configuration file in NVRAM and loads it into RAM as the running-config file.
At this point, all interfaces are initialized using the commands found in the startup-config file. Everything is loaded into RAM, so the boot sequence is complete.

References

3.1.7 Manage IOS Files Facts

resources\text\t_ios_files_ccna7\q_ios_files_04_ccna7.question.xml

Question 7.

✓ Correct

You are the senior network administrator for a large company. A junior administrator from one of your field offices sent you a router that he thinks is faulty. He says the router always uses default settings and boots to setup mode even though he has verified that startup-config contains the correct values.

What is the most likely source of the problem?

○ Startup-config in NVRAM is corrupt and must be erased and restored from backup.

→ ● The router configuration register is set to bypass startup configuration.

○ There is no space available in NVRAM.

○ The NVRAM chip is faulty, preventing the router from loading the configuration.

Explanation

The configuration register can be configured to bypass startup configuration settings. Use **Router(config)#config-register 0x2102** to change the configuration register.

Use **show version** to display the current configuration register setting.

The configuration register for most Cisco devices is normally 0x2102. When configured to bypass startup configuration, the setting will be 0x2142.

References

3.1.7 Manage IOS Files Facts

resources\text\t_ios_files_ccna7\q_ios_files_05_ccna7.question.xml

Question 8 ✓ Correct

The configuration register runs during the POST. What does it control?

○ What is stored in NVRAM.

→ ● How the router boots up.

○ The licensing information.

○ The running-config file.

Explanation

The configuration register runs during the POST, and it controls how the router boots up.

References

3.1.7 Manage IOS Files Facts

resources\text\t_ios_files_ccna7\q_ios_files_06_ccna7.question.xml

Question 9 ✓ Correct

You have made configuration changes to your Cisco device. Now you want to save the changes to use the next time the device is booted up. Which command could you use?

○ **flash start copy**

→ ● **copy run start**

○ **run copy start**

○ **copy start tftp**

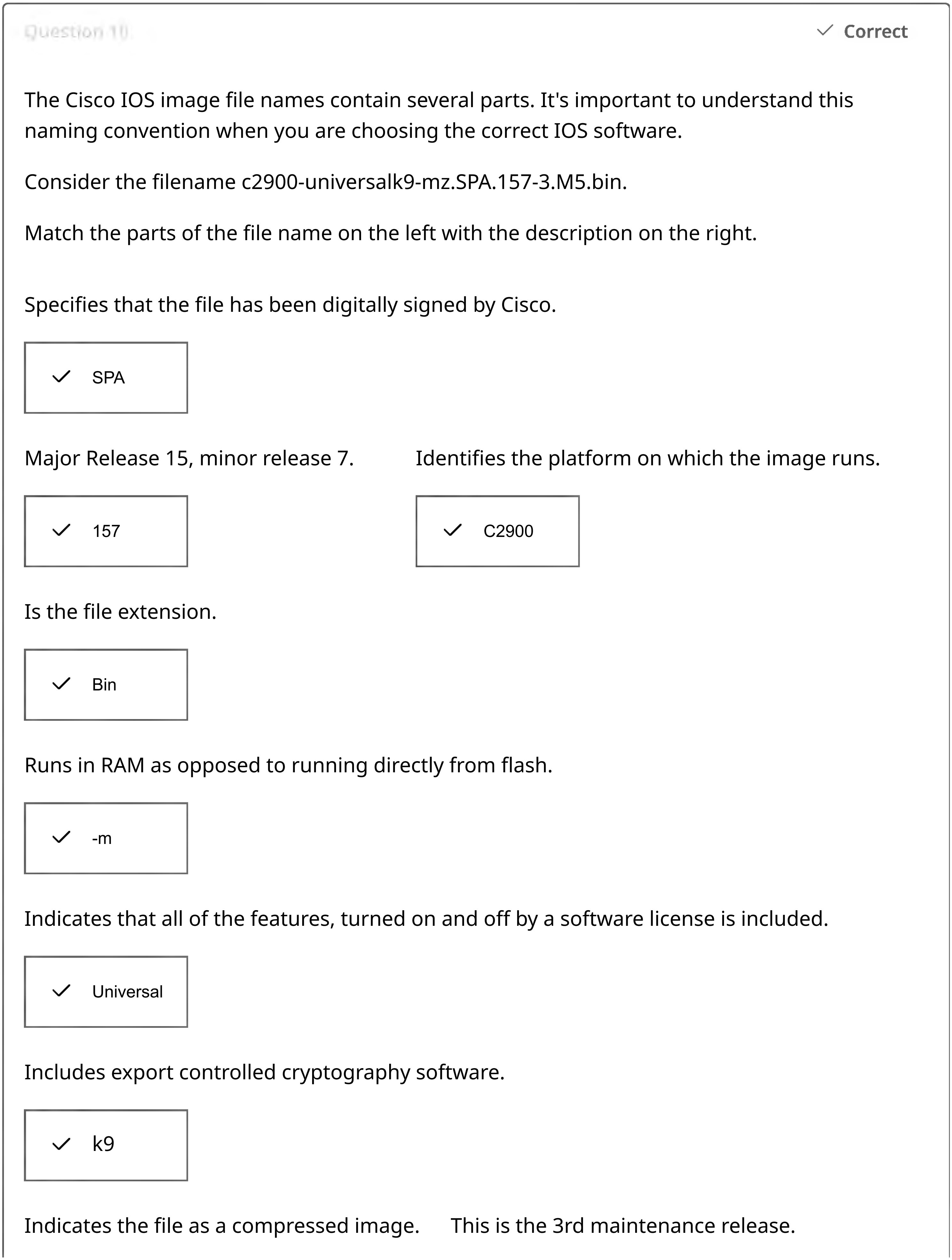
Explanation

If you want to save the changes made to a Cisco device, you need to copy them to the startup-config file to use the next time the device is booted up. You can do this with the **copy run start** command, which is basically just a shorter version of **copy running-config startup-config**. This command instructs the device to copy the contents of the running-config file to the startup-config file.

References

3.1.7 Manage IOS Files Facts

resources\text\t_ios_files_ccna7\q_ios_files_07_ccna7.question.xml



Question 10

✓ Correct

The Cisco IOS image file names contain several parts. It's important to understand this naming convention when you are choosing the correct IOS software.

Consider the filename c2900-universalk9-mz.SPA.157-3.M5.bin.

Match the parts of the file name on the left with the description on the right.

Specifies that the file has been digitally signed by Cisco.

✓ SPA

Major Release 15, minor release 7.

✓ 157

Identifies the platform on which the image runs.

✓ C2900

Is the file extension.

✓ Bin

Runs in RAM as opposed to running directly from flash.

✓ -m

Indicates that all of the features, turned on and off by a software license is included.

✓ Universal

Includes export controlled cryptography software.

✓ k9

Indicates the file as a compressed image.

This is the 3rd maintenance release.

✓ z

✓ -3

Specifies the version of the IOS

✓ M5

Explanation

Consider the filename c2900-universalk9-mz.SPA.157-3.M5.bin:

- C2900 identifies the platform on which the image runs. In this example, the platform is a Cisco 2900 router.
- Universal indicates that all of the features, turned on and off by a software license is included.
- k9 includes export controlled cryptography software.
- -m runs in RAM (memory) as opposed to running directly from flash.
- z indicates the file as a compressed image.
- SPA designates that the file has been digitally signed by Cisco.
- 157 designates major release 15 (Polaris), minor release 7 (aka, 15.7).
- -3 is the 3rd maintenance release.
- M5 specifies the version of the IOS, including the major release, minor release, maintenance release, and maintenance rebuild numbers. The M indicates that this is an extended maintenance release.
- .bin is the file extension indicating that this file is a binary executable file.

References

3.1.7 Manage IOS Files Facts

resources\text\t_ios_files_ccna7\q_ios_files_08_ccna7.question.xml

3.2.12 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 1/31/2025, 11:26:18 AM • **Time Spent:** 01:33

Score: 100%

Passing Score: 80%

Question 1

✓ Correct

Which command would you use to remove the contents of NVRAM?

○ **wipe nvram**

○ **delete nvram**

○ **clear nvram**

→ ● **erase nvram**

Explanation

Use the **erase nvram** command to deletes the contents of NVRAM (which also erases startup-config).

References

3.2.11 Command Editing Facts

resources\text\t_editing_ccna7\q_editing_01_ccna7.question.xml

Question 2 ✓ Correct

While working at the console of a Cisco device, you need to use the same command repeatedly.

Given that the command is quite long, what can you do to avoid having to retype it over and over?

○ Enter **terminal editing** at the command prompt.

○ Enter **terminal no history** at the command prompt.

○ Enter **show history** at the command prompt.

→ ● Press the Up arrow key.

Explanation

While working at the console of a Cisco device, you can press the Up arrow key to retrieve the last command used from the command history. Using command history can be very useful in situations where you need to use the same commands over and over.

The **terminal editing** command turns advanced editing on.

show history displays all the commands in the history buffer.

terminal no history turns command history off.

References

3.2.10 Command History Facts

resources\text\t_histlist_ccna7\q_histlist_01_ccna7.question.xml

Question 3 ✓ Correct

While working at the console of a Cisco device, you need to view a list of the commands that are available in the current mode.

Which command should you use?

→ ● **?**

○ **terminal history**

○ **terminal editing**

○ **show history**

Explanation

While working at the console of a Cisco device, you can enter **?** at the command prompt to display a list of all the commands that are available in the current mode.

show history displays all the commands in the history buffer.

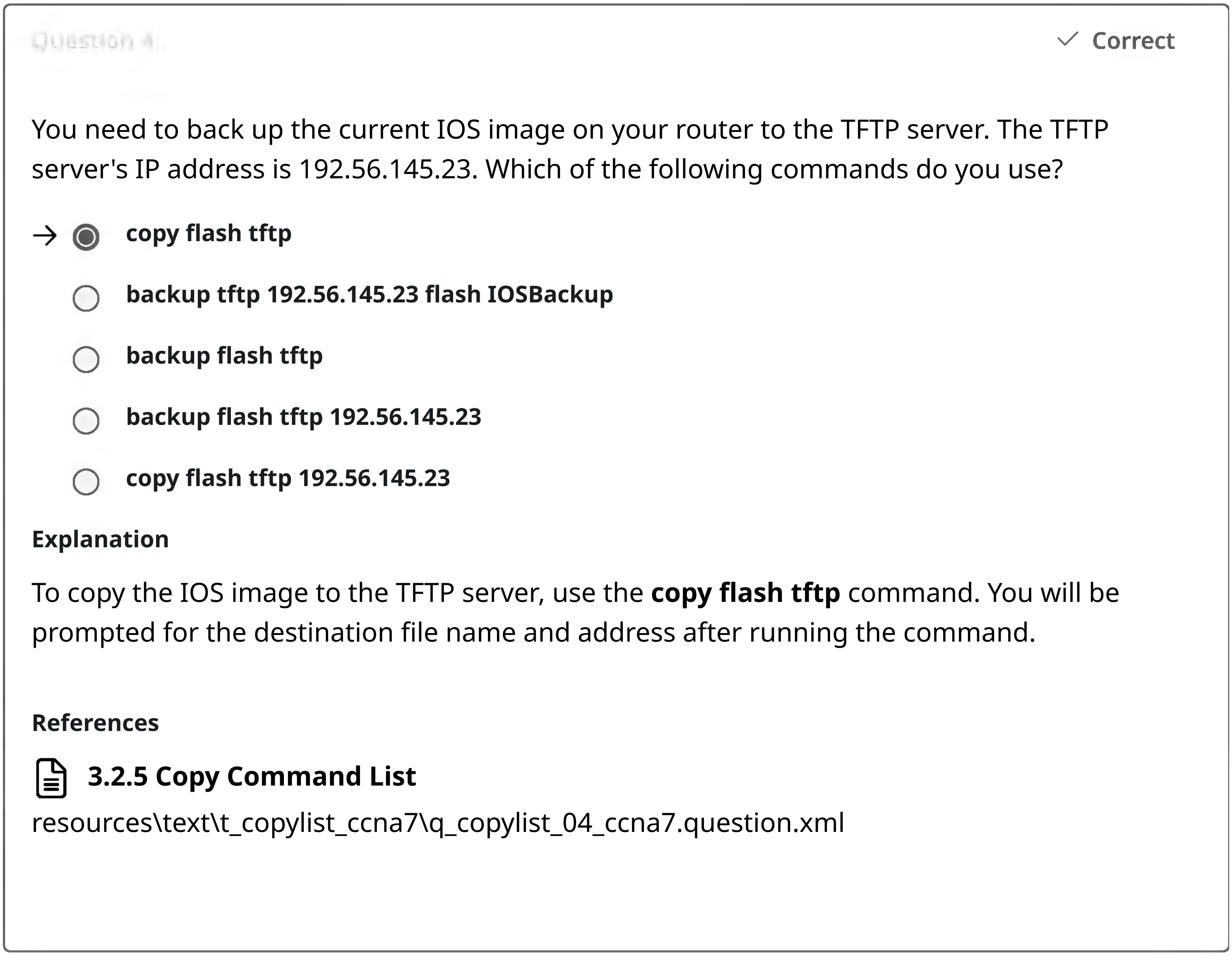
terminal history turns command history on.

terminal editing turns advanced editing on.

References

3.2.9 Command Help Facts

resources\text\t_chelp_ccna7\q_chelp_01_ccna7.question.xml



Question 4 ✓ Correct

You need to back up the current IOS image on your router to the TFTP server. The TFTP server's IP address is 192.56.145.23. Which of the following commands do you use?

→ ● **copy flash tftp**

○ **backup tftp 192.56.145.23 flash IOSBackup**

○ **backup flash tftp**

○ **backup flash tftp 192.56.145.23**

○ **copy flash tftp 192.56.145.23**

Explanation

To copy the IOS image to the TFTP server, use the **copy flash tftp** command. You will be prompted for the destination file name and address after running the command.

References

3.2.5 Copy Command List

resources\text\t_copylist_ccna7\q_copylist_04_ccna7.question.xml

Question 5 ✓ Correct

Match each command to its corresponding operation.

Save the current configuration to NVRAM.

✓ **copy run start**

Load the current configuration saved in NVRAM into memory.

✓ **copy start run**

Save the current configuration to a network server.

✓ **copy run tftp**

Copy a configuration file from a network server into NVRAM.

✓ **copy tftp start**

Explanation

The currently used configuration file is called the running-config file. The configuration file saved in NVRAM is startup-config. To save a configuration file, use the format **copy *from to***.

- Use **copy run start** to save the current configuration to NVRAM.
- Use **copy start run** to load the current configuration saved in NVRAM into memory.
- Use **copy run tftp** to save the current configuration to a network server.
- Use **copy tftp start** to copy a configuration file from a network server into NVRAM.

References

3.2.5 Copy Command List

resources\text\t_copylist_ccna7\q_copylist_03_ccna7.question.xml

Question fi

✓ Correct

You want to save the configuration file in NVRAM to a TFTP server with address 192.168.1.10 to be used as a backup. Which command would you use?

- ○ **copy tftp start**
- → ● **copy start tftp**
- ○ **copy tftp run**
- ○ **copy run tftp**
- ○ **copy start tftp 192.168.1.10**

Explanation

Use the **copy start tftp** command to copy the startup-config file to the TFTP server. You cannot specify the server address from the command line. After you issue the command, you will be prompted to supply the server address.

References

3.2.5 Copy Command List

resources\text\t_copylist_ccna7\q_copylist_02_ccna7.question.xml

Question 7 ✓ Correct

Which of the following configuration register values tells the router to use configuration information from NVRAM?

→ ● 0x2102

○ 0x2101

○ 0x001

○ 0x42

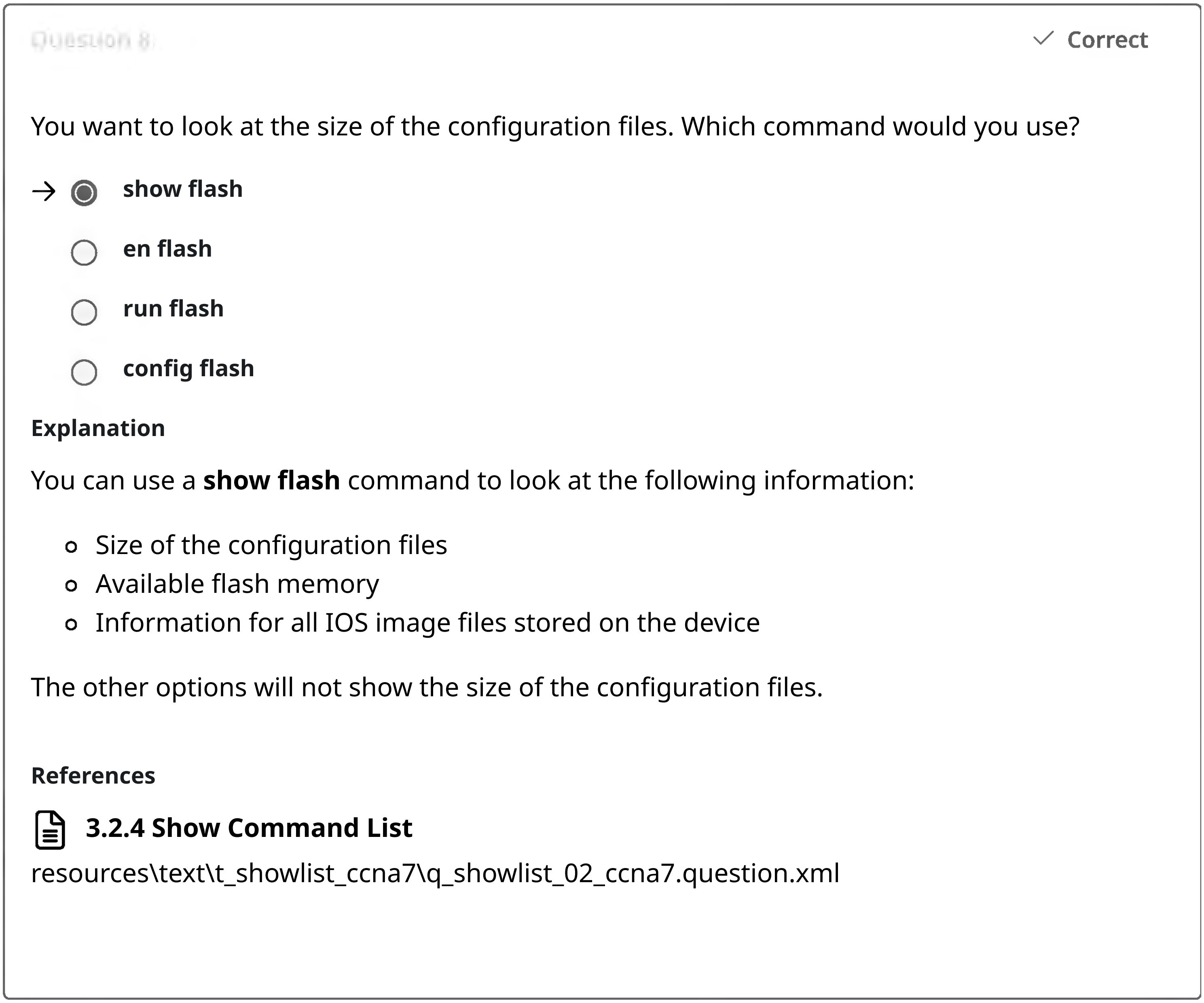
Explanation

The factory-default setting for the configuration register is 0x2102. This indicates that the router should attempt to load an IOS image from Flash memory and load the startup configuration from NVRAM.

References

3.2.5 Copy Command List

resources\text\t_copylist_ccna7\q_copylist_01_ccna7.question.xml



Question 8 ✓ Correct

You want to look at the size of the configuration files. Which command would you use?

→ ● **show flash**

○ **en flash**

○ **run flash**

○ **config flash**

Explanation

You can use a **show flash** command to look at the following information:

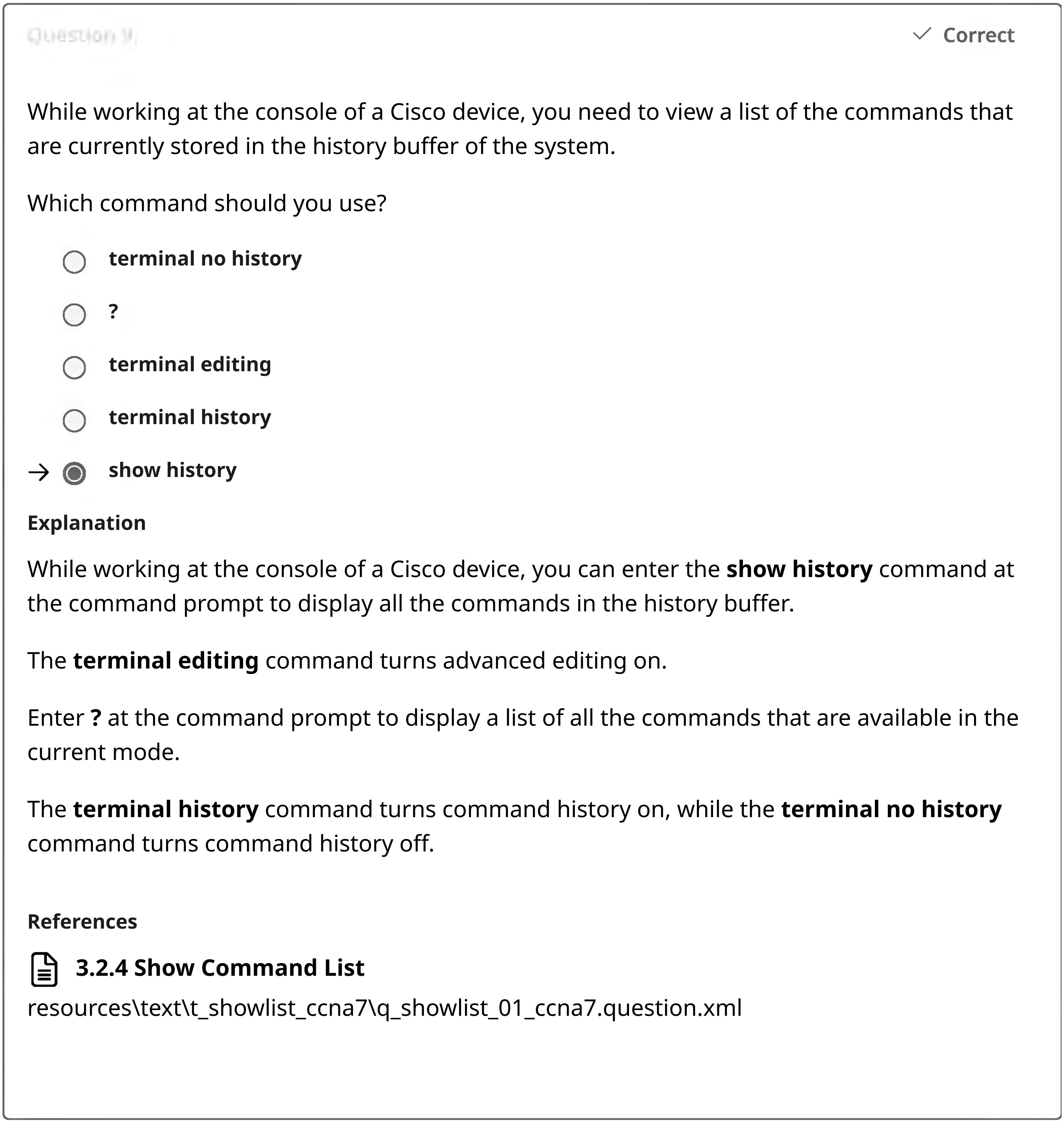
- Size of the configuration files
- Available flash memory
- Information for all IOS image files stored on the device

The other options will not show the size of the configuration files.

References

3.2.4 Show Command List

resources\text\t_showlist_ccna7\q_showlist_02_ccna7.question.xml



Question 9 ✓ Correct

While working at the console of a Cisco device, you need to view a list of the commands that are currently stored in the history buffer of the system.

Which command should you use?

- ○ **terminal no history**
- ○ **?**
- ○ **terminal editing**
- ○ **terminal history**
- → ● **show history**

Explanation

While working at the console of a Cisco device, you can enter the **show history** command at the command prompt to display all the commands in the history buffer.

The **terminal editing** command turns advanced editing on.

Enter **?** at the command prompt to display a list of all the commands that are available in the current mode.

The **terminal history** command turns command history on, while the **terminal no history** command turns command history off.

References

3.2.4 Show Command List

resources\text\t_showlist_ccna7\q_showlist_01_ccna7.question.xml

Question 10

✓ Correct

You are working on a Cisco device. The prompt is showing Router#. Which mode are you in?

○ ROMmon

→ ● Privileged EXEC

○ Global Configuration

○ User EXEC

Explanation

Mode	**Prompt**	**To Enter**	**To Exit**
User EXEC	Router>	Press **Enter** and then log in.	**Exit**, **Logout**, **Disconnect**
Privileged EXEC	Router#	**Enable**	**Disable**
Global Configuration	Router (config)#	**Config terminal**	**Exit**, **Ctrl** + **Z**

ROMmon mode is a command line mode that is used to recover a lost or forgotten password, to reinstall the IOS, or to format the flash file system.

References

3.2.3 Command Line Interface Facts

resources\text\t_modes_ccna7\q_modes_01_ccna7.question.xml

3.3.5 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 1/31/2025, 11:46:12 AM • **Time Spent:** 01:51

Score: 100%

Passing Score: 80%

Question 1

✓ Correct

You need to add VoIP and IP telephony support to a router.

Which feature set must be enabled to do this?

- ○ Data
- ○ Security
- ○ IP Base
- → ● Unified Communication

Explanation

Enabling the Unified Communications feature set on a Cisco router allows the device to provide VoIP and IP telephony support.

The IP Base feature set provides basic IP routing functionality. This feature set is a prerequisite for all other feature sets and is enabled by default on all Cisco routers.

The Data feature set provides mobile IP, multicast authentication, token ring, SNTP, and SDLC.

The Security feature set provides firewall, IPS, IPsec, 3DES, and VPN support.

References

3.3.4 IOS Licensing Facts

resources\text\t_ios_licensing_ccna7\q_ios_licensing_01_ccna7.question.xml

Question 2 ✓ Correct

You need to add the Security feature set to a router. Prior to accessing Cisco's website to purchase the appropriate license, you need to record the router's UDI.

Which command can you use to do this?

○ **show license feature**

○ **show license**

→ ● **show license udi**

○ **license install**

Explanation

Every Cisco device that supports universal images has an identifier assigned to it called the unique device identifier (UDI). The UDI is composed of two parts:

- Product ID (PID)
- Serial number (SN)

To identify a device's UDI, you can use either of the **show license udi** commands.

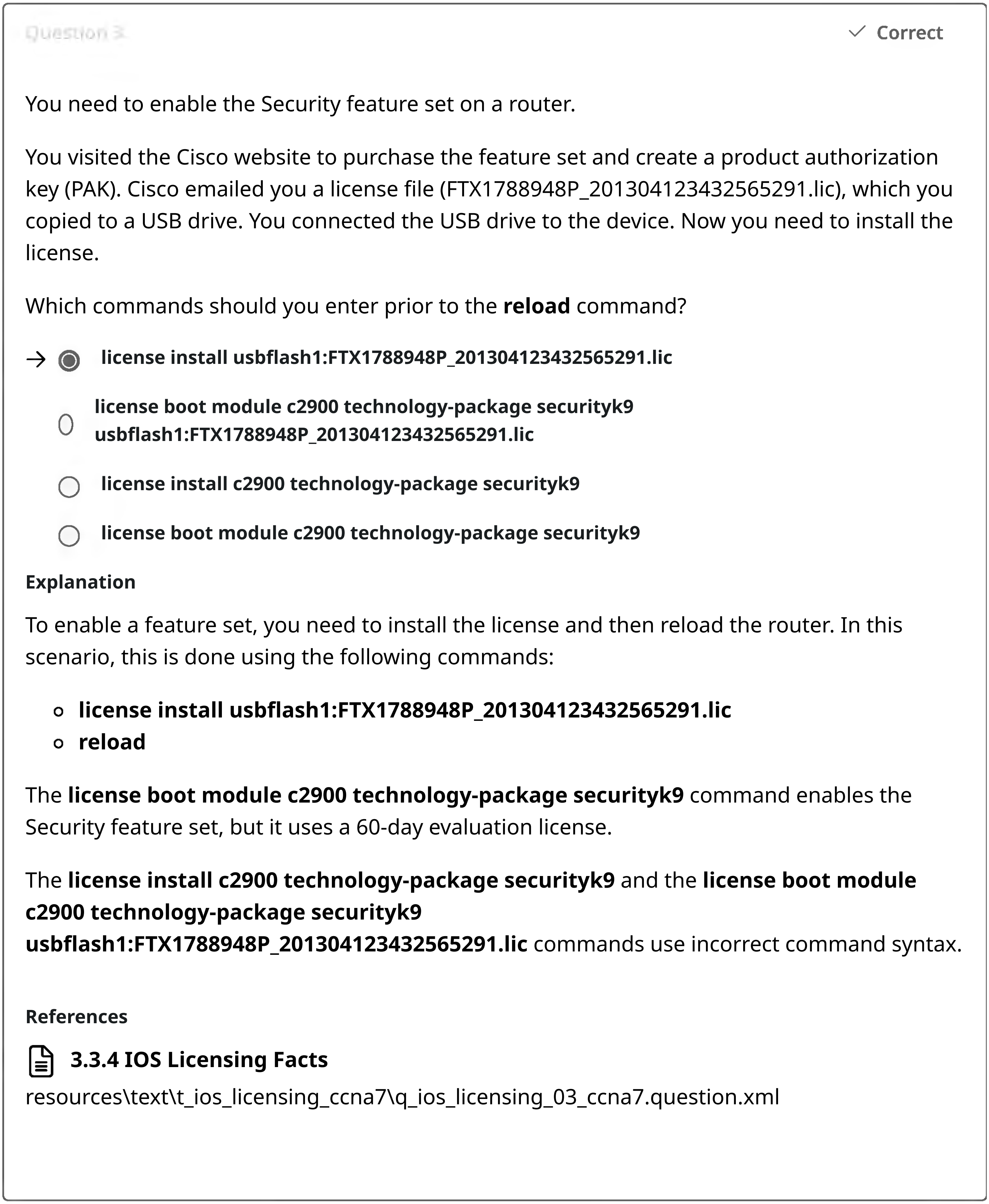
The **show license** and **show license feature** commands display the feature sets enabled on the device.

The **license install** command is used to install new licenses on the device.

References

3.3.4 IOS Licensing Facts

resources\text\t_ios_licensing_ccna7\q_ios_licensing_02_ccna7.question.xml



Question 3

✓ Correct

You need to enable the Security feature set on a router.

You visited the Cisco website to purchase the feature set and create a product authorization key (PAK). Cisco emailed you a license file (FTX1788948P_201304123432565291.lic), which you copied to a USB drive. You connected the USB drive to the device. Now you need to install the license.

Which commands should you enter prior to the **reload** command?

→ ● **license install usbflash1:FTX1788948P_201304123432565291.lic**

○ **license boot module c2900 technology-package securityk9 usbflash1:FTX1788948P_201304123432565291.lic**

○ **license install c2900 technology-package securityk9**

○ **license boot module c2900 technology-package securityk9**

Explanation

To enable a feature set, you need to install the license and then reload the router. In this scenario, this is done using the following commands:

- **license install usbflash1:FTX1788948P_201304123432565291.lic**
- **reload**

The **license boot module c2900 technology-package securityk9** command enables the Security feature set, but it uses a 60-day evaluation license.

The **license install c2900 technology-package securityk9** and the **license boot module c2900 technology-package securityk9 usbflash1:FTX1788948P_201304123432565291.lic** commands use incorrect command syntax.

References

3.3.4 IOS Licensing Facts

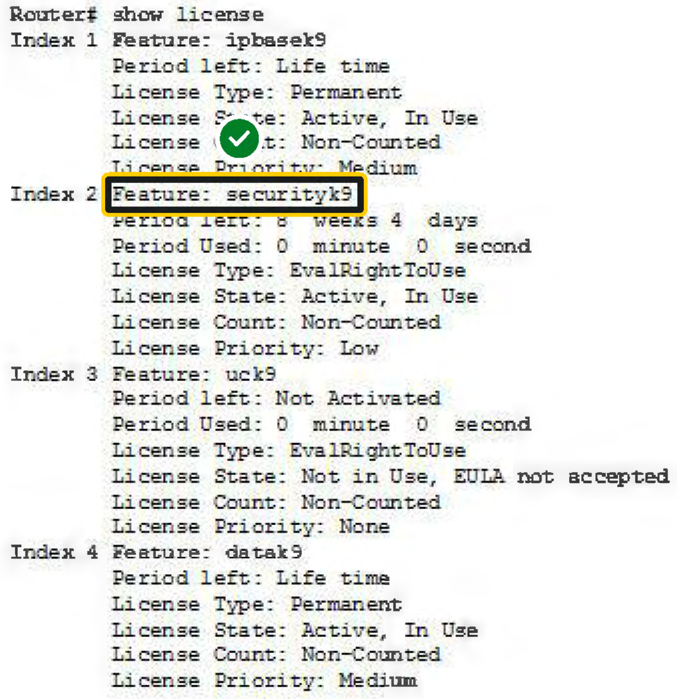
resources\text\t_ios_licensing_ccna7\q_ios_licensing_03_ccna7.question.xml

Question 4.

✓ Correct

Consider the output from the **show license** command shown in the figure below.

Click on the feature set that has been enabled using a right-to-use evaluation license.



```
Router# show license
Index 1 Feature: ipbasek9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: securityk9
        Period left: 8  weeks 4  days
        Period Used: 0  minute  0  second
        License Type: EvalRightToUse
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Low
Index 3 Feature: uck9
        Period left: Not Activated
        Period Used: 0  minute  0  second
        License Type: EvalRightToUse
        License State: Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None
Index 4 Feature: datak9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
```

Explanation

Features that are displayed with a license type of *EvalRightToUse* and a license state of *Active, In Use* in the output of the **show license** command have been enabled using a 60-day evaluation right-to-use license. In this example, the securityk9 feature has been enabled with this type of license.

In this example, the ipbasek9 and datak9 feature sets have been enabled using a product authorization key (PAK). The uck9 feature set is not enabled.

References

3.3.4 IOS Licensing Facts

resources\text\t_ios_licensing_ccna7\q_ios_licensing_04_ccna7.question.xml

Question 5

✓ Correct

You need to add multiprotocol label switching (MPLS) support to a router using the Data feature set.

Which feature set must be enabled before the Data feature set can be enabled?

→ ● ipbasek9

○ datak9

○ uck9

○ securityk9

Explanation

The IP Base (ipbasek9) feature set provides basic IP routing functionality. This feature set is a prerequisite for all other feature sets, and it is enabled by default on all Cisco routers.

Enabling the Unified Communications (uck9) feature set on a Cisco router allows the device to provide VoIP and IP telephony support.

The Data (datak9) feature set provides MPLS, ATM, and multiprotocol support.

The Security (securityk9) feature set provides firewall, IPS, IPsec, 3DES, and VPN support.

References

3.3.4 IOS Licensing Facts

resources\text\t_ios_licensing_ccna7\q_ios_licensing_05_ccna7.question.xml

Question 6. ✓ Correct

You want to view the feature sets that have been enabled on a router and what types of licenses they use.

Which commands can you use to do this? (Select two. Each option is a complete solution.)

→ ☑ **show version**

□ **license install**

□ **license boot module**

→ ☑ **show license**

□ **show license udi**

Explanation

To identify which feature sets have been enabled on a device and view the type of license used for each, you can use either of the following commands:

- **show version**
- **show license**

The **show license udi** command displays the device's UDI.

The **license install** and **license boot module** commands are used to enable features on the device.

References

3.3.4 IOS Licensing Facts

resources\text\t_ios_licensing_ccna7\q_ios_licensing_06_ccna7.question.xml

Question 7 ✓ Correct

You use a Cisco 2900 router in your network. You are considering purchasing and implementing the Unified Communications feature set on this router. However, you would like to evaluate this feature set for a period of time prior to purchasing it.

Which command activates the evaluation right-to-use license for this feature set?

→ ● **license boot module c2900 technology-package uck9**

○ **license boot module c2900 technology-package data9**

○ **license boot module c2900 technology-package securityk9**

○ **install license feature uck9 EvaluateRightToUse**

○ **license install evaluate uck9**

Explanation

The **license boot module *device_model* technology-package *feature_set*** command installs a 60-day evaluation license for the specified feature set. Evaluation licenses don't require a PAK. Replace ***device_model*** with the model number of the device. Replace ***feature_set*** with the name of the feature set to be enabled, such as uck9 (for Unified Communications).

The **license boot module c2900 technology-package securityk9** command uses the correct syntax, but installs the Security feature set instead of the Unified Communications feature set.

The **license boot module c2900 technology-package datak9** command also uses the correct syntax, but installs the Data feature set instead of the Unified Communications feature set.

The **license install evaluate uck9** and **install license feature uck9 EvaluateRightToUse** commands use incorrect syntax for installing an evaluation license.

References

3.3.4 IOS Licensing Facts

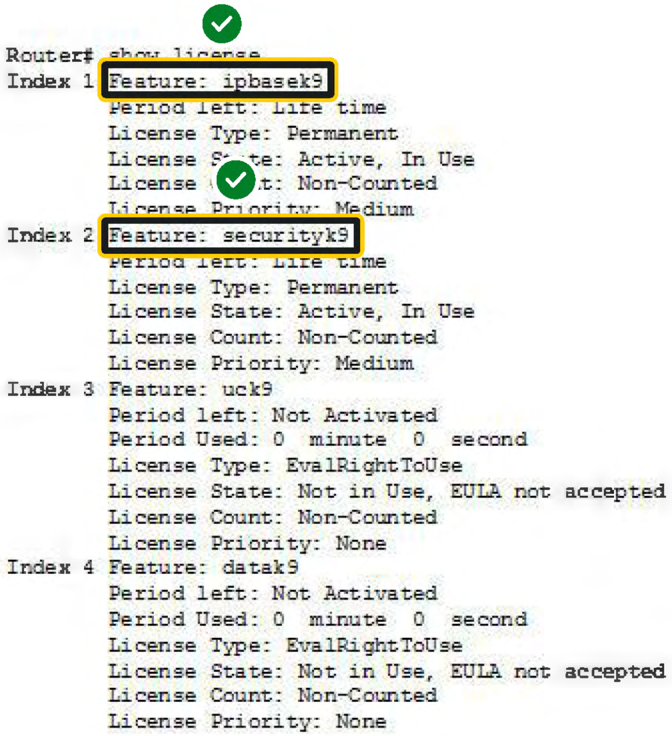
resources\text\t_ios_licensing_ccna7\q_ios_licensing_07_ccna7.question.xml

Question 8

✓ Correct

Consider the output from the **show license** command shown in the figure below.

Click on all feature sets that have been enabled using a product authorization key (PAK).



```
Router# show license
Index 1 Feature: ipbasek9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: securityk9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 3 Feature: uck9
        Period left: Not Activated
        Period Used: 0  minute  0  second
        License Type: EvalRightToUse
        License State: Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None
Index 4 Feature: datak9
        Period left: Not Activated
        Period Used: 0  minute  0  second
        License Type: EvalRightToUse
        License State: Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None
```

Explanation

Features that are displayed with a license type of *Permanent* in the output of the **show license** command have been enabled using a product authorization key (PAK). In this example, the following features have been enabled with a PAK:

- ipbasek9
- securityk9

In this example, the uck9 and datak9 feature sets have not been enabled.

References

3.3.4 IOS Licensing Facts

resources\text\t_ios_licensing_ccna7\q_ios_licensing_08_ccna7.question.xml

Question 9: ✓ Correct

Which mode is required to install the license on a Cisco device?

○ ROMmon mode

○ Global configuration mode

→ ● Privileged exec mode

○ User exec mode

Explanation

Privileged exec mode provides a user with editing capabilities. Use the license install command in privileged exec mode to install the file.

Global configuration mode provides advanced access to device configurations.

User exec mode provides the most basic level of access to a Cisco device.

ROMmon mode is a command line mode that is used to recover a lost or forgotten password, reinstall the IOS, or to format the flash file system.

References

3.3.4 IOS Licensing Facts

resources\text\t_ios_licensing_ccna7\q_ios_licensing_09_ccna7.question.xml

Question 10. ✓ Correct

Which command would you use to show you the following information in a table?

- Feature name
- Enforcement
- Evaluation
- Subscription
- Enabled
- RightToUser

○ **show license**

○ **show license history**

○ **show license UDI**

→ ● **show license feature**

Explanation

Entering **show license feature** puts the license information in a table.

Verify that the license has been installed using the **show license** command. This command will present you with information about the name of the feature including:

- License type (either permanent or evaluation)
- License state (either active or in use)
- License count (how many licenses are available and in use)
- License priority (indicates the priority of the license as either high or low)

You can find the unique device identifier, or UDI, with the **show license UDI** command.

show license history is not a valid command.

References

3.3.4 IOS Licensing Facts

resources\text\t_ios_licensing_ccna7\q_ios_licensing_10_ccna7.question.xml

3.4.8 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 2/5/2025, 12:51:21 PM • **Time Spent:** 02:23

Score: 100%

Passing Score: 80%

Question 1

✓ Correct

During the initial setup of a router, which of the following commands would set the host name as LAS?

→ ● Router(config)#**hostname LAS**

○ Router>**ip dns LAS**

○ Router>**host LAS**

○ Router(config)#**host LAS**

Explanation

Router(config)#**hostname LAS** sets the hostname as LAS. After you execute this command, the command prompt will appear as LAS(config)#. The command must be executed after executing the commands **enable** and **configure terminal**.

The other commands do not produce the desired change.

References

2.6.3 Routers

2.6.4 Router Facts

resources\text\t_intflist_ccna7\q_intflist_01_ccna7.question.xml

Question 2

✓ Correct

You just installed a new router (RTR07) in a field office. As part of the initial setup, you want to configure a description for the eighth gigabit Ethernet interface. Which of the following would set the description to WAN to Main Office?

○ **RTR07(config)#int gi0/8**
RTR07(config)#int description WAN to Main Office

→ ● **RTR07(config)#int gi0/8**
RTR07(config-if)#description WAN to Main Office

○ **RTR07>int gi0/8**
RTR07>description WAN to Main Office

○ **RTR07(config)#int gi0/8 set description WAN to Main Office**

Explanation

The correct syntax for the commands are:

RTR07(config)#int gi0/8

RTR07(config-if)#description WAN to Main Office

The first command specifies the eighth gigabit Ethernet interface on the device. The second command sets the description.

References

2.6.3 Routers

2.6.4 Router Facts

resources\text\t_intflist_ccna7\q_intflist_02_ccna7.question.xml

Question 3 ✓ Correct

You want to add a description to the first serial interface on the router. Which commands would you use?

○ **int fa 0**
description BOS to SFO

→ ● **int ser 0**
description BOS to SFO

○ **int ser 0**
set description BOS to SFO

○ **int fa 0**
add description BOS to SFO

Explanation

To add the description for the first serial interface on the router. you would use the following commands.

int ser 0

description BOS to SFO

The other commands will not add a description.

References

3.4.2 Hostname and Description Command List

resources\text\t_intflist_ccna7\q_intflist_03_ccna7.question.xml

Question 4 ✓ Correct

You are troubleshooting a router at the console. You issued the following command at the CLI:

```
pdx#debug arp
```

You see debug output, but the output scrolls past faster than you can read. What two commands allow you to view debug output one page at a time? (Select two.)

→ ☑ show log

→ ☑ logging buffered

□ no logging console

□ terminal debug output 1

□ debug scrolling off

Explanation

Use the **logging buffered** command to send debug output to RAM, which you can then view one page at a time with the **show log** command.

References

3.4.4 Screen Output Management Facts

resources\text\t_soutp_ccna7\q_soutp_01_ccna7.question.xml

Question 5 ✓ Correct

You have a test lab that you use to test different configurations before deploying them in your live network. You have been testing several commands from configuration mode, then going back to enable mode to view the running configuration. Every time you exit configuration mode, the following output is displayed:

```
%SYS-5-CONFIG_I: Configured from console by console
```

What command can stop these messages from appearing on your screen?

○ **terminal no monitor**

○ **no syslog**

○ **terminal no notify**

→ ● **no logging console**

Explanation

The IOS generates messages when different events occur. These events are called syslog messages. By default, the console port always receives syslog messages. The **no logging console** command tells the router not to send syslog messages to the console.

References

3.4.4 Screen Output Management Facts

resources\text\t_soutp_ccna7\q_soutp_02_ccna7.question.xml

Question 6. ✓ Correct

You would like to see logging message from IOS appear on the terminal. However, IOS does not send log messages to a terminal session over IP when using a remote SSH session. What command would send terminal output to the terminal session?

→ ● **terminal monitor**

○ **logging synchronous**

○ **show log**

○ **logging buffered**

Explanation

The **terminal monitor** command displays debugging output to the terminal session.

The **logging synchronous** command causes logging messages to be displayed above the command line instead of interrupting your requested session output and prompts.

You can use the **show log** command to show logs.

You can send logging information to RAM by entering **logging buffered**. You can then view the information one screen at a time by entering show log.

References

3.4.4 Screen Output Management Facts

resources\text\t_soutp_ccna7\q_soutp_03_ccna7.question.xml

Question 7 ✓ Correct

How does configuring banners add to the security of your router?

○ Banners identify allowed traffic by protocol or source or destination address, allowing you to control which devices or applications have access.

→ ○ Banners provide a notice of intent, informing users that access is controlled or that activity may be logged.

○ Banners turn on password checking, allowing only those with the correct password to gain access to the router.

○ Banners obscure the intended use of the device, making it harder for attackers to perform reconnaissance attacks.

○ Banners encrypt passwords, making them impossible to recognize and difficult to crack.

Explanation

A banner is a message that shows before and after login. Banners can be useful in security by informing connecting users of the proper use of a device. For example, the banner could state that only administrators are allowed access. Banners can also inform users that actions might be logged or tracked. In many locations, you cannot monitor users unless they are informed that their actions are tracked. Banners could prove useful if you ever need to prosecute someone. With an appropriate banner in place, unauthorized users cannot claim that they didn't know such action was not allowed.

Use the **login** command to require a password for a console or VTY connection. Use the **service password-encryption** command to provide simple encryption of passwords in the configuration file. Use an access list to control traffic based on protocol or IP address.

References

3.4.5 Banner Command List

resources\text\t_bannlist_ccna7\q_bannlist_01_ccna7.question.xml

Question 8 ✓ Correct

Following are three banner types that can be configured on a router:

- exec
- motd
- login

If all three banners were configured, in which order would they display when a Telnet session is used to connect to the router?

○ login, exec, motd

○ login, motd, exec

→ ● motd, login, exec

○ exec, motd, login

○ motd, exec, login

Explanation

Banners display in the following order:

1. The motd (message of the day) banner displays as soon as the connection is made.
2. The login banner displays immediately before the Telnet login prompt.
3. The exec banner displays after a successful login.

References

3.4.5 Banner Command List

resources\text\t_bannlist_ccna7\q_bannlist_02_ccna7.question.xml

Question 9 ✓ Correct

When you start up your router, you see the following messages:

```
Have a nice day!
The grass grows green
User Access Verification

Password:
The sky is blue
Router>
```

For security purposes, you would like to change the message **The grass grows green** to read **Only administrator access is allowed**. Which command should you use?

○ **banner motd *Only administrator access is allowed***

→ ● **banner login *Only administrator access is allowed***

○ **banner incoming *Only administrator access is allowed***

○ **banner exec *Only administrator access is allowed***

Explanation

The login banner shows immediately before the User Access Verification line. The first banner to display is the motd (message of the day) banner. The exec banner displays after a successful login.

References

3.4.5 Banner Command List

resources\text\t_bannlist_ccna7\q_bannlist_03_ccna7.question.xml

Question 10. ✓ Correct

After the completion of regularly scheduled maintenance on a router, you want to remove the message-of-the-day (MOTD) banner. Which command will accomplish that task?

○ **remove banner motd**

→ ● **no banner motd**

○ **banner motd clear**

○ **banner motd *clear***

Explanation

no banner motd command removes the message-of-the-day banner.

The other command will produce errors or, in the case of **banner motd *clear***, will set the message-of-the-day banner to the word *clear*.

References

3.4.5 Banner Command List

resources\text\t_bannlist_ccna7\q_bannlist_04_ccna7.question.xml

3.5.11 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 2/5/2025, 2:06:37 PM • **Time Spent:** 01:27

Score: 100%

Passing Score: 80%

Question 1

✓ Correct

Which of the following is the most important thing to do to prevent console access to the router?

○ Implement an access list to prevent console connections.

→ ● Keep the router in a locked room.

○ Disconnect the console cable when not in use.

○ Set the console and enable secret passwords.

Explanation

To control access to the router console, you must keep the router in a locked room. A console connection can only be established with a direct physical connection to the router. If the router is in a locked room, only those with access will be able to make a console connection. In addition, even if you had set console passwords, users with physical access to the router could perform router password recovery and gain access.

References

3.5.1 Password Levels

3.5.2 Configure Line Level Passwords

3.5.4 Device Password Facts

3.5.5 Configure Enable Mode Passwords

3.5.8 Router Password Recovery

3.5.9 Recover a Forgotten Password

3.5.10 Password Recovery Facts

resources\text\t_linelist_ccna7\q_linelist_01_ccna7.question.xml

Question 2 ✓ Correct

You want to prevent users from accessing a router through a Telnet session. What should you do?

→ ● For the VTY lines, add the **login** parameter and remove any passwords.

○ For the console line, add the **login** parameter and configure a password.

○ For the console line, set a password but remove the **login** parameter.

○ For the VTY lines, add the **login** parameter and configure a password.

○ For the console line, add the **login** parameter and remove any passwords.

○ For the VTY lines, set a password, but remove the **login** parameter.

Explanation

To prevent Telnet sessions with the router, configure the VTY lines with the **login** parameter, but without a password. This requires a password for login. But because no password has been configured, access will be denied with the message "Password required but not set."

References

3.5.1 Password Levels

3.5.2 Configure Line Level Passwords

3.5.4 Device Password Facts

3.5.5 Configure Enable Mode Passwords

3.5.8 Router Password Recovery

3.5.9 Recover a Forgotten Password

3.5.10 Password Recovery Facts

resources\text\t_linelist_ccna7\q_linelist_02_ccna7.question.xml

Question 3 ✓ Correct

You want users to enter a password before being able to access the router through a Telnet session. You use the following commands:

```
router#config t
router(config)#line vty 0 4
router(config-line)#password cisco
router(config-line)#exit
router(config)#exit
```

You open a Telnet session with the router and discover that the session starts without being prompted for a password. What should you do?

○ Use the **enable secret** command in line configuration mode to set the password.

○ In global configuration mode, configure the **enable secret** password.

→ ● In line configuration mode, add the **login** parameter.

○ Repeat the same configuration steps in **line con 0** mode.

Explanation

To require a password for a Telnet session, you must configure a password and add the **login** parameter. You can think of this command as turning password checking on. If a password is set but the **login** is missing, the password will not be required. If you add **login** but do not set a password, access will be denied (the prompt for a password will not be shown).

References

3.5.1 Password Levels

3.5.2 Configure Line Level Passwords

3.5.4 Device Password Facts

3.5.5 Configure Enable Mode Passwords

3.5.8 Router Password Recovery

3.5.9 Recover a Forgotten Password

3.5.10 Password Recovery Facts

resources\text\t_linelist_ccna7\q_linelist_03_ccna7.question.xml

Question 4 ✓ Correct

What is the main security weakness associated with the **service password-encryption** command?

- ○ Passwords are rendered as 4-digit hexadecimal values.
- → ● Passwords are easily broken.
- ○ Passwords are kept in the configuration register.
- ○ Password values are transposed.

Explanation

The **service password-encryption** command encrypts all passwords as type 7 passwords. Encrypted type 7 passwords are not secure and are easily broken. But the encrypted values do provide some level of protection from someone looking over your shoulder after having issued the **show running-config** command.

Passwords are never kept in the configuration register; they are kept in the startup-config file.

References

3.5.1 Password Levels

3.5.2 Configure Line Level Passwords

3.5.4 Device Password Facts

3.5.5 Configure Enable Mode Passwords

3.5.8 Router Password Recovery

3.5.9 Recover a Forgotten Password

3.5.10 Password Recovery Facts

resources\text\t_linelist_ccna7\q_linelist_04_ccna7.question.xml

Question 5 ✓ Correct

While configuring a new router, you use the following commands:

```
Router(config)#enable password cisco
Router(config)#enable secret highway
Router(config)#username admin password television
Router(config)#line con 0
Router(config-line)#password airplane
Router(config-line)#login
Router(config-line)#line vty 0 4
Router(config-line)#password garage
Router(config-line)#login
```

Which password would you use to open a Telnet session to the router?

→ ● garage

○ airplane

○ cisco

○ highway

Explanation

The password set for VTY lines is used to establish the Telnet session. The password set for line con 0 is used to make a connection to the console. After you connect to the console or the Telnet connection, you are in user EXEC mode.

To enter privileged EXEC mode, use the enable secret password. If the enable secret password is not set, use the enable password.

References

3.5.1 Password Levels

3.5.2 Configure Line Level Passwords

3.5.4 Device Password Facts

3.5.5 Configure Enable Mode Passwords

3.5.8 Router Password Recovery

3.5.9 Recover a Forgotten Password

3.5.10 Password Recovery Facts

resources\text\t_linelist_ccna7\q_linelist_05_ccna7.question.xml

Question 6. ✓ Correct

Which of the following commands configures a password to switch to privileged EXEC mode and saves the password using MD5 hashing?

○ **service password-encryption**

○ **enable password**

○ **password**

→ ● **enable secret**

Explanation

Use **enable secret** to configure a password for privileged EXEC mode that is stored using MD5 hashing.

enable password sets an unencrypted version of the password. **password** configures configure console and VTY passwords. **service password-encryption** adds simple encryption to the enable password. However, this encryption can be broken more easily than the MD5 hash used for the enable secret password.

References

3.5.1 Password Levels

3.5.2 Configure Line Level Passwords

3.5.4 Device Password Facts

3.5.5 Configure Enable Mode Passwords

3.5.8 Router Password Recovery

3.5.9 Recover a Forgotten Password

3.5.10 Password Recovery Facts

resources\text\t_linelist_ccna7\q_linelist_06_ccna7.question.xml

Question 7 ✓ Correct

You are at a customer site and need to access their router. The previous administrator left the company and did not document the password to the device. Which of the following would you access to start the password recovery process?

- ○ IOS
- ○ BIOS
- ○ bootstrap
- → ● ROMmon

Explanation

To start the recovery process, access ROMmon mode on the device. ROMmon mode can be accessed via a console by using a break sequence during the boot process. Removing external flash memory while the device is powered off will also cause the device to boot in ROMmon mode.

Bootstrap is the boot loader software that loads from the ROM into RAM and loads the IOS operating system.

Accessing IOS does not provide the means to reset a lost or unknown password.

Accessing the BIOS does not provide a way to reset a lost or unknown password.

References

3.5.1 Password Levels

3.5.2 Configure Line Level Passwords

3.5.4 Device Password Facts

3.5.5 Configure Enable Mode Passwords

3.5.8 Router Password Recovery

3.5.9 Recover a Forgotten Password

3.5.10 Password Recovery Facts

resources\text\t_passwrec_ccna7\q_passwrec_01_ccna7.question.xml

Question 8 ✓ Correct

As part of the password recovery process on a router, you want the device to ignore the startup config file when the device is rebooted. Which of the following commands would you use to do this?

○ **copy running-config startup-config**

→ ● **confreg 0x2142**

○ **enable**

○ **reset**

Explanation

You can use **confreg 0x2142** to change the configuration register to 0x2142. This instructs the device to ignore the startup-config file the next time your device starts.

The other commands do not accomplish the task. **copy running-config startup-config** will erase your startup configuration instead of telling the device to ignore the startup config.

References

3.5.1 Password Levels

3.5.2 Configure Line Level Passwords

3.5.4 Device Password Facts

3.5.5 Configure Enable Mode Passwords

3.5.8 Router Password Recovery

3.5.9 Recover a Forgotten Password

3.5.10 Password Recovery Facts

resources\text\t_passwrec_ccna7\q_passwrec_02_ccna7.question.xml

Question 9: ✓ Correct

After configuring a router to ignore the startup configuration when the device boots, what command would you use to tell the device to load the startup configuration upon boot?

○ **confreg 0x2142**

→ ● **confreg 0x2102**

○ **restart**

○ **copy startup-config running-config**

Explanation

Using the command **confreg 0x2102** changes the configuration register to look for the startup configuration file on boot.

The command **confreg 0x2142** sets the configuration register to ignore the startup configuration file.

The other commands are not used to change the configuration register.

References

3.5.1 Password Levels

3.5.2 Configure Line Level Passwords

3.5.4 Device Password Facts

3.5.5 Configure Enable Mode Passwords

3.5.8 Router Password Recovery

3.5.9 Recover a Forgotten Password

3.5.10 Password Recovery Facts

resources\text\t_passwrec_ccna7\q_passwrec_03_ccna7.question.xml

Question 10 ✓ Correct

One of the steps in the password recovery process for a router is to access the ROM monitor. Which of the following methods will accomplish this? (Select two.)

→ ☑ Use a break sequence during the boot process.

☐ Run the **confreg 0x2142** command.

→ ☑ Remove the external flash memory while the device is powered off and then boot.

☐ Boot into the BIOS.

☐ Run the **confreg 0x2102** command.

Explanation

Access ROMmon mode on your device. You can access ROMmon mode via a console by using a break sequence during the boot-up process. Removing external flash memory while the device is turned off will also cause a device to boot in ROMmon mode.

Using the **confreg 0x2142** command sets the configuration register so the device will ignore the startup config file when the device is rebooted.

Using the **confreg 0x2102** command changes the configuration register so the device will look to the startup config file on restart.

Booting into the BIOS does not enable ROMmon mode.

References

3.5.1 Password Levels

3.5.2 Configure Line Level Passwords

3.5.4 Device Password Facts

3.5.5 Configure Enable Mode Passwords

3.5.8 Router Password Recovery

3.5.9 Recover a Forgotten Password

3.5.10 Password Recovery Facts

resources\text\t_passwrec_ccna7\q_passwrec_04_ccna7.question.xml

3.6.9 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)

Date: 2/5/2025, 7:10:49 PM • **Time Spent:** 01:49

Score: 100%

Passing Score: 80%

Question 1 ✓ Correct

You are configuring a router that has a previous configuration. You need to turn CDP on for the entire router and turn it off for the serial 0/0/1 interface. Match each command on the left with its associated configuration task on the right.

Enter global configuration mode.

✓ **router#config t**

Turn CDP on for the router.

✓ **router(config)#cdp run**

Enter interface configuration mode.

✓ **router(config)#int s0/0/1**

Turn CDP off for the interface.

✓ **router(config-if)#no cdp enable**

Explanation

To configure CDP for the entire device, use the **cdp run**/**no cdp run** command in global configuration mode. To configure CDP for a specific interface, use **cdp enable**/**no cdp enable**. Use the following commands to complete the required tasks:

```
router#conf t
router(config)#cdp run
router(config)#int s0/0/1
router(config-if)#no cdp enable
```

References

3.6.1 Cisco Discovery Protocol (CDP)

3.6.2 Set Up CDP

3.6.3 CDP Command List

3.6.8 Support Non-Cisco Devices with LLDP

resources\text\t_cdplist_ccna7\q_cdplist_01_ccna7.question.xml

Question 2

✓ Correct

Which of the following commands would you use to modify the CDP packet exchange interval to send CDP packets every 30 seconds?

→ ● **cdp timer 30**

○ **cdp holdtime 30**

○ **cdp interval 30**

○ **cdp exchange 30**

○ **cdp broadcast 30**

Explanation

Use the **cdp timer** command in global configuration mode to modify the frequency with which CDP packets are sent from the router.

References

3.6.1 Cisco Discovery Protocol (CDP)

3.6.2 Set Up CDP

3.6.3 CDP Command List

3.6.8 Support Non-Cisco Devices with LLDP

resources\text\t_cdplist_ccna7\q_cdplist_02_ccna7.question.xml

Question 3 ✓ Correct

You are physically seated at a host connected to the console of the Seattle router as shown in the exhibit. You need to know what IP address has been configured on the E0 interface on the New York router.

What are your options? (Select two.)

→ ☑ Telnet to New York. From privileged mode, type **show interface E0**.

□ From privileged mode on Seattle, type **show cdp neighbors detail**.

□ Telnet to Toronto. From privileged mode, type **show interface E0**.

□ Telnet to Seattle. From privileged mode, type **show cdp neighbors detail**.

→ ☑ Telnet to Toronto. From privileged mode, type **show cdp neighbors detail**.

Explanation

You could either Telnet to Toronto and use the **show cdp neighbors detail** command, or you could Telnet to New York and in privileged mode type **show interface E0**.

Typing **show cdp neighbors detail** from the Seattle router will only show the interfaces of directly connected neighbors like Toronto. CDP cannot hop across devices to display information about neighbors on the other side.

Typing **show interface E0** from the Toronto router will only display information about the E0 interface on the Toronto router.

References

3.6.1 Cisco Discovery Protocol (CDP)

3.6.2 Set Up CDP

3.6.3 CDP Command List

3.6.8 Support Non-Cisco Devices with LLDP

resources\text\t_cdplist_ccna7\q_cdplist_03_ccna7.question.xml

Question 4 ✓ Correct

For security reasons, you want to prevent the Toronto router from sharing any information about itself with neighboring devices. Which command should you run on the Toronto router?

○ Toronto#**no cdp run**

○ Toronto#**no cdp enable**

→ ● Toronto(config)#**no cdp run**

○ Toronto(config)#**no cdp enable**

Explanation

To disable CDP on the router, use the **no cdp run** command in global configuration mode.

no cdp enable disables CDP on a specific interface only. It must be issued from interface configuration mode. Neither **no cdp enable** nor **no cdp run** can be issued from privileged mode.

References

3.6.1 Cisco Discovery Protocol (CDP)

3.6.2 Set Up CDP

3.6.3 CDP Command List

3.6.8 Support Non-Cisco Devices with LLDP

resources\text\t_cdplist_ccna7\q_cdplist_04_ccna7.question.xml

Question 5 ✓ Correct

You have just entered the configure terminal on a router and specified a gigabit interface. You want to disable CDP on that interface, but you want to keep CDP enabled on the device. Which of the following commands would you use?

○ Router(config-if)#**no cdp**

○ Router(config-if)#**cdp run**

○ Router(config-if)#**no cdp run**

→ ● Router(config-if)#**no cdp enable**

Explanation

no cdp enable disables CDP on the specified interface, but keeps CDP enabled for the device.

no cdp run disables CDP for all interfaces on the device.

cdp run enables CDP for all interfaces on the device.

no cdp is an incomplete command.

References

3.6.1 Cisco Discovery Protocol (CDP)

3.6.2 Set Up CDP

3.6.3 CDP Command List

3.6.8 Support Non-Cisco Devices with LLDP

resources\text\t_cdplist_ccna7\q_cdplist_05_ccna7.question.xml

Question 6 ✓ Correct

Which of the following protocols enables Cisco devices to discover non-Cisco devices?

○ DCBXP

→ ● LLDP

○ CDP

○ TLV

Explanation

Cisco devices support Link Layer Discovery Protocol (LLDP), which is a vendor-neutral device discovery protocol that allows network devices to advertise information about themselves.

TLV descriptions are used by LLDP to communicate type, length, and value information to other devices on the network. CDP is Cisco's vendor-specific discovery protocol. DCBXP is an extension of LLDP that is used to announce, exchange, and negotiate node parameters between peer network devices.

References

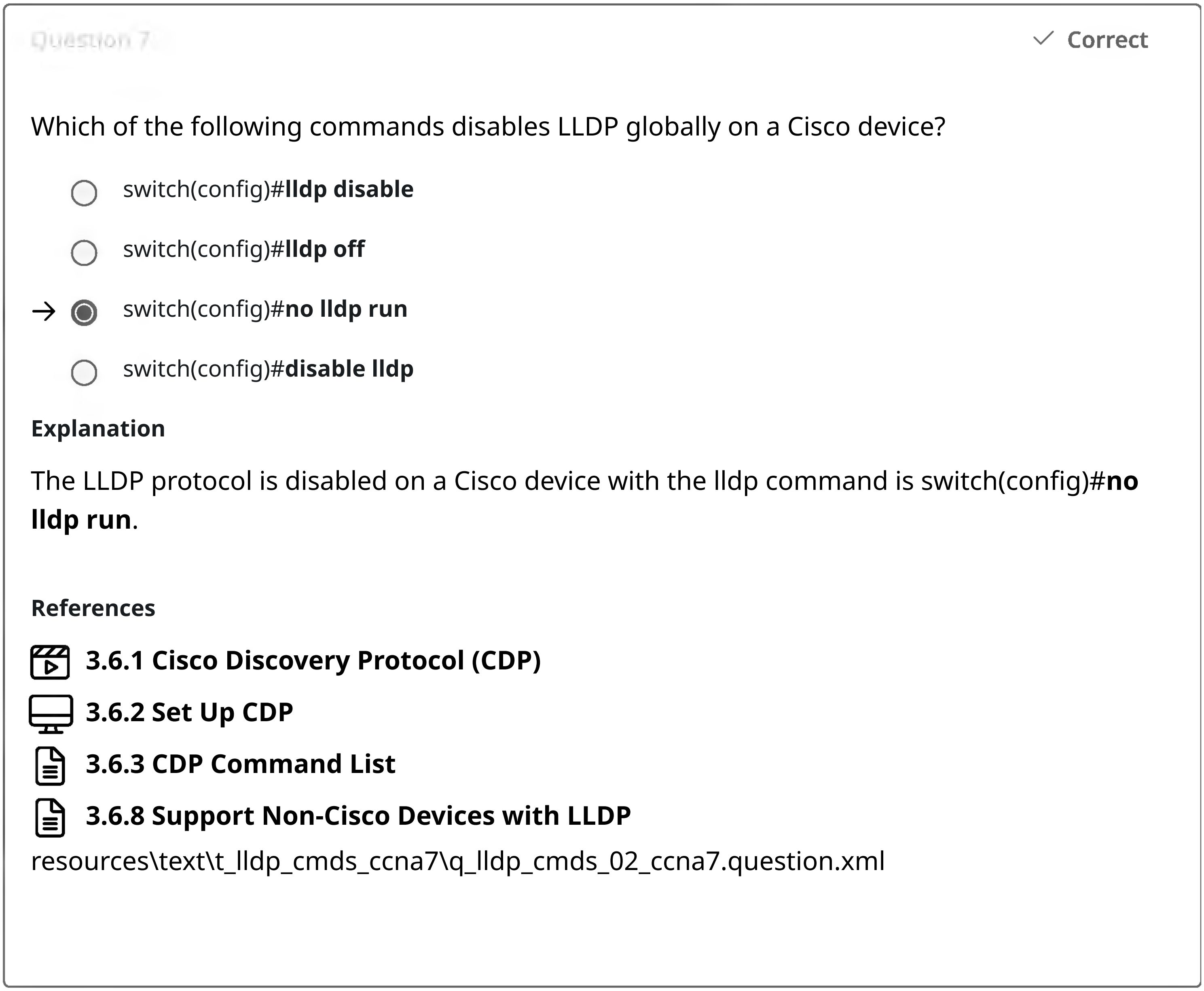
3.6.1 Cisco Discovery Protocol (CDP)

3.6.2 Set Up CDP

3.6.3 CDP Command List

3.6.8 Support Non-Cisco Devices with LLDP

resources\text\t_lldp_cmds_ccna7\q_lldp_cmds_01_ccna7.question.xml



Question 7

✓ Correct

Which of the following commands disables LLDP globally on a Cisco device?

○ switch(config)#**lldp disable**

○ switch(config)#**lldp off**

→ ● switch(config)#**no lldp run**

○ switch(config)#**disable lldp**

Explanation

The LLDP protocol is disabled on a Cisco device with the lldp command is switch(config)#**no lldp run**.

References

3.6.1 Cisco Discovery Protocol (CDP)

3.6.2 Set Up CDP

3.6.3 CDP Command List

3.6.8 Support Non-Cisco Devices with LLDP

resources\text\t_lldp_cmds_ccna7\q_lldp_cmds_02_ccna7.question.xml

Question 8 ✓ Correct

Jaden is the network engineer at a branch office. There are non-Cisco devices on the network that Jaden would like to make sure are discovered by the Cisco router. Jaden has just enabled the Link Layer Discovery Protocol (LLDP) on the router. Which of the following is true about LLDP?

○ Enabled by default.

○ Does not need to be enabled globally before being used.

○ Uses the same commands as CDP.

→ ● Configured on a per-interface basis.

Explanation

When using LLDP, keep in mind that LLDP:

- Is configured on a per-interface basis.
- Is disabled by default.
- Uses similar configuration commands as CDP.
- Must be enabled globally before being used.

References

3.6.1 Cisco Discovery Protocol (CDP)

3.6.2 Set Up CDP

3.6.3 CDP Command List

3.6.8 Support Non-Cisco Devices with LLDP

resources\text\t_lldp_cmds_ccna7\q_lldp_cmds_03_ccna7.question.xml

Question 9. ✓ Correct

To show all non-Cisco devices using LLDP, which of the following commands would you execute on a Cisco router?

○ Router#**show lldp traffic**

○ Router(config-if)#**lldp transmit**

→ ● Router#**show lldp neighbors**

○ Router#**show lldp interface**

Explanation

show lldp neighbors displays information about all neighboring non-Cisco devices, including:

- Local interface
- Device ID
- Port ID
- Holdtime
- Capability

show lldp interface displays information about interfaces that have LLDP enabled, including transmit and receive configuration, as well as the current state.

show lldp traffic shows the current state of LLDP traffic, including the number of frames in and out, the number of dropped frames, and the number of Type-Length-Values (TLVs) discarded or un-recognized.

lldp transmit disables the interface from sending LLDP information.

References

3.6.1 Cisco Discovery Protocol (CDP)

3.6.2 Set Up CDP

3.6.3 CDP Command List

3.6.8 Support Non-Cisco Devices with LLDP

resources\text\t_lldp_cmds_ccna7\q_lldp_cmds_04_ccna7.question.xml

Question 10 ✓ Correct

The default amount of time that a device will hold information about its neighbors using LLDP is 120 seconds. Which of the following command allows you to change the value?

○ Router#**show lldp entry neighbor_name**

→ ● Router(config)#**lldp holdtime [number of seconds]**

○ Router#**clear lldp counters**

○ Router(config)#**lldp timer [number of seconds]**

Explanation

lldp holdtime [number of seconds] specifies the amount of time that information in a packet is still valid. The default is 120 seconds. Use the no lldp holdtime command to reset the value to its default.

lldp timer [number of seconds] specifies how often LLDP packets are exchanged. The default is 30 seconds. Use the **no lldp timer** command to reset the value to its default.

clear lldp counters resets traffic counters to 0.

show lldp entry neighbor_name displays similar information for the specified LLDP neighbor.

References

3.6.1 Cisco Discovery Protocol (CDP)

3.6.2 Set Up CDP

3.6.3 CDP Command List

3.6.8 Support Non-Cisco Devices with LLDP

resources\text\t_lldp_cmds_ccna7\q_lldp_cmds_05_ccna7.question.xml

4.1.9 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)

Date: 2/10/2025, 10:15:32 AM • **Time Spent:** 01:39

Score: 100%

Passing Score: 80%

Question 1 ✓ Correct

What is the decimal format of the following binary IP address?

11001110.00111010.10101010.01000011

→ ● 206.58.170.67

○ 190.42.154.51

○ 238.90.202.99

○ 205.57.169.66

Explanation

The decimal equivalent of the 11001110.00111010.10101010.01000011 IP address is 206.58.170.67. To convert from binary to decimal, use the decimal equivalent of the following binary numbers:

- 10000000: 128
- 01000000: 64
- 00100000: 32
- 00010000: 16
- 00001000: 8
- 00000100: 4
- 00000010: 2
- 00000001: 1

To find the decimal form of a binary number, add up each decimal equivalent for each 1 bit in the address. For example, the equation for the number 11001110 is 128 + 64 + 8 + 4 + 2 = 206.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

resources\text\t_numbering_ccna7\q_numbering_01_ccna7.question.xml

Question 2 ✓ Correct

What is the correct binary form of the decimal IP address 192.168.1.1?

○ 00001010.10101000.00000001.00000001

○ 11000000.10101000.00000010.00000001

○ 10101100.00010001.00000001.00000001

→ ● 11000000.10101000.00000001.00000001

Explanation

The decimal equivalent of the 11000000.10101000.00000001.00000001 IP address is 192.168.1.1. To convert from binary to decimal, use the decimal equivalent of the following binary numbers:

- 10000000: 128
- 01000000: 64
- 00100000: 32
- 00010000: 16
- 00001000: 8
- 00000100: 4
- 00000010: 2
- 00000001: 1

For each bit position with a 1 value in the binary form of the address, add the decimal values for that bit. For example, the decimal equivalent of 11000000 is: 128 + 64 + 0 + 0 + 0 + 0 + 0 + 0 = 192

The decimal equivalent of 10101100.00010001.00000001.00000001 is 172.17.1.1.

The decimal equivalent of 00001010.10101000.00000001.00000001 is 10.168.1.1.

The decimal equivalent of 11000000.10101000.00000010.00000001 is 192.168.2.1.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

resources\text\t_numbering_ccna7\q_numbering_02_ccna7.question.xml

Question 3.

✓ Correct

Match each decimal value on the left with the corresponding hexadecimal value on the right. Not all decimal values have a corresponding hexadecimal value.

11

✓ 17

B

✓ 11

D

✓ 13

F

✓ 15

C

✓ 12

10

✓ 16

Explanation

Hexadecimal is a Base 16 numbering system, which means there are 16 characters possible for each number place. These characters go from 0 to 9, as decimal does; however, hexadecimal uses the letter A to represent the decimal number 10, B to represent 11, and so on up to F, which represents 15. The easiest way to convert between decimal and hexadecimal is to memorize the corresponding values for each hexadecimal number using the following tables.

Hex Value	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Decimal Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Hex Value	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
Decimal Value	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

resources\text\t_numbering_ccna7\q_numbering_03_ccna7.question.xml

Question 4 ✓ Correct

Which of the following are valid IP addresses? (Select three.)

□ 137.65.256.1

□ 256.1.1.1

→ ☑ 172.17.1.3

→ ☑ 137.65.1.1

□ 137.65.1.257

→ ☑ 224.0.0.1

□ 10.256.1.1

Explanation

An IPv4 address is a 32-bit binary number represented as four octets (four 8-bit values). Each octet is separated by a period. Because each octet is 8 bits long, the smallest possible decimal value for a single octet is 0, while the largest possible decimal value is 255. In this example, the following are valid IP addresses:

- 137.65.1.1
- 172.17.1.3
- 224.0.0.1

The other addresses are not valid because they contain values larger than 255.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

📄 **4.2.2 Subnet Facts**

🎬 **4.2.3 Subnet Math**

📄 **4.2.4 Subnet Math Facts**

🎬 **4.2.5 Variable Length Subnet Masking (VLSM)**

📄 **4.2.6 VLSM Facts**

📄 **4.2.7 Subnet Operations Facts**

🎬 **4.3.1 Subnet Design**

🖥 **4.3.2 Configure Subnets**

📄 **4.3.3 Subnet Design Facts**

resources\text\t_ip_addclass_ccna7\q_ip_addclass_01_ccna7.question.xml

Question 5 ✓ Correct

A workstation has been assigned the following IP addressing information:

- IP address: 192.168.1.26
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.1.254
- DNS server: 192.168.1.1

Given this information, what is the network IP address of this workstation?

○ 192.0.0.0

○ 192.168.0.0

→ ● 192.168.1.0

○ 192.168.1.255

Explanation

The IP address includes both the network and the host address. The subnet mask is a 32-bit number associated with each IP address that identifies the network portion of the address. In binary form, the subnet mask is always a series of 1s followed by a series of 0s (1s and 0s are never mixed in sequence in the mask). In this example, the decimal form of the subnet mask is 255.255.255.0. This specifies that the network address in this example is 192.168.1.0

192.168.1.255 is the broadcast address for this network.

A network address of 192.168.0.0 would require a subnet mask of 255.255.0.0.

A network address of 192.0.0.0 would require a subnet mask of 255.0.0.0.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_ip_addclass_ccna7\q_ip_addclass_02_ccna7.question.xml

Question 6. ✓ Correct

A network host has an IP address of 137.65.1.2 assigned to it. Given that the network uses the default classful subnet mask, what is the default routing prefix for this address using CIDR subnet mask notation?

→ ● /16

○ /24

○ /32

○ /8

Explanation

Because 137.65.1.2 falls within the range of 128.0.0.0 to 191.255.255.255, it is a class B address and uses a default subnet mask of 255.255.0.0. Therefore, the default routing prefix is /16.

/8 is the default routing prefix for class A IP addresses, while /24 is the default routing prefix for class C IP addresses. A default routing prefix of /32 would use all available bits in an IPv4 address for the network address, leaving no host addresses available.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

- **4.2.6 VLSM Facts**
- **4.2.7 Subnet Operations Facts**
- **4.3.1 Subnet Design**
- **4.3.2 Configure Subnets**
- **4.3.3 Subnet Design Facts**
- **4.4.1 Route Summarization Overview**
- **4.4.2 Route Summarization Network Design**
- **4.4.3 Route Summarization Facts**
- **4.4.4 Configure Route Summarization**
- **4.4.5 Route Summarization Command List**
- **6.2.3 Set Up Static Routing**
- **6.4.1 IPv4 Routing Overview**
- **6.4.2 Routing Troubleshooting Tools**
- **6.4.3 Use Ping and Traceroute**
- **6.4.4 Host Configuration Issues**
- **6.4.5 Router Configuration Issues**
- **6.4.6 Use Show Commands on the Router**
- **6.4.7 Troubleshooting IPv4 Routing Facts**
- **6.5.5 IP Troubleshooting Utility Facts**
- **6.5.6 IP Troubleshooting Facts**

resources\text\t_ip_addclass_ccna7\q_ip_addclass_03_ccna7.question.xml

Question 7 ✓ Correct

Your network uses a network address of 137.65.0.0 with a subnet mask of 255.255.0.0.

How many IP addresses are available for assignment to network hosts on this network?

→ ● 65534

○ 254

○ 16777214

○ 2

Explanation

Given a network address and subnet mask, you can have 2 to the *n*th power - 2 hosts per subnet. Begin by converting the subnet mask to a binary number. To find the number of valid hosts, n = the number of unmasked bits in the mask. In this example, there are 16 unmasked bits in the mask. Therefore, the number of available hosts is 2 to the 16th power - 2, which equals 65534.

References

- **4.1.1 Numbering Systems**
- **4.1.2 Numbering System Facts**
- **4.1.3 IP Addresses**
- **4.1.4 IP Address Format**
- **4.1.5 IP Address Classes**
- **4.1.6 IP Address Class Facts**
- **4.1.7 Public vs. Private IP Addresses**
- **4.1.8 Public and Private IP Address Facts**
- **4.2.1 Subnets**
- **4.2.2 Subnet Facts**
- **4.2.3 Subnet Math**
- **4.2.4 Subnet Math Facts**
- **4.2.5 Variable Length Subnet Masking (VLSM)**
- **4.2.6 VLSM Facts**
- **4.2.7 Subnet Operations Facts**

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_ip_addclass_ccna7\q_ip_addclass_04_ccna7.question.xml

Question 8 ✓ Correct

Which of the following IP addresses is a valid IP address for a host on a public network?

○ 172.16.254.12

→ ● 142.15.6.1

○ 192.168.16.45

○ 10.3.125.2

Explanation

A public network is a network that does not limit traffic to members of a corporation or other group. The internet is an example of a public network. Certain sets of IP addresses are reserved for private networks only and cannot be used on public networks. They are:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

resources\text\t_prvpub_ccna7\q_prvpub_01_ccna7.question.xml

Question 9: ✓ Correct

Which of the following are private IP addresses? (Select two.)

□ 198.162.1.12

→ ☑ 192.168.250.11

□ 127.99.1.155

→ ☑ 10.244.12.16

□ 172.32.119.199

Explanation

10.244.12.16 and 192.168.250.11 are private IP addresses. Private addresses fall within the following range:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

Private addresses are used only within a private network and cannot be used on the internet. A service such as Network Address Translation (NAT) is required to translate private addresses into public addresses.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

resources\text\t_prvpub_ccna7\q_prvpub_02_ccna7.question.xml

Question 10 ✓ Correct

Which of the following devices is most likely to be assigned a public IP address?

○ A workstation on your company network that has internet access.

○ A database server used by your company's website for storing customer information.

○ A router on your company network that segments your LAN into two subnets.

→ ● A router that connects your home network to the internet.

Explanation

To connect a private network, home or business to the internet, you must have a router with a public IP address. The public address allows hosts on the internet to send packets to the router.

When you connect a private network to the internet, only the router interface connected to the internet needs a public address. You can then use Network Address Translation (NAT) and assign private addresses to hosts on your private network (including all routers on the private network). The NAT router translates your private addresses into the public address.

You can even use NAT to place publicly available hosts, such as web servers, on the private network (although these servers are often placed in a special subnet connected to the internet and assigned public addresses). With port address translation, incoming messages sent to the publicly available servers are relayed to the private network. Servers that hold confidential data, such as database servers, are normally placed on the private network, and can only be contacted directly by the necessary devices (such as a web server).

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

resources\text\t_prvpub_ccna7\q_prvpub_03_ccna7.question.xml

4.2.8 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)

Date: 2/10/2025, 11:52:40 AM • **Time Spent:** 03:03

Score: 100%

Passing Score: 80%

Question 1. ✓ Correct

Your network has a network address of 172.17.0.0 with a subnet mask of 255.255.255.0.

Which of the following are true concerning this network? (Select two.)

→ ☑ 172.17.0.255 is the network broadcast address.

☐ 256 IP addresses can be assigned to host devices.

→ ☑ 254 IP addresses can be assigned to host devices.

☐ 172.17.255.255 is the network broadcast address.

☐ 172.17.0.1 is reserved for the default gateway.

Explanation

A Class B address can be subnetted to provide additional subnet addresses. Notice how, by using a custom subnet mask, the Class B address looks like a Class C address:

- Network address: 172.17.0.0
- Subnet mask: 255.255.255.0
- Number of subnets: 256
- Number of hosts per subnet: 254 per subnet
- Subnet addresses: 172.17.1.0, 172.17.2.0, 172.17.3.0, and so on
- Host address ranges: 172.17.1.1 to 172.17.1.254, 172.17.2.1 to 172.17.2.254, 172.17.3.1 to 172.17.3.254, and so on

References

🎬 **4.1.1 Numbering Systems**

📄 **4.1.2 Numbering System Facts**

🎬 **4.1.3 IP Addresses**

🎬 **4.1.4 IP Address Format**

🎬 **4.1.5 IP Address Classes**

📄 **4.1.6 IP Address Class Facts**

🎬 **4.1.7 Public vs. Private IP Addresses**

📄 **4.1.8 Public and Private IP Address Facts**

🎬 **4.2.1 Subnets**

📄 **4.2.2 Subnet Facts**

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_ip_subn_ccna7\q_ip_subn_01_ccna7.question.xml

Question 2 ✓ Correct

You have two subnets on your private network, one with a 20-bit mask, and another with a 22-bit mask. How many available host addresses are there on each subnet? (Select two.)

□ 510

□ 512

→ ☑ 1022

□ 1024

□ 2046

□ 2048

→ ☑ 4094

□ 4096

Explanation

Subnets with masks shorter than 24 bits have the following number of hosts:

- 23-bits = 510
- 22-bits = 1022
- 21-bits = 2046
- 20-bits = 4094
- 19-bits = 8190
- 18-bits = 16382
- 17-bits = 32766

To calculate the number of hosts per subnet for masks shorter than 24-bits:

1. Start with a 24-bit mask and a magic number of 256.
2. For each bit you remove from the mask, double the magic number. For example, a 23-bit mask has a magic number of 512.
3. For each subnet, subtract the two reserved addresses (the subnet address and the broadcast address) from the magic number. For example, for a 23-bit mask, there are 512 - 2 = 510 hosts.

References

4.1.1 Numbering Systems

- 📄 4.1.2 Numbering System Facts
- 🎬 4.1.3 IP Addresses
- 🎬 4.1.4 IP Address Format
- 🎬 4.1.5 IP Address Classes
- 📄 4.1.6 IP Address Class Facts
- 🎬 4.1.7 Public vs. Private IP Addresses
- 📄 4.1.8 Public and Private IP Address Facts
- 🎬 4.2.1 Subnets
- 📄 4.2.2 Subnet Facts
- 🎬 4.2.3 Subnet Math
- 📄 4.2.4 Subnet Math Facts
- 🎬 4.2.5 Variable Length Subnet Masking (VLSM)
- 📄 4.2.6 VLSM Facts
- 📄 4.2.7 Subnet Operations Facts
- 🎬 4.3.1 Subnet Design
- 🖥 4.3.2 Configure Subnets
- 📄 4.3.3 Subnet Design Facts
- 🎬 4.4.1 Route Summarization Overview
- 🎬 4.4.2 Route Summarization Network Design
- 📄 4.4.3 Route Summarization Facts
- 🖥 4.4.4 Configure Route Summarization
- 📄 4.4.5 Route Summarization Command List
- 🖥 6.2.3 Set Up Static Routing
- 🎬 6.4.1 IPv4 Routing Overview
- 🎬 6.4.2 Routing Troubleshooting Tools
- 🖥 6.4.3 Use Ping and Traceroute
- 🎬 6.4.4 Host Configuration Issues
- 🎬 6.4.5 Router Configuration Issues
- 🖥 6.4.6 Use Show Commands on the Router
- 📄 6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

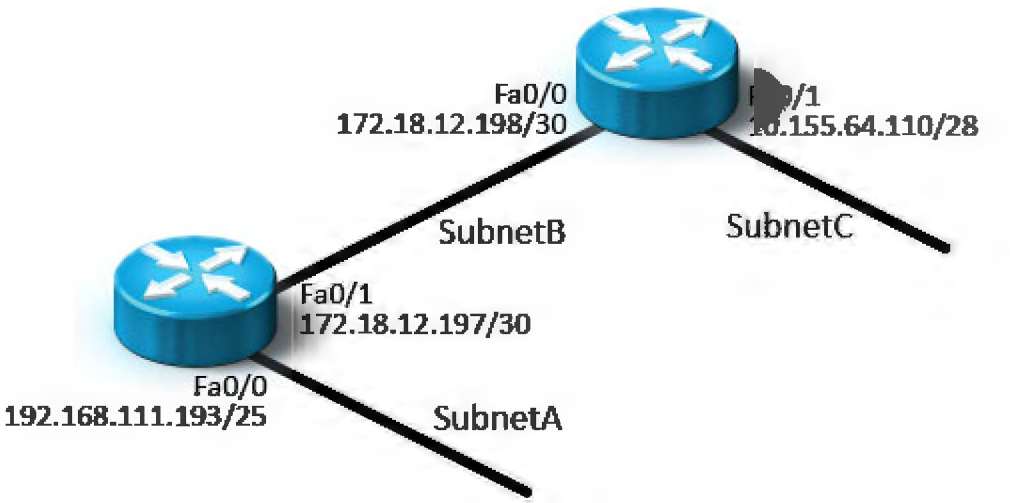
6.5.6 IP Troubleshooting Facts

resources\text\t_ip_subn_ccna7\q_ip_subn_02_ccna7.question.xml

✓ Correct

You have a small network with three subnets as shown in the exhibit. IP addresses for each router interface are also indicated in the exhibit.

How many IP addresses on each subnet remain that can be assigned to hosts?



○ SubnetA = 61, SubnetB = 0, SubnetC = 5

○ SubnetA = 126, SubnetB = 2, SubnetC = 14

○ SubnetA = 254, SubnetB = 6, SubnetC = 30

→ ● SubnetA = 125, SubnetB = 0, SubnetC = 13

○ SubnetA = 253, SubnetB = 4, SubnetC = 29

○ SubnetA = 62, SubnetB = 0, SubnetC = 6

Explanation

The scenario asks you for how many addresses remain that can be assigned to hosts. In this scenario, remember to remove the following addresses from each range:

- The subnet address.
- The broadcast address.
- Addresses assigned to the router interfaces. For Subnets A and C, one address on the subnet is assigned. For SubnetB, two addresses have been assigned.

The following mask values provide for the following number of hosts:

- Mask of /25 provides 126 host addresses, with one of those being used by the router.
- Mask of /30 provides for two host addresses. Both addresses are used by routers.
- Mask of /28 provides for 14 host addresses, with one of those being used by the router.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_ip_subn_ccna7\q_ip_subn_03_ccna7.question.xml

Question 4. ✓ Correct

Drag each binary subnet mask on the left to its appropriate decimal equivalent on the right.

255.0.0.0

✓ 11111111.00000000.00000000.00000000

255.255.255.128

✓ 11111111.11111111.11111111.10000000

255.224.0.0

✓ 11111111.11100000.00000000.00000000

255.255.0.0

✓ 11111111.11111111.00000000.00000000

255.255.255.252

✓ 11111111.11111111.11111111.11111100

Explanation

To perform subnetting operations, you will need to be proficient at converting decimal and binary numbers. When working with IP addresses, work with each octet separately. The following shows the decimal value for various binary values with a single 1 bit:

- 10000000: 128
- 01000000: 64
- 00100000: 32
- 00010000: 16
- 00001000: 8
- 00000100: 4
- 00000010: 2
- 00000001: 1

To find the decimal value of a number with multiple 1 bits, simply add the decimal value of the bits together. In this example:

- 11111111.11111111.00000000.00000000 = 255.255.0.0
- 11111111.00000000.00000000.00000000 = 255.0.0.0
- 11111111.11111111.11111111.10000000 = 255.255.255.128
- 11111111.11111111.11111111.11111100 = 255.255.255.252
- 11111111.11100000.00000000.00000000 = 255.224.0.0

References

🎬 **4.1.1 Numbering Systems**

📄 **4.1.2 Numbering System Facts**

🎬 **4.1.3 IP Addresses**

🎬 **4.1.4 IP Address Format**

🎬 **4.1.5 IP Address Classes**

📄 **4.1.6 IP Address Class Facts**

🎬 **4.1.7 Public vs. Private IP Addresses**

📄 **4.1.8 Public and Private IP Address Facts**

🎬 **4.2.1 Subnets**

📄 **4.2.2 Subnet Facts**

🎬 **4.2.3 Subnet Math**

📄 **4.2.4 Subnet Math Facts**

🎬 **4.2.5 Variable Length Subnet Masking (VLSM)**

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_ip_submath_ccna7\q_ip_submath_01_ccna7.question.xml

Question 5 ✓ Correct

You have a network address of 132.66.0.0 and a subnet mask of 255.255.224.0.

Which four of the following are valid subnet addresses?

→ ☑ 132.66.192.0

□ 132.98.0.0

□ 132.66.255.0

→ ☑ 132.66.0.0

□ 132.130.0.0

→ ☑ 132.66.96.0

→ ☑ 132.66.224.0

Explanation

To determine the valid subnet addresses, complete the following steps:

1. Convert the custom subnet mask value to binary (224 = 11100000).
2. Select the rightmost masked bit (100000).
3. Convert this bit to decimal. This is the increment value (32).
4. Add the increment value to the network address up to the subnet mask value. In this example, the possible subnet addresses are:

- 132.66.0.0
- 132.66.32.0
- 132.66.64.0
- 132.66.96.0
- 132.66.128.0
- 132.66.160.0
- 132.66.192.0
- 132.66.224.0

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_ip_submath_ccna7\q_ip_submath_02_ccna7.question.xml

Question 6.

✓ Correct

You have a network address of 201.79.187.0 and a subnet mask of 255.255.255.192.

Which three of the following are valid host addresses for subnet 201.79.187.128?

→ ☑ 201.79.187.166

□ 201.79.187.33

□ 201.79.187.12

□ 201.79.187.196

→ ☑ 201.79.187.189

→ ☑ 201.79.187.132

Explanation

You can calculate the range of host addresses by completing the following steps:

1. Convert the octet of interest in the subnet mask to binary (11000000).
2. Convert the octet of interest in the subnet address to binary (10000000).
3. In the subnet address, set all host bits to 1 (10111111). This is the broadcast address.
4. Convert the broadcast address to decimal (201.79.187.191).
5. Valid host addresses are one more than the subnet address (201.79.187.129) and one less than the broadcast address (201.79.187.190).

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

- 🎬 **4.2.3 Subnet Math**
- 📄 **4.2.4 Subnet Math Facts**
- 🎬 **4.2.5 Variable Length Subnet Masking (VLSM)**
- 📄 **4.2.6 VLSM Facts**
- 📄 **4.2.7 Subnet Operations Facts**
- 🎬 **4.3.1 Subnet Design**
- 🖥 **4.3.2 Configure Subnets**
- 📄 **4.3.3 Subnet Design Facts**
- 🎬 **4.4.1 Route Summarization Overview**
- 🎬 **4.4.2 Route Summarization Network Design**
- 📄 **4.4.3 Route Summarization Facts**
- 🖥 **4.4.4 Configure Route Summarization**
- 📄 **4.4.5 Route Summarization Command List**
- 🖥 **6.2.3 Set Up Static Routing**
- 🎬 **6.4.1 IPv4 Routing Overview**
- 🎬 **6.4.2 Routing Troubleshooting Tools**
- 🖥 **6.4.3 Use Ping and Traceroute**
- 🎬 **6.4.4 Host Configuration Issues**
- 🎬 **6.4.5 Router Configuration Issues**
- 🖥 **6.4.6 Use Show Commands on the Router**
- 📄 **6.4.7 Troubleshooting IPv4 Routing Facts**
- 📄 **6.5.5 IP Troubleshooting Utility Facts**
- 📄 **6.5.6 IP Troubleshooting Facts**

resources\text\t_ip_submath_ccna7\q_ip_submath_03_ccna7.question.xml

Question 7 ✓ Correct

While calculating how many subnets are available for a given IP address and subnet mask, when should you use the 2^n - 2 formula? (Select two.)

☐ The network uses a classless routing protocol, such as RIP version 2, EIGRP, or OSPF.

☐ Variable-length Subnet Mask (VLSM) is used.

→ ☑ The network uses a classful routing protocol, such as RIP version 1 or IGRP.

☐ The **ip subnet zero** command is configured.

→ ☑ The **no ip subnet zero** command is configured.

Explanation

Use *2^n - 2* if the network uses a classful routing protocol, such as RIP version 1 or IGRP, or if the **no ip subnet zero** command is configured.

Use *2^n* if:

- The network uses a classless routing protocol, such as RIP version 2, EIGRP, or OSPF.
- The **ip subnet zero** command is configured.
- Variable-length Subnet Mask (VLSM) is used.
- No network details are provided.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_vlsm_ccna7\q_vlsm_01_ccna7.question.xml

Question 8

✓ Correct

You have a network address of 202.200.55.0 with a subnet mask of 255.255.255.224.

Which of the following is the broadcast address for subnet 202.200.55.96?

○ 202.200.55.1

○ 202.200.55.96

○ 202.200.55.97

○ 202.200.55.111

→ ● 202.200.55.127

○ 202.200.55.255

Explanation

The broadcast address for this subnet is 202.200.55.127. The broadcast address is always the last valid IP address in the host range for the subnet. Use the following process to determine the broadcast address.

1. Convert the last octet of the subnet mask to binary (1110000).
2. Convert the last octet of the subnet address to binary (00000000).
3. In the subnet address, set all host bits to 1 (00011111).
4. Convert the address to decimal (127). This is the broadcast address.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_subnetoperations_ccna7\q_subnetoperations_01_ccna7.question.xml

Question [illegible]

✓ Correct

Your network has been assigned 168.11.0.0 as the network address. You have determined that you need 70 subnets.

Which subnet mask value should you select to provide 70 subnets?

- ○ 255.255.252.0
- ○ 255.255.248.0
- ○ 255.255.240.0
- → ● 255.255.254.0
- ○ 255.255.255.0

Explanation

Use 255.255.254.0 as the subnet mask. This masks seven bits in the network address for subnet addresses. Using the formula (*2^m*), seven masked bits provide 2^7, or up to 128 subnets.

References

- **4.1.1 Numbering Systems**
- **4.1.2 Numbering System Facts**
- **4.1.3 IP Addresses**
- **4.1.4 IP Address Format**
- **4.1.5 IP Address Classes**
- **4.1.6 IP Address Class Facts**
- **4.1.7 Public vs. Private IP Addresses**
- **4.1.8 Public and Private IP Address Facts**
- **4.2.1 Subnets**
- **4.2.2 Subnet Facts**
- **4.2.3 Subnet Math**
- **4.2.4 Subnet Math Facts**
- **4.2.5 Variable Length Subnet Masking (VLSM)**
- **4.2.6 VLSM Facts**

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_subnetoperations_ccna7\q_subnetoperations_02_ccna7.question.xml

Question 10 ✓ Correct

You need to connect a router to a subnet. The subnet uses the IP address 192.168.12.0/26. You are instructed to assign the last IP address on the subnet to the router.

Which IP address will you use?

○ 192.168.12.255

○ 192.168.12.254

○ 192.168.12.63

→ ● 192.168.12.62

○ 192.168.12.30

○ 192.168.12.31

○ 192.168.12.15

○ 192.168.12.14

Explanation

The last IP address on subnet 192.168.12.0/26 that can be assigned to a host is 192.168.12.62. You cannot use 192.168.12.63 because this is the broadcast address. With the 26-bit mask, valid host addresses are between 192.168.12.1 and 192.168.12.62.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

📄 **4.2.4 Subnet Math Facts**

🎬 **4.2.5 Variable Length Subnet Masking (VLSM)**

📄 **4.2.6 VLSM Facts**

📄 **4.2.7 Subnet Operations Facts**

🎬 **4.3.1 Subnet Design**

🖥 **4.3.2 Configure Subnets**

📄 **4.3.3 Subnet Design Facts**

🎬 **4.4.1 Route Summarization Overview**

🎬 **4.4.2 Route Summarization Network Design**

📄 **4.4.3 Route Summarization Facts**

🖥 **4.4.4 Configure Route Summarization**

📄 **4.4.5 Route Summarization Command List**

🖥 **6.2.3 Set Up Static Routing**

🎬 **6.4.1 IPv4 Routing Overview**

🎬 **6.4.2 Routing Troubleshooting Tools**

🖥 **6.4.3 Use Ping and Traceroute**

🎬 **6.4.4 Host Configuration Issues**

🎬 **6.4.5 Router Configuration Issues**

🖥 **6.4.6 Use Show Commands on the Router**

📄 **6.4.7 Troubleshooting IPv4 Routing Facts**

📄 **6.5.5 IP Troubleshooting Utility Facts**

📄 **6.5.6 IP Troubleshooting Facts**

resources\text\t_subnetoperations_ccna7\q_subnetoperations_03_ccna7.question.xml

4.3.6 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)

Date: 2/10/2025, 1:44:09 PM • **Time Spent:** 01:45

Score: 100%

Passing Score: 80%

Question 1 ✓ Correct

You are configuring a network and have been assigned the network address of 221.12.12.0. You want to subnet the network to allow 5 subnets with 20 hosts per subnet. Which subnet mask should you use?

○ 255.255.255.128

○ 255.255.255.248

○ 255.255.255.192

○ 255.255.255.240

→ ● 255.255.255.224

Explanation

Use 255.255.255.224 as the subnet mask. To find the number of subnets supported, use the formula *2^n*, where *n* is the number of additional masked bits. 224 masks 3 bits, giving you 2^3, or 8 subnets.

To find the maximum number of hosts per subnet, use the formula *2^n - 2*, where *n* is the number of unmasked bits. 224 has 5 unmasked bits, giving you 2^5 - 2, or 30 hosts per subnet.

Selecting 255.255.255.240 as the subnet mask gives you 14 possible subnets (2^4 - 2), but each subnet would only have a maximum of 14 hosts (2^4 - 2).

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

- 🎬 **4.2.3 Subnet Math**
- 📄 **4.2.4 Subnet Math Facts**
- 🎬 **4.2.5 Variable Length Subnet Masking (VLSM)**
- 📄 **4.2.6 VLSM Facts**
- 📄 **4.2.7 Subnet Operations Facts**
- 🎬 **4.3.1 Subnet Design**
- 🖥 **4.3.2 Configure Subnets**
- 📄 **4.3.3 Subnet Design Facts**
- 🎬 **4.4.1 Route Summarization Overview**
- 🎬 **4.4.2 Route Summarization Network Design**
- 📄 **4.4.3 Route Summarization Facts**
- 🖥 **4.4.4 Configure Route Summarization**
- 📄 **4.4.5 Route Summarization Command List**
- 🖥 **6.2.3 Set Up Static Routing**
- 🎬 **6.4.1 IPv4 Routing Overview**
- 🎬 **6.4.2 Routing Troubleshooting Tools**
- 🖥 **6.4.3 Use Ping and Traceroute**
- 🎬 **6.4.4 Host Configuration Issues**
- 🎬 **6.4.5 Router Configuration Issues**
- 🖥 **6.4.6 Use Show Commands on the Router**
- 📄 **6.4.7 Troubleshooting IPv4 Routing Facts**
- 📄 **6.5.5 IP Troubleshooting Utility Facts**
- 📄 **6.5.6 IP Troubleshooting Facts**

resources\text\t_ip_cfgp_ccna7\q_ip_cfgp_01_ccna7.question.xml

Question 2 ✓ Correct

You have a single router with three subnets as shown. Each subnet has the number of hosts specified.

You need to select a subnet mask for each subnet that provides sufficient host addresses without wasting addresses.

Which mask values should you use?

→ ●
- SubnetA = 255.255.255.192
- SubnetB = 255.255.255.224
- SubnetC = 255.255.255.128

○
- SubnetA = 255.255.255.64
- SubnetB = 255.255.255.32
- SubnetC = 255.255.255.64

○
- SubnetA = 255.255.255.128
- SubnetB = 255.255.255.240
- SubnetC = 255.255.255.192

○
- SubnetA = 255.255.255.224
- SubnetB = 255.255.255.240
- SubnetC = 255.255.255.192

Explanation

To support 50 hosts, use a mask of 255.255.255.192. This masks 26 bits and provides up to 62 hosts. A mask of 255.255.255.224 only provides 30 host addresses.

To support 15 hosts, use a mask of 255.255.255.224. This masks 27 bits and provides up to 30 hosts. A mask of 255.255.255.240 would provide only 14 host addresses.

To support 65 hosts, use a mask of 255.255.255.128. This masks 25 bits and provides up to 126 hosts. The mask of 255.255.255.192 provides only 62 host addresses.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_ip_cfgp_ccna7\q_ip_cfgp_02_ccna7.question.xml

Question 3 ✓ Correct

You need to design a network that supports 275 hosts. You want to place all hosts in a single broadcast domain, and you want to make sure you do not waste IP addresses.

How should you implement your plan?

○ Use a router to create two subnets. Put 250 hosts on one subnet and 25 hosts on the other subnet. Use 255.255.255.0 and 255.255.255.224 as subnet masks.

○ Use a router to create two subnets, with half of the hosts on each subnet. Use a mask of 255.255.255.0 on each subnet.

○ Connect a router to a switch with a single connection. Create two subinterfaces on the router. Use a mask of 255.255.255.0 for each subinterface.

○ Use a bridge on a single subnet. Use a mask of 255.255.255.128 for each bridge port.

→ ● Place all hosts on the same subnet. Use a mask of 255.255.254.0.

Explanation

To have all hosts on the same broadcast domain, you will need a single subnet. Use a mask of 255.255.254.0 to support up to 510 hosts. While this method wastes 235 host addresses, it is the only method described that results in a single broadcast domain.

Like physical interfaces, a subinterface marks the boundary of a subnet and therefore a broadcast domain. Both sides of a bridge are on the same subnet, but you do not assign subnet masks to the bridge. Using different network addresses on each side of the bridge would prevent hosts from communicating with each other. Using a mask of 255.255.255.0 would not provide enough addresses, resulting in some hosts sharing an address.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

- **4.1.7 Public vs. Private IP Addresses**
- **4.1.8 Public and Private IP Address Facts**
- **4.2.1 Subnets**
- **4.2.2 Subnet Facts**
- **4.2.3 Subnet Math**
- **4.2.4 Subnet Math Facts**
- **4.2.5 Variable Length Subnet Masking (VLSM)**
- **4.2.6 VLSM Facts**
- **4.2.7 Subnet Operations Facts**
- **4.3.1 Subnet Design**
- **4.3.2 Configure Subnets**
- **4.3.3 Subnet Design Facts**
- **4.4.1 Route Summarization Overview**
- **4.4.2 Route Summarization Network Design**
- **4.4.3 Route Summarization Facts**
- **4.4.4 Configure Route Summarization**
- **4.4.5 Route Summarization Command List**
- **6.2.3 Set Up Static Routing**
- **6.4.1 IPv4 Routing Overview**
- **6.4.2 Routing Troubleshooting Tools**
- **6.4.3 Use Ping and Traceroute**
- **6.4.4 Host Configuration Issues**
- **6.4.5 Router Configuration Issues**
- **6.4.6 Use Show Commands on the Router**
- **6.4.7 Troubleshooting IPv4 Routing Facts**
- **6.5.5 IP Troubleshooting Utility Facts**
- **6.5.6 IP Troubleshooting Facts**

resources\text\t_ip_cfgp_ccna7\q_ip_cfgp_03_ccna7.question.xml

Question 4 ✓ Correct

You have a network with two routers as shown. You need to choose subnet addresses for subnets 1 and 2.

Which of the following subnets would you use? (Select two.)

→ ☑ 172.30.12.0/28

□ 172.30.12.8/28

→ ☑ 172.30.12.128/26

□ 172.30.12.64/26

□ 172.30.12.64/27

□ 172.30.12.8/27

Explanation

For subnet 1, you will need a 28-bit mask to provide up to 14 host addresses. Using a 27-bit mask would waste IP addresses. For subnet 2, you will need a 26-bit mask to give you up to 62 host addresses (a 27-bit mask provides only 30 host addresses).

For subnet 1, use 172.30.12.0 as the subnet address. 172.30.12.8 is not a valid subnet address for a 28-bit mask (valid subnets must be in increments of 16: 0, 16, 32, etc.). For subnet 2, use 172.30.12.128.

172.30.12.64 is a valid subnet address, but the range of IP addresses (172.30.12.65 to 172.30.12.126) overlaps with the 172.30.12.96/27 subnet.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

🎬 **4.2.1 Subnets**

📄 **4.2.2 Subnet Facts**

🎬 **4.2.3 Subnet Math**

📄 **4.2.4 Subnet Math Facts**

🎬 **4.2.5 Variable Length Subnet Masking (VLSM)**

📄 **4.2.6 VLSM Facts**

📄 **4.2.7 Subnet Operations Facts**

🎬 **4.3.1 Subnet Design**

🖥 **4.3.2 Configure Subnets**

📄 **4.3.3 Subnet Design Facts**

🎬 **4.4.1 Route Summarization Overview**

🎬 **4.4.2 Route Summarization Network Design**

📄 **4.4.3 Route Summarization Facts**

🖥 **4.4.4 Configure Route Summarization**

📄 **4.4.5 Route Summarization Command List**

🖥 **6.2.3 Set Up Static Routing**

🎬 **6.4.1 IPv4 Routing Overview**

🎬 **6.4.2 Routing Troubleshooting Tools**

🖥 **6.4.3 Use Ping and Traceroute**

🎬 **6.4.4 Host Configuration Issues**

🎬 **6.4.5 Router Configuration Issues**

🖥 **6.4.6 Use Show Commands on the Router**

📄 **6.4.7 Troubleshooting IPv4 Routing Facts**

📄 **6.5.5 IP Troubleshooting Utility Facts**

📄 **6.5.6 IP Troubleshooting Facts**

resources\text\t_ip_cfgp_ccna7\q_ip_cfgp_04_ccna7.question.xml

Question 5 ✓ Correct

You have a small network with three subnets as shown. IP addresses for each router interface are also indicated.

You need to connect Wrk1_A to SubnetA and Wrk5_C to SubnetC. Which IP addresses should you use? (Select two.)

□ Wrk1_A = 192.168.111.32

→ ☑ Wrk1_A = 192.168.111.62

□ Wrk1_A = 192.168.111.65

→ ☑ Wrk5_C = 10.155.64.97

□ Wrk5_C = 10.155.64.111

□ Wrk5_C = 10.155.64.114

Explanation

For Wrk1_A, use 192.168.111.62; for Wrk5_C, use 10.155.64.97.

- SubnetA uses a 27-bit mask. The subnet used by the router has a subnet address of 192.168.111.32 with a broadcast address of 192.168.111.63.
- SubnetC uses a 28-bit mask. The subnet used by the router has a subnet address of 10.155.64.96 with a broadcast address of 10.155.64.111.

Hosts on the same subnet must have IP addresses within the subnet range. Neither the subnet address nor the broadcast address can be assigned to hosts.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

- **4.2.1 Subnets**
- **4.2.2 Subnet Facts**
- **4.2.3 Subnet Math**
- **4.2.4 Subnet Math Facts**
- **4.2.5 Variable Length Subnet Masking (VLSM)**
- **4.2.6 VLSM Facts**
- **4.2.7 Subnet Operations Facts**
- **4.3.1 Subnet Design**
- **4.3.2 Configure Subnets**
- **4.3.3 Subnet Design Facts**
- **4.4.1 Route Summarization Overview**
- **4.4.2 Route Summarization Network Design**
- **4.4.3 Route Summarization Facts**
- **4.4.4 Configure Route Summarization**
- **4.4.5 Route Summarization Command List**
- **6.2.3 Set Up Static Routing**
- **6.4.1 IPv4 Routing Overview**
- **6.4.2 Routing Troubleshooting Tools**
- **6.4.3 Use Ping and Traceroute**
- **6.4.4 Host Configuration Issues**
- **6.4.5 Router Configuration Issues**
- **6.4.6 Use Show Commands on the Router**
- **6.4.7 Troubleshooting IPv4 Routing Facts**
- **6.5.5 IP Troubleshooting Utility Facts**
- **6.5.6 IP Troubleshooting Facts**

resources\text\t_ip_cfgp_ccna7\q_ip_cfgp_05_ccna7.question.xml

Question 6. ✓ Correct

Your client has a class B network address and needs to support 500 hosts on as many subnets as possible.

Which subnet mask should you recommend?

○ 255.255.255.0

→ ● 255.255.254.0

○ 255.255.255.128

○ 255.255.255.224

Explanation

When applied to a class B network IP address, the subnet mask 255.255.254.0 can support 510 hosts on 126 subnets. To calculate this subnet mask, use the formula *2^n - 2* to find the number of available host addresses (where *n* is the number of unmasked bits or bits with a 0 value). So *2^n - 2* must equal at least 500 hosts.

- 2^8 - 2 = 254 hosts
- 2^9 - 2 = 510 hosts
- 2^10 - 2 = 1024 hosts

The best choice is 2^9 - 2, which gives 510 hosts and leaves 7 bits remaining in the second octet of the mask to address subnets. The number of subnet addresses that will be available are 126 subnets (2^7 - 2).

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

- 📄 **4.2.2 Subnet Facts**
- 🎬 **4.2.3 Subnet Math**
- 📄 **4.2.4 Subnet Math Facts**
- 🎬 **4.2.5 Variable Length Subnet Masking (VLSM)**
- 📄 **4.2.6 VLSM Facts**
- 📄 **4.2.7 Subnet Operations Facts**
- 🎬 **4.3.1 Subnet Design**
- 🖥 **4.3.2 Configure Subnets**
- 📄 **4.3.3 Subnet Design Facts**
- 🎬 **4.4.1 Route Summarization Overview**
- 🎬 **4.4.2 Route Summarization Network Design**
- 📄 **4.4.3 Route Summarization Facts**
- 🖥 **4.4.4 Configure Route Summarization**
- 📄 **4.4.5 Route Summarization Command List**
- 🖥 **6.2.3 Set Up Static Routing**
- 🎬 **6.4.1 IPv4 Routing Overview**
- 🎬 **6.4.2 Routing Troubleshooting Tools**
- 🖥 **6.4.3 Use Ping and Traceroute**
- 🎬 **6.4.4 Host Configuration Issues**
- 🎬 **6.4.5 Router Configuration Issues**
- 🖥 **6.4.6 Use Show Commands on the Router**
- 📄 **6.4.7 Troubleshooting IPv4 Routing Facts**
- 📄 **6.5.5 IP Troubleshooting Utility Facts**
- 📄 **6.5.6 IP Troubleshooting Facts**

resources\text\t_ip_cfgp_ccna7\q_ip_cfgp_06_ccna7.question.xml

Question 7 ✓ Correct

You have a network address of 133.233.11.0 and a subnet mask of 255.255.255.240.

How many assignable host addresses are on each subnet?

○ 0

○ 2

○ 6

→ ● 14

○ 30

○ 62

Explanation

You can calculate the number of possible host addresses by completing the following steps:

1. Convert the subnet mask to binary (240 = 11110000).
2. Count the total number of unmasked bits in the subnet mask (4).
3. Use the formula *2^n - 2* where *n* is the number of unmasked bits. In this example, there are 2^4 - 2, or 14, host addresses for each subnet.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

- **4.2.5 Variable Length Subnet Masking (VLSM)**
- **4.2.6 VLSM Facts**
- **4.2.7 Subnet Operations Facts**
- **4.3.1 Subnet Design**
- **4.3.2 Configure Subnets**
- **4.3.3 Subnet Design Facts**
- **4.4.1 Route Summarization Overview**
- **4.4.2 Route Summarization Network Design**
- **4.4.3 Route Summarization Facts**
- **4.4.4 Configure Route Summarization**
- **4.4.5 Route Summarization Command List**
- **6.2.3 Set Up Static Routing**
- **6.4.1 IPv4 Routing Overview**
- **6.4.2 Routing Troubleshooting Tools**
- **6.4.3 Use Ping and Traceroute**
- **6.4.4 Host Configuration Issues**
- **6.4.5 Router Configuration Issues**
- **6.4.6 Use Show Commands on the Router**
- **6.4.7 Troubleshooting IPv4 Routing Facts**
- **6.5.5 IP Troubleshooting Utility Facts**
- **6.5.6 IP Troubleshooting Facts**

resources\text\t_ip_cfgp_ccna7\q_ip_cfgp_07_ccna7.question.xml

[redacted] ✓ Correct

You have been assigned the IP address of 197.177.25.0 for your network. You have determined that you need five subnets to allow future growth. What subnet mask value would you use?

255.255.255.224 ✓

Explanation

Use 255.255.255.224 as the subnet mask value. You will need to borrow 3 bits for the custom subnet mask.

To calculate the subnet mask value, complete the following steps:

1. Convert the default subnet mask to binary.
2. Borrow bits from the mask. Use the formula *2^m* to identify the number of subnets and *2^n - 2* to identify the number of hosts per subnet for each selected mask.
3. Continue borrowing bits until you get enough subnets and hosts.

Verify your answer as follows:

There are 3 additional masked bits. Using the formula 2^3, you get 8 subnets. Borrowing only 2 bits gives you only 4 subnets. Borrowing 4 bits gives you too many subnets.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_ip_cfgp_ccna7\q_ip_cfgp_08_ccna7.question.xml

Question 9 ✓ Correct

You have a network address of 132.66.0.0 and a subnet mask of 255.255.254.0.

How many possible host addresses are on each subnet, excluding host addresses of all 1s and all 0s?

○ 62

○ 0

→ ● 510

○ 1022

Explanation

You can calculate the number of possible host addresses by completing the following steps:

1. Convert the subnet mask to binary (254 = 11111110).
2. Count the total number of unmasked bits in the subnet mask, including the empty octet to get a total of 9. For example, 1111111**0.00000000**.
3. Use the formula *2^n - 2*, where *n* is the number of unmasked bits. In this example, there are 2^9 - 2, or 510, host addresses for each subnet.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

📄 **4.2.6 VLSM Facts**

📄 **4.2.7 Subnet Operations Facts**

🎬 **4.3.1 Subnet Design**

🖥 **4.3.2 Configure Subnets**

📄 **4.3.3 Subnet Design Facts**

🎬 **4.4.1 Route Summarization Overview**

🎬 **4.4.2 Route Summarization Network Design**

📄 **4.4.3 Route Summarization Facts**

🖥 **4.4.4 Configure Route Summarization**

📄 **4.4.5 Route Summarization Command List**

🖥 **6.2.3 Set Up Static Routing**

🎬 **6.4.1 IPv4 Routing Overview**

🎬 **6.4.2 Routing Troubleshooting Tools**

🖥 **6.4.3 Use Ping and Traceroute**

🎬 **6.4.4 Host Configuration Issues**

🎬 **6.4.5 Router Configuration Issues**

🖥 **6.4.6 Use Show Commands on the Router**

📄 **6.4.7 Troubleshooting IPv4 Routing Facts**

📄 **6.5.5 IP Troubleshooting Utility Facts**

📄 **6.5.6 IP Troubleshooting Facts**

resources\text\t_ip_cfgp_ccna7\q_ip_cfgp_09_ccna7.question.xml

✓ Correct

You have a network address of 220.16.22.0 and have selected 255.255.255.224 as the subnet mask value. How many possible subnets are there?

8 ✓

Explanation

There are eight possible subnets. You can identify the number of possible subnets by completing the following steps:

1. Convert the mask to binary (224=11100000).
2. Count the number of extra bits in the mask.
3. Use the formula *2^m* to find the number of subnets.

There are 3 extra masked bits. 2^3 gives you 8 subnets.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

📄 **4.3.3 Subnet Design Facts**

🎬 **4.4.1 Route Summarization Overview**

🎬 **4.4.2 Route Summarization Network Design**

📄 **4.4.3 Route Summarization Facts**

🖥 **4.4.4 Configure Route Summarization**

📄 **4.4.5 Route Summarization Command List**

🖥 **6.2.3 Set Up Static Routing**

🎬 **6.4.1 IPv4 Routing Overview**

🎬 **6.4.2 Routing Troubleshooting Tools**

🖥 **6.4.3 Use Ping and Traceroute**

🎬 **6.4.4 Host Configuration Issues**

🎬 **6.4.5 Router Configuration Issues**

🖥 **6.4.6 Use Show Commands on the Router**

📄 **6.4.7 Troubleshooting IPv4 Routing Facts**

📄 **6.5.5 IP Troubleshooting Utility Facts**

📄 **6.5.6 IP Troubleshooting Facts**

resources\text\t_ip_cfgp_ccna7\q_ip_cfgp_10_ccna7.question.xml

4.4.6 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 2/10/2025, 1:56:02 PM • **Time Spent:** 01:29

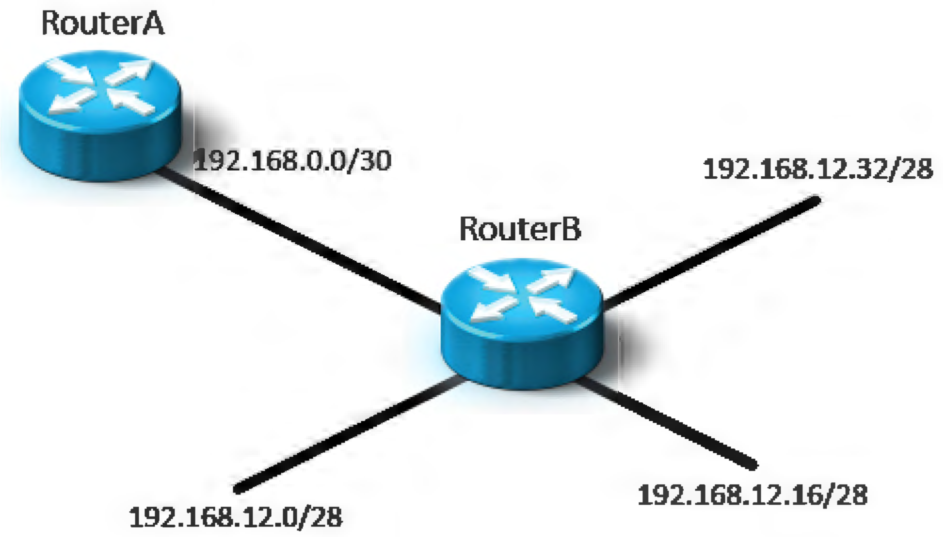
Score: 100%

Passing Score: 80%

✓ Correct

You have a network with two routers as shown. RouterA and RouterB are configured to use RIP version 2 with auto-summarization enabled.

Which summarized network entry will RouterA have in its routing table for the subnets connected to RouterB?



→ ● 192.168.12.0/24

○ 192.168.12.32/29

○ 192.168.12.48/28

○ 192.168.12.32/27

○ 192.168.0.0/16

Explanation

Subnets on RouterB will be summarized as 192.168.12.0/24. Auto-summarization with RIP v2 or EIGRP summarizes routes along classful network boundaries (meaning the default subnet mask is used).

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

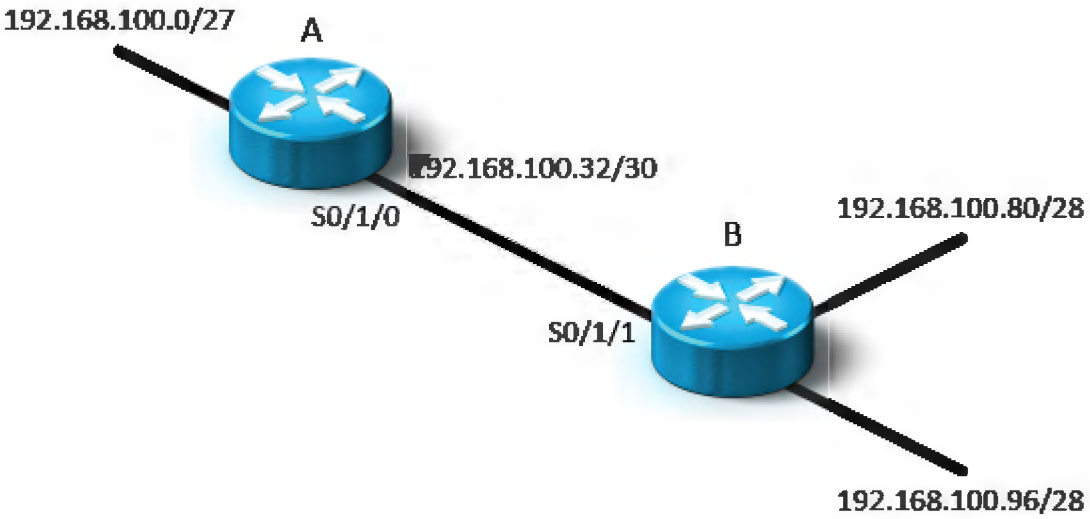
- 📄 **4.1.6 IP Address Class Facts**
- 🎬 **4.1.7 Public vs. Private IP Addresses**
- 📄 **4.1.8 Public and Private IP Address Facts**
- 🎬 **4.2.1 Subnets**
- 📄 **4.2.2 Subnet Facts**
- 🎬 **4.2.3 Subnet Math**
- 📄 **4.2.4 Subnet Math Facts**
- 🎬 **4.2.5 Variable Length Subnet Masking (VLSM)**
- 📄 **4.2.6 VLSM Facts**
- 📄 **4.2.7 Subnet Operations Facts**
- 🎬 **4.3.1 Subnet Design**
- 🖥 **4.3.2 Configure Subnets**
- 📄 **4.3.3 Subnet Design Facts**
- 🎬 **4.4.1 Route Summarization Overview**
- 🎬 **4.4.2 Route Summarization Network Design**
- 📄 **4.4.3 Route Summarization Facts**
- 🖥 **4.4.4 Configure Route Summarization**
- 📄 **4.4.5 Route Summarization Command List**
- 🖥 **6.2.3 Set Up Static Routing**
- 🎬 **6.4.1 IPv4 Routing Overview**
- 🎬 **6.4.2 Routing Troubleshooting Tools**
- 🖥 **6.4.3 Use Ping and Traceroute**
- 🎬 **6.4.4 Host Configuration Issues**
- 🎬 **6.4.5 Router Configuration Issues**
- 🖥 **6.4.6 Use Show Commands on the Router**
- 📄 **6.4.7 Troubleshooting IPv4 Routing Facts**
- 📄 **6.5.5 IP Troubleshooting Utility Facts**
- 📄 **6.5.6 IP Troubleshooting Facts**

resources\text\t_rtg_summ_ccna7\q_rtg_summ_01_ccna7.question.xml

✓ Correct

You have a network with two routers as shown. You would like to configure a single static route on RouterA that summarizes the routes accessible through RouterB.

Which static route would you configure?



○ ip route 192.168.100.80 255.255.255.192 192.168.100.34

○ ip route 192.168.100.80 255.255.255.240 192.168.100.34

○ ip route 192.168.100.80 255.255.255.224 192.168.100.34

→ ● ip route 192.168.100.64 255.255.255.192 192.168.100.34

○ ip route 192.168.100.64 255.255.255.224 192.168.100.34

Explanation

The summarized route will use the subnet address of 192.168.100.64 with a mask of 255.255.255.192. When you summarize routes, you use a smaller subnet mask. This means the mask must be 27 bits or smaller. Converting the last octet of each subnet that must be summarized gives you:

80 = 01010000 96 = 01100000
This means that the subnet address is 01000000 (64), and the mask value is 11000000 (192).

You cannot use a subnet address of 192.168.100.80 because this is not a valid subnet address for a 26-bit mask. Valid addresses are multiples of 64 (0, 64, 128, 192). You cannot use a mask value of 255.255.255.224 with network 192.168.100.80 because this is not a valid subnet for that mask.

A better design in this scenario would be to use subnet addresses of 192.168.100.96/28 and 192.168.100.112/28. This would allow you to summarize both routes as 192.168.100.96/27.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

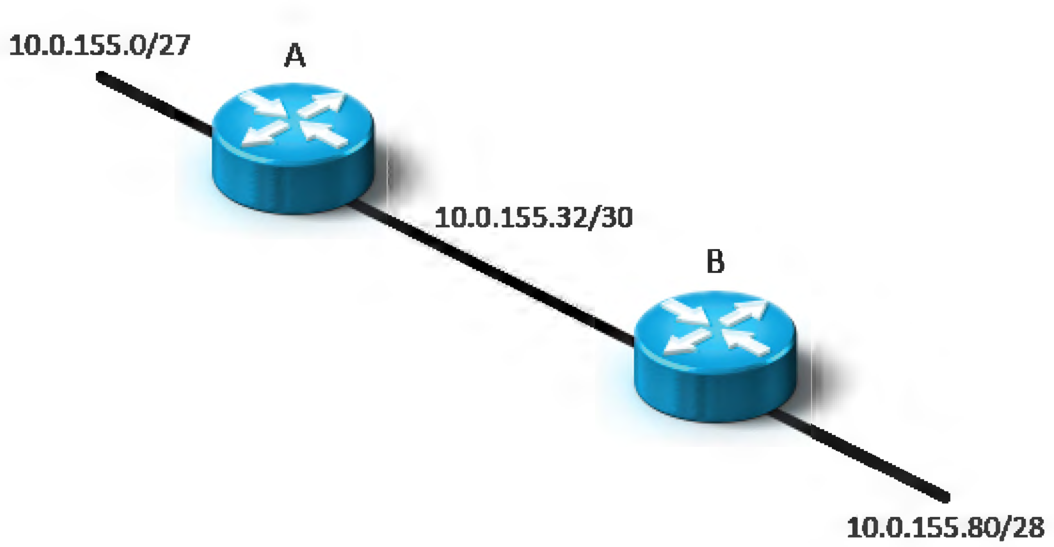
resources\text\t_rtg_summ_ccna7\q_rtg_summ_02_ccna7.question.xml

✓ Correct

You have a network with two routers as shown. Router A currently has a single static route to network 10.0.155.80/28.

You need to add another subnet to router B. This subnet should also use a 28-bit mask. You would like to replace the existing static route to network 10.0.155.80/28 with a single summarized static route that includes the old network and the new network. You want to minimize wasted addresses.

What should you do? (Select two.)



→ ☑ Configure the static route to use a network of 10.0.155.64 and a mask of 255.255.255.224.

□ Configure the static route to use a network of 10.0.155.80 and a mask of 255.255.255.224.

□ Configure the static route to use a network of 10.0.155.80 and a mask of 255.255.255.192.

→ ☑ Use 10.0.155.64/28 for the new subnet.

□ Use 10.0.155.96/28 for the new subnet.

□ Configure the static route to use a network of 10.0.155.64 and a mask of 255.255.255.192.

Explanation

For efficient summarization, use 10.0.155.64/28 for the new subnet and configure the static route with a network of 10.0.155.64 and a mask of 255.255.255.224. With the 27-bit mask, the IP address range for the summarized network includes 10.0.155.64 to 10.0.155.96. This includes hosts on both subnets.

Using a mask of 255.255.255.192 would include IP addresses from 10.0.155.64 to 10.0.155.127. IP addresses between 96-127 are currently not on any defined subnets, meaning that this route definition would block out addresses that would be wasted. Using a network of 10.0.155.80 for the summarized route is impossible when using a 27-bit or 26-bit mask, as that address is not a valid subnet address for the mask value.

References

- **4.1.1 Numbering Systems**
- **4.1.2 Numbering System Facts**
- **4.1.3 IP Addresses**
- **4.1.4 IP Address Format**
- **4.1.5 IP Address Classes**
- **4.1.6 IP Address Class Facts**
- **4.1.7 Public vs. Private IP Addresses**
- **4.1.8 Public and Private IP Address Facts**
- **4.2.1 Subnets**
- **4.2.2 Subnet Facts**
- **4.2.3 Subnet Math**
- **4.2.4 Subnet Math Facts**
- **4.2.5 Variable Length Subnet Masking (VLSM)**
- **4.2.6 VLSM Facts**
- **4.2.7 Subnet Operations Facts**
- **4.3.1 Subnet Design**
- **4.3.2 Configure Subnets**
- **4.3.3 Subnet Design Facts**
- **4.4.1 Route Summarization Overview**
- **4.4.2 Route Summarization Network Design**
- **4.4.3 Route Summarization Facts**

- 🖥 **4.4.4 Configure Route Summarization**
- 📄 **4.4.5 Route Summarization Command List**
- 🖥 **6.2.3 Set Up Static Routing**
- 🎬 **6.4.1 IPv4 Routing Overview**
- 🎬 **6.4.2 Routing Troubleshooting Tools**
- 🖥 **6.4.3 Use Ping and Traceroute**
- 🎬 **6.4.4 Host Configuration Issues**
- 🎬 **6.4.5 Router Configuration Issues**
- 🖥 **6.4.6 Use Show Commands on the Router**
- 📄 **6.4.7 Troubleshooting IPv4 Routing Facts**
- 📄 **6.5.5 IP Troubleshooting Utility Facts**
- 📄 **6.5.6 IP Troubleshooting Facts**

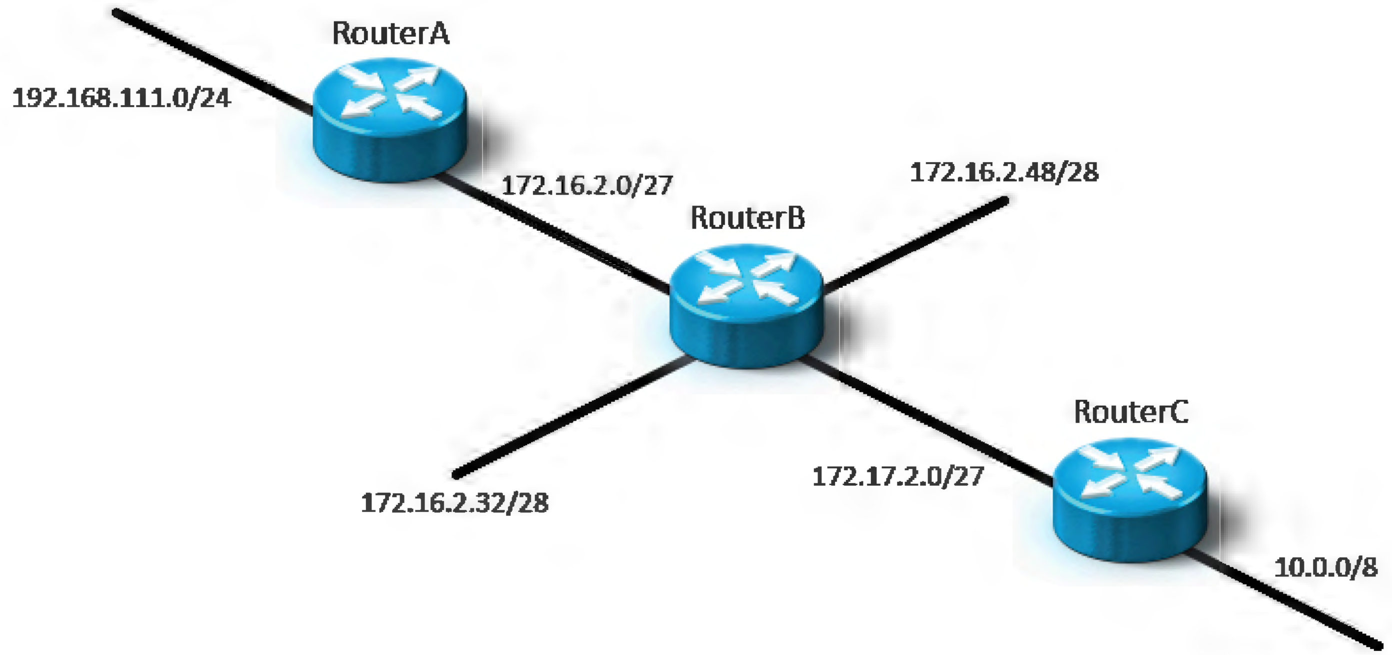
resources\text\t_rtg_summ_ccna7\q_rtg_summ_03_ccna7.question.xml

✓ Correct

You have a network with three routers as shown.

All routers are configured to share information for all known routes using the same routing protocol. Automatic summarization is enabled.

Router B shares its known networks with router A. Which of the following routes will be in router A's routing table?



○ 172.16.2.0/24

○ 172.16.2.0/27 and 172.16.2.32/27

→ ● 172.16.2.0/27, 172.16.2.32/28, and 172.16.2.48/28

○ 172.16.0.0/16

Explanation

Router A will have routes to networks 172.16.2.0/27, 172.16.2.32/28, and 172.16.2.48/28. Auto-summarization only takes place on classful network boundaries, and only when the router is sharing information with a router in a different classful network. Because router B is in the same classful network as router A, it cannot summarize its networks when reporting them to router A.

If you had turned the routing protocol off, you could summarize the two networks on router B as a single network of 172.16.2.32/27. If the link between router A and router B was not on the 172.16.0.0/16 classful network, then router B would have summarized its networks as 172.16.0.0/16 when advertising them to router A.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_rtg_summ_ccna7\q_rtg_summ_04_ccna7.question.xml

Question 5 ✓ Correct

Which of the following allow you to disable automatic summarization? (Select two.)

☐ OSPF v2

☐ RIP

→ ☑ EIGRP

☐ OSPF

→ ☑ RIP2

Explanation

With automatic summarization, the router identifies adjacent networks and calculates the summarized route.

- Auto-summarization is supported on classless and classful routing protocols.
- Auto-summarization uses the default class boundary to summarize routes.
- RIP (version 1 and version 2) and EIGRP support auto-summarization; OSPF does not.
- For RIPv2 and EIGRP, you can disable automatic summarization.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_rtg_summ_ccna7\q_rtg_summ_05_ccna7.question.xml

Question 6. ✓ Correct

A network administrator is working with a range of subnets from 172.16.16.0/24 through 172.16.31.0/24. They need to identify a summarized route for this group of subnets.

What should be the subnet address and mask of the summarized route?

○ Subnet Address: 172.16.0.0, Mask: 255.255.0.0

○ Subnet Address: 172.16.31.0, Mask: 255.255.255.0

○ Subnet Address: 172.16.16.0, Mask: 255.255.255.0

→ ● Subnet Address: 172.16.16.0, Mask: 255.255.240.0

Explanation

Subnet Address: 172.16.16.0, Mask: 255.255.240.0 is the correct answer. The subnet address of the summarized route is 172.16.16.0 and the mask is 255.255.240.0 (/20). This is determined by converting the last significant octet of the first and the last subnet in the contiguous range to binary, identifying the last consecutive binary bit that is shared, and converting all bits to the right of the shared bit to 0 for the subnet address and all bits to the left of the shared bit to 1 for the mask.

Subnet Address: 172.16.16.0, Mask: 255.255.255.0 is incorrect because the mask 255.255.255.0 (/24) would only cover a single subnet, not a range of subnets from 172.16.16.0 through 172.16.31.0.

Subnet Address: 172.16.0.0, Mask: 255.255.0.0 is incorrect because the mask 255.255.0.0 (/16) would cover all subnets in the 172.16.0.0 network, not just the range from 172.16.16.0 through 172.16.31.0.

Subnet Address: 172.16.31.0, Mask: 255.255.255.0 is incorrect because the mask 255.255.255.0 (/24) would only cover a single subnet, not a range of subnets from 172.16.16.0 through 172.16.31.0. Also, the subnet address should be the first subnet in the range, not the last.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_rtg_summ_ccna7\q_rtg_summ_06_ccna7.question.xml

Question 7 ✓ Correct

On your network, you have subnetting the network address 10.0.0.0 into smaller subnets, and it is separated by a network with different classful network addresses, such as 12.0.0.0. Which route summarization command do you need to execute?

○ Router(config-router)#**auto-summary**

○ Router(config-if)#**ip summary-address rip 12.0.0 255.0.0.0**

○ Router(config-if)#**show ip ospf summary-address**

→ ● Router(config-router)#**no auto-summary**

Explanation

no auto-summary disable automatic summarization if you have a network address (such as 10.0.0.0) subnetted into smaller subnets and separated by a network with a different classful network address (such as 12.0.0.0).

ip summary-address rip 12.0.0 255.0.0.0 configures a summary address on a specified interface.

auto-summary enables automatic route summarization. By default, subnets are summarized based on classful boundaries when advertising routes on networks with a different class boundary.

show ip ospf summary-address is a command unrelated to automatic summarization. This command shows a summary of all address redistribution information configured in an OSPF instance.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

- 🎬 **4.2.1 Subnets**
- 📄 **4.2.2 Subnet Facts**
- 🎬 **4.2.3 Subnet Math**
- 📄 **4.2.4 Subnet Math Facts**
- 🎬 **4.2.5 Variable Length Subnet Masking (VLSM)**
- 📄 **4.2.6 VLSM Facts**
- 📄 **4.2.7 Subnet Operations Facts**
- 🎬 **4.3.1 Subnet Design**
- 🖥 **4.3.2 Configure Subnets**
- 📄 **4.3.3 Subnet Design Facts**
- 🎬 **4.4.1 Route Summarization Overview**
- 🎬 **4.4.2 Route Summarization Network Design**
- 📄 **4.4.3 Route Summarization Facts**
- 🖥 **4.4.4 Configure Route Summarization**
- 📄 **4.4.5 Route Summarization Command List**
- 🖥 **6.2.3 Set Up Static Routing**
- 🎬 **6.4.1 IPv4 Routing Overview**
- 🎬 **6.4.2 Routing Troubleshooting Tools**
- 🖥 **6.4.3 Use Ping and Traceroute**
- 🎬 **6.4.4 Host Configuration Issues**
- 🎬 **6.4.5 Router Configuration Issues**
- 🖥 **6.4.6 Use Show Commands on the Router**
- 📄 **6.4.7 Troubleshooting IPv4 Routing Facts**
- 📄 **6.5.5 IP Troubleshooting Utility Facts**
- 📄 **6.5.6 IP Troubleshooting Facts**

resources\text\t_rt_sumcmd_ccna7\q_rt_sumcmd_01_ccna7.question.xml

Question 8 ✓ Correct

The following commands have been executed on a router:

```
Router(config-router)#no auto-summary
Router(config-router)#exit
Router(config)#int fa 0/1
Router(config-if)#ip summary-address rip 172.16.0.0 255.255.0.0
```

Which interface type is fa 0/1?

→ ● Outbound

○ Inbound null

○ Inbound

○ Outbound null

Explanation

ip summary-address rip 172.16.0.0 255.255.0.0 configures a summary address on a specified interface.

- Use this command on outbound interfaces of the appropriate routers.
- The neighboring device will have only a summary route in its routing table.
- If the neighboring devices receive a query packet for a network that matches the summary route, they send a network a.b.c.d/m unreachable message in response and do not extend the query packets any further.
- This command adds a summary route to the routing table with the route's next-hop interface set to null0.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

- 🎬 **4.2.1 Subnets**
- 📄 **4.2.2 Subnet Facts**
- 🎬 **4.2.3 Subnet Math**
- 📄 **4.2.4 Subnet Math Facts**
- 🎬 **4.2.5 Variable Length Subnet Masking (VLSM)**
- 📄 **4.2.6 VLSM Facts**
- 📄 **4.2.7 Subnet Operations Facts**
- 🎬 **4.3.1 Subnet Design**
- 🖥 **4.3.2 Configure Subnets**
- 📄 **4.3.3 Subnet Design Facts**
- 🎬 **4.4.1 Route Summarization Overview**
- 🎬 **4.4.2 Route Summarization Network Design**
- 📄 **4.4.3 Route Summarization Facts**
- 🖥 **4.4.4 Configure Route Summarization**
- 📄 **4.4.5 Route Summarization Command List**
- 🖥 **6.2.3 Set Up Static Routing**
- 🎬 **6.4.1 IPv4 Routing Overview**
- 🎬 **6.4.2 Routing Troubleshooting Tools**
- 🖥 **6.4.3 Use Ping and Traceroute**
- 🎬 **6.4.4 Host Configuration Issues**
- 🎬 **6.4.5 Router Configuration Issues**
- 🖥 **6.4.6 Use Show Commands on the Router**
- 📄 **6.4.7 Troubleshooting IPv4 Routing Facts**
- 📄 **6.5.5 IP Troubleshooting Utility Facts**
- 📄 **6.5.6 IP Troubleshooting Facts**

resources\text\t_rt_sumcmd_ccna7\q_rt_sumcmd_02_ccna7.question.xml

Question 9: ✓ Correct

When using the **ip summary-address** command, which of the following is true?

○ The interface being configured should be an inbound interface.

○ The routing table contains the next-hop interface set to the IP address of the next router.

○ The summary route will be added to all inbound interfaces on the router.

→ ● Neighboring devices only have a summary route in their routing tables.

Explanation

Neighboring devices only have a summary route in their routing tables. The command should be used on outgoing interfaces. The command adds a summary route to the routing table with the route's next-hop interface set to null0.

References

- **4.1.1 Numbering Systems**
- **4.1.2 Numbering System Facts**
- **4.1.3 IP Addresses**
- **4.1.4 IP Address Format**
- **4.1.5 IP Address Classes**
- **4.1.6 IP Address Class Facts**
- **4.1.7 Public vs. Private IP Addresses**
- **4.1.8 Public and Private IP Address Facts**
- **4.2.1 Subnets**
- **4.2.2 Subnet Facts**
- **4.2.3 Subnet Math**
- **4.2.4 Subnet Math Facts**
- **4.2.5 Variable Length Subnet Masking (VLSM)**
- **4.2.6 VLSM Facts**
- **4.2.7 Subnet Operations Facts**
- **4.3.1 Subnet Design**

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_rt_sumcmd_ccna7\q_rt_sumcmd_03_ccna7.question.xml

Question 10 ✓ Correct

Which of the following describes route summarization?

→ ● Combines a contiguous set of addresses into a single address.

○ Provides a summary of all routes on the entire network.

○ Aggregates multiple routers to appear as the same router.

○ Increases the size of the routing table, but reduces network traffic when using OSPF in automatic mode.

Explanation

Route summarization combines a contiguous set of addresses into a single address to reduce network traffic. Route summarization is also referred to as route aggregation.

OSPF does not support automatic route summarization.

References

4.1.1 Numbering Systems

4.1.2 Numbering System Facts

4.1.3 IP Addresses

4.1.4 IP Address Format

4.1.5 IP Address Classes

4.1.6 IP Address Class Facts

4.1.7 Public vs. Private IP Addresses

4.1.8 Public and Private IP Address Facts

4.2.1 Subnets

4.2.2 Subnet Facts

4.2.3 Subnet Math

4.2.4 Subnet Math Facts

4.2.5 Variable Length Subnet Masking (VLSM)

4.2.6 VLSM Facts

4.2.7 Subnet Operations Facts

4.3.1 Subnet Design

4.3.2 Configure Subnets

4.3.3 Subnet Design Facts

4.4.1 Route Summarization Overview

4.4.2 Route Summarization Network Design

4.4.3 Route Summarization Facts

4.4.4 Configure Route Summarization

4.4.5 Route Summarization Command List

6.2.3 Set Up Static Routing

6.4.1 IPv4 Routing Overview

6.4.2 Routing Troubleshooting Tools

6.4.3 Use Ping and Traceroute

6.4.4 Host Configuration Issues

6.4.5 Router Configuration Issues

6.4.6 Use Show Commands on the Router

6.4.7 Troubleshooting IPv4 Routing Facts

6.5.5 IP Troubleshooting Utility Facts

6.5.6 IP Troubleshooting Facts

resources\text\t_rt_sumcmd_ccna7\q_rt_sumcmd_04_ccna7.question.xml

4.5.11 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 2/11/2025, 11:42:08 AM • **Time Spent:** 04:07

Score: 90%

Passing Score: 80%

Question 1.

× **Incorrect**

Consider the following IPv6 address:

FD01:0001:0001:005::7/64

Drag the component parts of this address on the left to the corresponding descriptions on the right. Not all descriptions on the right have corresponding components on the left.

Global Routing Prefix

✓ FD01:0001:0001:005

Subnet ID

✓ :005

Interface ID

✓ ::7

Prefix Length

✓ /64

Global ID

Unique Local Unicast Prefix

✓ FD

Explanation

The IPv6 address FD01:0001:0001:005::7/64 is a unique local unicast address. As such, it is composed of the following component parts:

- Unique Local Unicast Prefix: FD
- Global Routing Prefix: FD01:0001:0001:005
- Subnet ID: 005
- Interface ID: ::7
- Prefix Length: /64

References

4.5.1 IPv6 Overview

4.5.2 IPv6 Benefits Facts

4.5.4 IPv6 Address Facts

4.5.5 IPv6 Address Type Facts

4.5.6 EUI-64 and Auto-Configuration

4.5.7 EUI-64 Addressing Facts

4.5.8 Configure IPv6

4.5.9 IPv6 Implementation Strategy Facts

4.5.10 IPv6 Configuration Facts

8.1.1 IPv6 Routing

8.1.2 IPv6 Routing Facts

8.1.3 Explore IPv6 Addressing on Routers

8.1.4 Common IPv6 Troubleshooting Issues

8.1.5 IPv6 Routing Facts

8.2.2 Configure OSPFv3 Routing

8.2.4 OSPFv3 Routing Facts

resources\text\t_ipv6_addg_ccna7\q_ipv6_addg_01_ccna7.question.xml

Question 2

✓ Correct

Consider the following IPv6 address:

FE80:0000:0000:0055:0000:0000:000A:AB00

Which of the following are valid shortened forms of this address? (Select two.)

☐ FE80::55::A:AB00

→ ☑ FE80::55:0000:0000:A:AB00

☐ FE80::55::A:AB

→ ☑ FE80:0000:0000:0055::000A:AB00

☐ FE80::0055::000A:AB

Explanation

Valid shortened forms are:

- FE80::55:0000:0000:A:AB00
- FE80:0000:0000:0055::000A:AB00 (FE80:0000:0000:55::A:AB00 could also be used)

Leading 0s within a quartet can be omitted. For example, 0055 can be shortened as 55. Addresses with consecutive zeros can be expressed more concisely by substituting a double-colon for the group of zeros. However, only one set of consecutive 0s can be omitted.

References

4.5.1 IPv6 Overview

4.5.2 IPv6 Benefits Facts

4.5.4 IPv6 Address Facts

4.5.5 IPv6 Address Type Facts

4.5.6 EUI-64 and Auto-Configuration

4.5.7 EUI-64 Addressing Facts

4.5.8 Configure IPv6

4.5.9 IPv6 Implementation Strategy Facts

4.5.10 IPv6 Configuration Facts

8.1.1 IPv6 Routing

8.1.2 IPv6 Routing Facts

8.1.3 Explore IPv6 Addressing on Routers

8.1.4 Common IPv6 Troubleshooting Issues

8.1.5 IPv6 Routing Facts

8.2.2 Configure OSPFv3 Routing

8.2.4 OSPFv3 Routing Facts

resources\text\t_ipv6_addg_ccna7\q_ipv6_addg_02_ccna7.question.xml

Question 3.

✓ Correct

Based on the address prefix for each IPv6 address on the right, identify the address type from the list on the left. (Addresses used might not represent actual addresses used in production.)

2001:6789:9078::ABCE:AFFF:FE98:0001

✓ Global unicast

FD00::8907:FF:FE76:ABC

✓ Unique local

FEA0::AB89:9FF:FE77:1234

✓ Link-local

FF00:98BD:6532::1

✓ Multicast

FF02::1:2

✓ Multicast

Explanation

Based on previous standards, global unicast addresses start with 20, but can now include any prefix that is not reserved. Addresses beginning with FC or FD are unique local addresses. Addresses beginning with FE8, FE9, FEA, or FEB are link-local addresses. Addresses beginning with FF are multicast addresses. There are no broadcast addresses in IPv6.

References

4.5.1 IPv6 Overview

- 📄 **4.5.2 IPv6 Benefits Facts**
- 📄 **4.5.4 IPv6 Address Facts**
- 📄 **4.5.5 IPv6 Address Type Facts**
- 🎬 **4.5.6 EUI-64 and Auto-Configuration**
- 📄 **4.5.7 EUI-64 Addressing Facts**
- 🖥 **4.5.8 Configure IPv6**
- 📄 **4.5.9 IPv6 Implementation Strategy Facts**
- 📄 **4.5.10 IPv6 Configuration Facts**
- 🎬 **8.1.1 IPv6 Routing**
- 📄 **8.1.2 IPv6 Routing Facts**
- 🖥 **8.1.3 Explore IPv6 Addressing on Routers**
- 🎬 **8.1.4 Common IPv6 Troubleshooting Issues**
- 📄 **8.1.5 IPv6 Routing Facts**
- 🖥 **8.2.2 Configure OSPFv3 Routing**
- 📄 **8.2.4 OSPFv3 Routing Facts**

resources\text\t_ipv6_addt_ccna7\q_ipv6_addt_01_ccna7.question.xml

Question 4 ✓ Correct

Which of the following IPv6 addresses is equivalent to the IPv4 loopback address of 127.0.0.1?

- ○ ::
- ○ FE80::1
- → ● ::1
- ○ FF02::1

Explanation

The IPv6 loopback address is ::1. The local loopback address is not assigned to an interface. It can be used to verify that the TCP/IP protocol stack has been properly installed on the host.

:: is the unspecified address (also identified ::/128). The unspecified address is used when there is no IPv6 address. It is typically used during system startup, when the host has not yet configured its address. The unspecified address should not be assigned to an interface.

Multicast addresses have an FF00::/8 prefix. FF02::/8 is the multicast prefix for all nodes on the local link.

References

4.5.1 IPv6 Overview

4.5.2 IPv6 Benefits Facts

4.5.4 IPv6 Address Facts

4.5.5 IPv6 Address Type Facts

8.1.1 IPv6 Routing

8.1.2 IPv6 Routing Facts

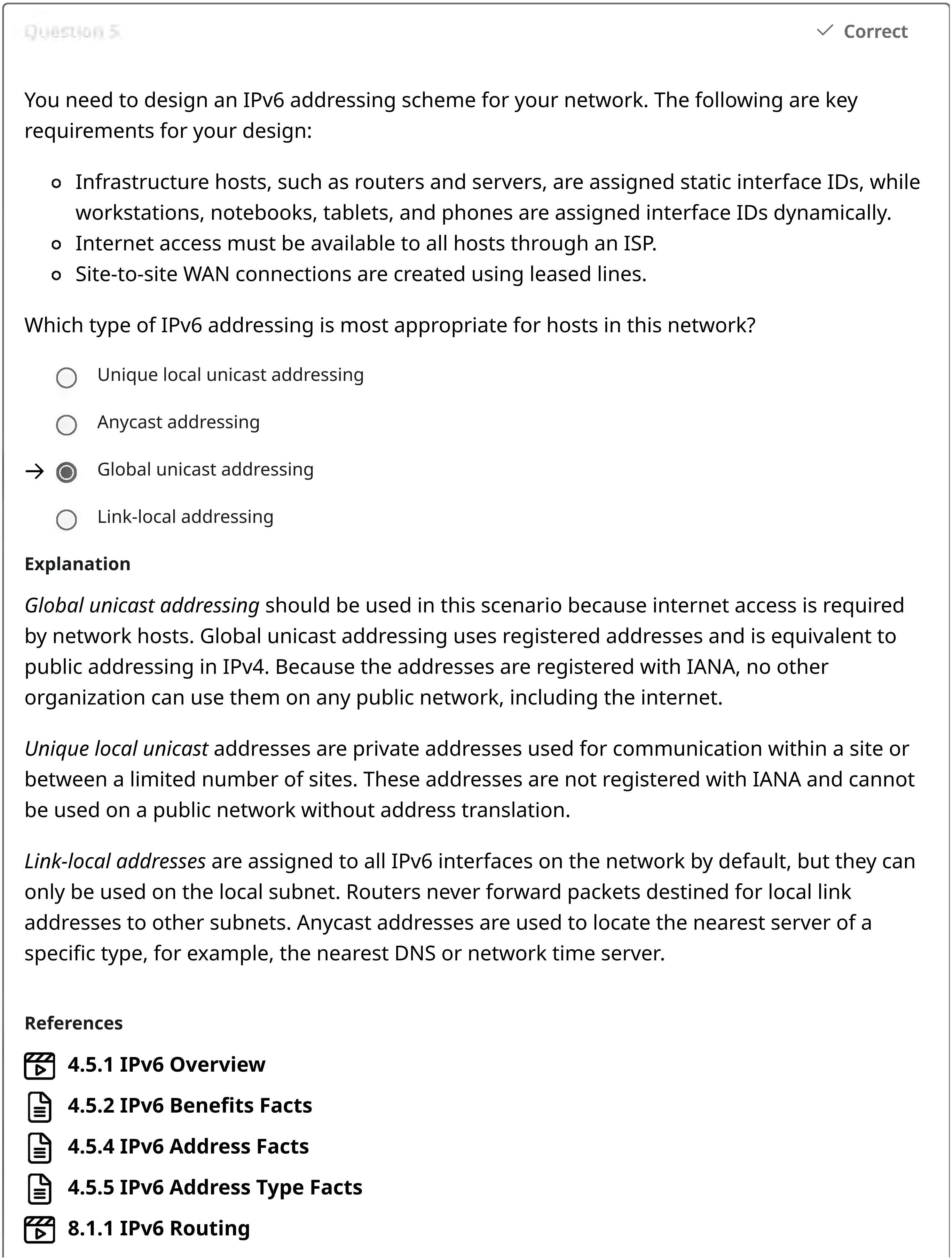
8.1.3 Explore IPv6 Addressing on Routers

8.1.4 Common IPv6 Troubleshooting Issues

8.1.5 IPv6 Routing Facts

8.2.2 Configure OSPFv3 Routing

resources\text\t_ipv6_addt_ccna7\q_ipv6_addt_02_ccna7.question.xml



Question 5

✓ Correct

You need to design an IPv6 addressing scheme for your network. The following are key requirements for your design:

- Infrastructure hosts, such as routers and servers, are assigned static interface IDs, while workstations, notebooks, tablets, and phones are assigned interface IDs dynamically.
- Internet access must be available to all hosts through an ISP.
- Site-to-site WAN connections are created using leased lines.

Which type of IPv6 addressing is most appropriate for hosts in this network?

○ Unique local unicast addressing

○ Anycast addressing

→ ● Global unicast addressing

○ Link-local addressing

Explanation

Global unicast addressing should be used in this scenario because internet access is required by network hosts. Global unicast addressing uses registered addresses and is equivalent to public addressing in IPv4. Because the addresses are registered with IANA, no other organization can use them on any public network, including the internet.

Unique local unicast addresses are private addresses used for communication within a site or between a limited number of sites. These addresses are not registered with IANA and cannot be used on a public network without address translation.

Link-local addresses are assigned to all IPv6 interfaces on the network by default, but they can only be used on the local subnet. Routers never forward packets destined for local link addresses to other subnets. Anycast addresses are used to locate the nearest server of a specific type, for example, the nearest DNS or network time server.

References

4.5.1 IPv6 Overview

4.5.2 IPv6 Benefits Facts

4.5.4 IPv6 Address Facts

4.5.5 IPv6 Address Type Facts

8.1.1 IPv6 Routing

8.1.2 IPv6 Routing Facts

8.1.3 Explore IPv6 Addressing on Routers

8.1.4 Common IPv6 Troubleshooting Issues

8.1.5 IPv6 Routing Facts

8.2.2 Configure OSPFv3 Routing

resources\text\t_ipv6_addt_ccna7\q_ipv6_addt_03_ccna7.question.xml

Question 6 ✓ Correct

Your organization has decided to implement unique local unicast IPv6 addressing. A global ID of FD01:A001:0001::/48 has been selected for the organization's IPv6 addressing scheme. The next 16 bits beyond the global ID have been used to define the following subnets:

- FD01:A001:0001:0001::/64
- FD01:A001:0001:0002::/64
- FD01:A001:0001:0003::/64
- FD01:A001:0001:0004::/64

You need to statically assign an interface ID to a router interface connected to the FD01:A001:0001:0003::/64 subnet. To ensure uniqueness, the interface ID should be constructed using the MAC address of the router interface.

Which interface configuration command would you use to do this?

→ ● **ipv6 address FD01:A001:0001:0003::/64 eui-64**

○ **ipv6 address FD01:A001:0001:0002::1/64**

○ **ipv6 address FD01:A001:0001:0003::/48 eui-64**

○ **ipv6 address FD01:A001:0001:0002::/64 eui-64**

○ **ipv6 address FD01:A001:0001:0003::1/64**

Explanation

The **ipv6 address FD01:A001:0001:0003::/64 eui-64** command statically assigns an interface ID to a router interface connected to the FD01:A001:0001:0003::/64 subnet using the MAC address of the router interface. When you use the **eu-64** option with the ipv6 address command, only the 64-bit network prefix for the address needs to be specified. The last 64 bits are automatically computed from the interface's MAC address.

The **ipv6 address FD01:A001:0001:0003::1/64** command statically assigns an interface ID of 0000:0000:0000:0001 to the router interface. This is a valid interface ID for the subnet, but it does not use the MAC address of the router interface. The **ipv6 address FD01:A001:0001:0002::1/64**, **ipv6 address FD01:A001:0001:0002::/64 eui-64**, and **ipv6 address FD01:A001:0001:0003::/48 eui-64** commands specify the wrong subnet for the scenario.

References

4.5.1 IPv6 Overview

4.5.2 IPv6 Benefits Facts

4.5.4 IPv6 Address Facts

4.5.5 IPv6 Address Type Facts

4.5.6 EUI-64 and Auto-Configuration

4.5.7 EUI-64 Addressing Facts

4.5.8 Configure IPv6

4.5.9 IPv6 Implementation Strategy Facts

4.5.10 IPv6 Configuration Facts

8.1.1 IPv6 Routing

8.1.2 IPv6 Routing Facts

8.1.3 Explore IPv6 Addressing on Routers

8.1.4 Common IPv6 Troubleshooting Issues

8.1.5 IPv6 Routing Facts

8.2.2 Configure OSPFv3 Routing

8.2.4 OSPFv3 Routing Facts

resources\text\t_eui64_ccna7\q_eui64_01_ccna7.question.xml

Question 7 ✓ Correct

You are working on a workstation with the following MAC address:

10-01-64-AB-78-96

Which of the following will be the link-local address using the modified EUI-64 format?

○ FC00::1001:64FF:FEAB:7896

○ FE80::1001:64AB:7896:FFFF

→ ● FE80::1201:64FF:FEAB:7896

○ FC00::1001:64AB:7896:FFFF

○ FE80::1001:64AB:7896

○ FC00::1001:64AB:7896

Explanation

Link-local addresses have a prefix of FE80::/10, meaning that they begin with FE80, FE90, FEA0, or FEB0. On Ethernet networks, the modified EUI-64 format interface ID can be automatically derived from the MAC address using the following process:

1. The MAC address is split into 24-bit halves.
2. The hex constant FFFE is inserted between the two halves to complete the 64-bit address.
   For example, 10-01-64-AB-78-96 becomes 1001:64**FF:FE**AB:7896 .
3. The seventh bit of the MAC address (reading from left to right) is set to binary 1. This bit is called the universal/local (U/L) bit.
   - Modifying the seventh binary bit modifies the second hex value in the address.
   - For a MAC address of 10-01-64-AB-78-96, the first two hex values translate to the binary number of 0001 0000.
   - Setting the seventh bit to 1 yields 0001 0010, which translates into 12 hex.

   In this example, the MAC address of 10-01-64-AB-78-96 in modified EUI-64 format becomes 1**2**01:64**FF:FE**AB:7896.

   Addresses with a FC00::/7 prefix are unique local addresses.

References

4.5.6 EUI-64 and Auto-Configuration

4.5.7 EUI-64 Addressing Facts

4.5.10 IPv6 Configuration Facts

8.1.1 IPv6 Routing

8.1.2 IPv6 Routing Facts

8.1.3 Explore IPv6 Addressing on Routers

8.1.4 Common IPv6 Troubleshooting Issues

8.1.5 IPv6 Routing Facts

8.2.2 Configure OSPFv3 Routing

resources\text\t_eui64_ccna7\q_eui64_02_ccna7.question.xml

Question 8: ✓ Correct

Which of the following are characteristics of 6-to-4 tunneling? (Select three.)

☐ Manually-configured tunnel endpoints

→ ☑ Dual stack routers

→ ☑ Works through NAT

☐ IPv4-only hosts communicate with IPv6-only hosts

☐ Dual stack hosts

→ ☑ Tunnel endpoints configured on routers

☐ Does not work through NAT

Explanation

With 6-to-4 tunneling, tunneling endpoints are configured automatically between devices. 6-to-4 tunneling:

- Is configured between routers at different sites.
- Requires dual-stack routers as the tunnel endpoints. Hosts can be IPv6-only hosts.
- Works through NAT.
- Uses a dynamic association of an IPv6 site prefix to the IPv4 address of the destination tunnel endpoint.
- Automatically generates an IPv6 address for the site using the 2002::/16 prefix followed by the public IPv4 address of the tunnel endpoint router.

References

4.5.1 IPv6 Overview

4.5.2 IPv6 Benefits Facts

4.5.4 IPv6 Address Facts

4.5.5 IPv6 Address Type Facts

4.5.6 EUI-64 and Auto-Configuration

4.5.7 EUI-64 Addressing Facts

4.5.8 Configure IPv6

4.5.9 IPv6 Implementation Strategy Facts

4.5.10 IPv6 Configuration Facts

8.1.1 IPv6 Routing

8.1.2 IPv6 Routing Facts

8.1.3 Explore IPv6 Addressing on Routers

8.1.4 Common IPv6 Troubleshooting Issues

8.1.5 IPv6 Routing Facts

8.2.2 Configure OSPFv3 Routing

8.2.4 OSPFv3 Routing Facts

resources\text\t_ipv6impl_ccna7\q_ipv6impl_01_ccna7.question.xml

Question 11:

✓ Correct

Your company has just started contracting with the government. As part of the contract, you have configured a special server for running a custom application. Contract terms dictate that this server use only IPv6.

You have several hosts that need to communicate with this server. These hosts only run IPv4 and cannot be configured to run IPv6.

Which solution would you use to allow the IPv4 clients to communicate with the IPv6 server?

→ ● NAT-PT

○ Dual stack

○ 6-to-4

○ ISATAP

○ Teredo

Explanation

The only solution that allows IPv4 hosts to communicate with the IPv6 server without running IPv6 on the client systems is Network Address Translation-Protocol Translation (NAT-PT). NAT-PT converts the IPv6 packet header into an IPv4 packet header, and vice versa. The device references a translation table as it converts the headers to ensure the packet is sent to the correct host.

A dual stack client is a host that runs both IPv4 and IPv6. In this scenario, it is not possible to run IPv4 on the server, and it is not possible to run IPv6 on the clients, so a dual stack configuration is not possible.

Teredo, 6-to-4, and Intra-site Automatic Tunnel Addressing Protocol (ISATAP) are all tunneling protocols that allow an IPv6 host to communicate with another IPv6 host through an IPv4 network. None of the tunneling protocols enable an IPv4 host to communicate with an IPv6 host.

References

4.5.1 IPv6 Overview

4.5.2 IPv6 Benefits Facts

4.5.4 IPv6 Address Facts

4.5.5 IPv6 Address Type Facts

4.5.6 EUI-64 and Auto-Configuration

4.5.7 EUI-64 Addressing Facts

4.5.8 Configure IPv6

4.5.9 IPv6 Implementation Strategy Facts

4.5.10 IPv6 Configuration Facts

8.1.1 IPv6 Routing

8.1.2 IPv6 Routing Facts

8.1.3 Explore IPv6 Addressing on Routers

8.1.4 Common IPv6 Troubleshooting Issues

8.1.5 IPv6 Routing Facts

8.2.2 Configure OSPFv3 Routing

8.2.4 OSPFv3 Routing Facts

resources\text\t_ipv6impl_ccna7\q_ipv6impl_02_ccna7.question.xml

Question 10 ✓ Correct

Which of the following IPv6 addresses is used by a host to contact a DHCP server?

○ FF02::2

→ ● FF02::1:2

○ FE80::2

○ FF02::1

○ FE80::1:2

○ FE80::1

Explanation

FF02::1:2 is the IPv6 address used to contact a DHCP server.

All addresses with the FF00::/8 prefix are multicast addresses.

IPv6 uses multicasts instead of broadcasts.

FF02::2 is the multicast address for all routers on the local link; FF02::1 is for all hosts on the link.

FE80::/10 is the prefix for link-local unicast addresses.

References

4.5.1 IPv6 Overview

4.5.2 IPv6 Benefits Facts

4.5.4 IPv6 Address Facts

4.5.5 IPv6 Address Type Facts

4.5.6 EUI-64 and Auto-Configuration

4.5.7 EUI-64 Addressing Facts

4.5.8 Configure IPv6

4.5.9 IPv6 Implementation Strategy Facts

4.5.10 IPv6 Configuration Facts

8.1.1 IPv6 Routing

8.1.2 IPv6 Routing Facts

8.1.3 Explore IPv6 Addressing on Routers

8.1.4 Common IPv6 Troubleshooting Issues

8.1.5 IPv6 Routing Facts

8.2.2 Configure OSPFv3 Routing

8.2.4 OSPFv3 Routing Facts

resources\text\t_ipv6_config_ccna7\q_ipv6_config_01_ccna7.question.xml

4.6.8 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 2/11/2025, 1:51:21 PM • **Time Spent:** 02:06

Score: 100%

Passing Score: 80%

Question 1

✓ Correct

You have a TCP/IP network with 50 hosts. There have been inconsistent communication problems between hosts. You run a protocol analyzer and discover that two hosts are assigned the same IP address.

Which protocol can you implement on your network to help prevent problems such as this?

○ IP

○ ICMP

○ IGMP

○ SNMP

→ ● DHCP

○ TCP

Explanation

You can use the dynamic host configuration protocol to set up a DHCP server that will assign IP addresses to network hosts automatically. DHCP servers will not assign the same IP address to two different hosts.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

resources\text\t_dhcp_ccna7\q_dhcp_01_ccna7.question.xml

Question 2 ✓ Correct

Which of the following statements about the dynamic host configuration protocol (DHCP) are true? (Select two.)

☐ It cannot be configured to assign the same IP address to the same host each time it boots.

→ ☑ It can deliver other configuration information in addition to IP addresses.

→ ☑ A DHCP server assigns addresses to requesting hosts.

☐ It is used only to deliver IP addresses to hosts.

☐ It can deliver IP addresses to hosts, but it cannot provide DNS server host configuration information.

Explanation

DHCP servers deliver IP addresses as well as other host configuration information to network hosts, including the default gateway and DNS server.

DHCP can be configured to assign any available address to a host, or it can assign a specific address to a specific host.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

4.7.1 DNS

4.7.2 Configure DNS

4.7.3 DNS Facts

4.7.4 Configure DNS on a Router

4.7.5 DNS Configuration Facts

resources\text\t_dhcp_ccna7\q_dhcp_02_ccna7.question.xml

Question 3 ✓ Correct

You have a DHCP server on your network. Which of the following is the correct order of DHCP messages exchanged between a client and server when the client obtains an IP address using a 4-way handshake?

○ DHCPREQUEST, DHCPOFFER, DHCPDISCOVER, DHCPACK

○ DHCPOFFER, DHCPREQUEST, DHCPDISCOVER, DHCPACK

○ DHCPREQUEST, DHCPOFFER, DHCPACK, DHCPDISCOVER

→ ● DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK

○ DHCPACK, DHCPREQUEST, DHCPDISCOVER, DHCPOFFER

Explanation

A DHCP client uses the following process to obtain an IP address:

1. Lease Request. The client initializes a limited version of TCP/IP and broadcasts a DHCPDISCOVER packet requesting the location of a DHCP server.
2. Lease Offer. All DHCP servers with available IP addresses send DHCPOFFER packets to the client. These include the client's hardware address, the IP address the server is offering, the subnet mask, the duration of the IP lease, and the IP address of the DHCP server making the offer.
3. Lease Selection. The client selects the IP address from the first offer it receives and broadcasts a DHCPREQUEST packet requesting to lease the IP address in that offer.
4. IP Lease Acknowledgment. The DHCP server that made the offer responds, and all other DHCP servers withdraw their offers. The IP addressing information is assigned to the client, and the offering DHCP server sends a DHCPACK (acknowledgement) packet directly to the client. The client finishes initializing and binding the TCP/IP protocol.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

4.7.1 DNS

4.7.2 Configure DNS

4.7.3 DNS Facts

4.7.4 Configure DNS on a Router

4.7.5 DNS Configuration Facts

resources\text\t_dhcp_ccna7\q_dhcp_03_ccna7.question.xml

✓ Correct

You have a small network as shown.

You configure DHCP on Router1 to provide IP addresses to all hosts connected to SwitchA. Following the configuration, you verify that Wrk1 has received an IP address from the DHCP service. Wrk1 can ping every host on the subnet, but cannot communicate with any hosts connected to Switch B or on the internet.

What should you do?

[redacted]

○ Manually configure the default gateway address on Wrk1.

○ Configure NAT on Router1.

→ ○ Configure the DHCP server to deliver the default gateway address along with the IP address.

○ Reconfigure the DHCP service to run on Router2 instead of Router1.

Explanation

The reason that Wrk1 cannot reach hosts on other subnets is because it has not been configured with a default gateway address. Configure the DHCP service to deliver the default gateway address.

Manually configuring the default gateway address on Wrk1 would require that you do the same for every host on the subnet. Manually configuring the default gateway also requires disabling DHCP, so you would also need to manually configure IP addresses for each host.

Configuring DHCP on Router2 would only solve the problem if the following conditions were met:

- The DHCP service on Router2 would need to be configured to deliver the default gateway address.
- DCHP requests originating from hosts attached to SwitchA would need to be able to pass through Router1.

NAT provides network address translation, where IP addresses are modified as they pass from a private network to the public network. In the diagram, NAT would be configured on Router2 for the entire network. By itself, NAT does not provide DHCP.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

resources\text\t_dhcp_ccna7\q_dhcp_04_ccna7.question.xml

Question 5

✓ Correct

You have a small network connected to the internet as shown below.

Router1 will provide NAT services to all hosts on the private network and DHCP services to hosts connected to SubnetA.

Srv1 is located on SubnetA. You want to make sure that this server is assigned the same IP address every time it boots, but you still want to centrally manage the address that it uses.

What should you do?

○ Create an address pool with the IP address for Srv1.

→ ● Configure a DHCP binding for Srv1.

○ Manually configure the IP address for Srv1.

○ Add a static inside-to-outside address translation rule for Srv1.

○ Add a static outside-to-inside address translation rule for Srv1.

Explanation

DHCP dynamically assigns IP addresses to hosts. To make sure that a specific host gets the same IP address each time, create a binding for the host. The binding associates the MAC address with the desired IP address.

An address pool identifies all possible addresses that can be assigned to hosts using DHCP. The pool does not have settings to associate the address with a specific host.

NAT translations are used to make sure that an inside host IP address is always associated with a specific outside global IP address.

Use a static translation rule to allow outside hosts to contact inside hosts.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

resources\text\t_dhcp_ccna7\q_dhcp_05_ccna7.question.xml

Question 6 ✓ Correct

You want to configure DHCP on your Cisco router to provide automatic IP address assignment to a single subnet. You will use 192.168.12.0/27 for the subnet address.

The router interface has been configured with an IP address of 192.168.12.1. Additionally, you want to make sure that a specific server, SrvFS, always gets the last IP address on the subnet.

How should you configure DHCP on the router? (Select two.)

☐ Create a DHCP binding for address 192.168.12.62.

☐ Create an address pool with a start address of 192.168.12.2 and end address of 192.168.12.62.

☐ Create a DHCP binding for address 192.168.12.14.

☐ Create an address pool with a start address of 192.168.12.2 and end address of 192.168.12.14.

→ ☑ Create a DHCP binding for address 192.168.12.30.

→ ☑ Create an address pool with a start address of 192.168.12.2 and end address of 192.168.12.30.

Explanation

The DHCP address pool identifies the range of IP addresses that can be assigned by the DHCP server. Because the router itself has been assigned the first IP address on the subnet, the pool range begins at 192.168.12.2. To identify the ending range, you must apply the subnet mask to the subnet to find the ending address. A 27-bit mask provides subnets with 32 addresses per subnet. Removing the last address for the broadcast address, the last address in the range is 192.168.12.30.

To assign an IP address to a specific host, define a DHCP binding. The DHCP binding associates the MAC address with the desired IP address. The assigned IP address can be part of the pool range.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

resources\text\t_dhcpconfig_ccna7\q_dhcpconfig_01_ccna7.question.xml

Question 7

✓ Correct

Question 8 ✓ Correct

You have configured DHCP on your router. A partial configuration is shown below:

```
hostname RouterA
!
interface FastEthernet0/0
 ip address 192.168.11.1 255.255.255.0
 speed auto
 duplex auto
 ip access-group 1 in
!
interface FastEthernet0/1
 no ip address
 speed auto
 duplex auto
!
ip dhcp excluded-address 192.168.11.1 192.168.11.50
ip dhcp excluded-address 192.168.12.1 192.168.12.50
!
ip dhcp pool 0
 network 192.168.11.0 255.255.255.0
 domain-name westsim.com
 dns-server 192.168.11.2 192.168.12.2
!
ip dhcp pool 2
 host 192.168.11.166
 hardware-address 02c7.f800.0422
!
access-list 1 permit 192.168.11.0 0.0.0.255
!
```

Srv2 is a host connected to the Fa0/0 interface of RouterA with a MAC address of 02c7.f800.0422. When it boots, it is assigned the IP address of 192.168.11.166. It can only communicate with hosts on the same subnet.

What should you do to correct the problem?

○ Add 192.168.11.166 as an excluded address.

○ Change the host address in DHCP pool 2 to 192.168.11.1.

○ Manually configure a default gateway address on Srv2.

You have configured DHCP on your router. A partial configuration is shown below:

```
hostname RouterA
!
interface FastEthernet0/0
 ip address 192.168.11.1 255.255.255.0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 ip address 192.168.12.1 255.255.255.0
 speed auto
 duplex auto
!
ip dhcp excluded-address 192.168.11.1 192.168.11.50
!
ip dhcp pool 0
 network 192.168.11.0 255.255.255.0
 domain-name westsim.com
 dns-server 192.168.11.2 192.168.12.2
 default-router 192.168.11.1
!
ip dhcp pool 1
 network 192.168.12.0 255.255.255.0
 domain-name westsim.com
 dns-server 192.168.11.2 192.168.12.2
 default-router 192.168.12.1
!
ip dhcp pool 2
 host 192.168.12.166
 hardware-address 02c7.f800.0422
!
access-list 1 permit 192.168.11.0 0.0.0.255
!
```

Srv2 is a host connected to the Fa0/1 interface of RouterA. Its MAC address is 02c7.f800.0422 and is configured to use DHCP to request an IP address.

→ It will not be assigned an IP address.

○ 192.168.12.166

192.168.11.34

192.168.11.166

192.168.12.16

Explanation

Srv2 will not be assigned an IP address because DHCP is not listening for requests on Fa0/1. DHCP runs on interfaces based on the IP address assigned to the interface. If the interface is assigned an IP address that matches a DHCP pool, then DHCP listens for requests on that interface. But because Fa0/1 does not have an IP address, it will not run DHCP.

If Fa0/1 had been assigned an IP address on the 192.168.12.0/24 subnet, it would assign address 192.168.12.166 to the host based on the binding defined in DHCP pool 2.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

resources\text\t_dhcpconfig_ccna7\q_dhcpconfig_02_ccna7:question.xml

→ Add a **default-router** statement to DHCP pool 2.

○ Add an **ip access-group** statement for Fa0/0.

Explanation

Srv2 cannot communicate with hosts on other subnets because it is not configured with a default router. This is happening because DHCP pool 2 is not configured with a **default-router** statement. This parameter assigns a default gateway value along with an IP address.

Manually configuring a default gateway for Srv2 would only work if you manually assigned the IP address; you cannot get the IP address from DHCP and have a manually assigned default gateway address.

Srv2 has been assigned the address of 192.168.11.166 because its MAC address matches the MAC address configured for pool 2.

Access lists are not used when configuring DHCP.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

resources\text\t_dhcpconfig_ccna7\q_dhcpconfig_03_ccna7:question.xml

Question 9 ✓ Correct

You have a Cisco router connected to a local ISP. The ISP dictates that the router use DHCP to receive its IP address and other configuration information.

Which command should you use when configuring the ISP interface on the router?

- ○ **ip dhcp-client**
- ○ **ip dhcp database**
- → ● **ip address dhcp**
- ○ **ip dhcp-server**

Explanation

To configure a Cisco device to use DHCP to receive configuration information, use the **ip address dhcp** command. On a router, use this command in interface mode for the physical interface. On a switch, use the command in VLAN 1 interface mode. The command replaces any manually configured address for the interface. The Cisco device also receives the default gateway and name server information from the DHCP router if those items are not manually specified.

Use the **ip dhcp-server** and **ip dhcp database** commands to manage a Cisco device that is a DHCP server. Use the **ip dhcp-client** command to configure advanced settings for the DHCP client.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

resources\text\t_dhcpconfig_ccna7\q_dhcpconfig_04_ccna7.question.xml

Question 10

✓ Correct

You have three hosts on network 192.168.10.0/24 as shown.

If interface Fa0/0 on RouterB has the **ip helper-address 172.17.10.20** configuration command in its running configuration, which of the following statements are true? (Select two.)

→ ☑ The hosts may receive their IP address information through DHCP.

□ RouterB will discard the DHCP packets from the hosts.

□ RouterA will discard the DHCP packets routed through RouterB.

□ RouterB will forward broadcast packets sent to the DNS, BOOTP, TFTP, FTP, and ARP ports.

□ The voice traffic will be separated from the data traffic using 802.1q tagging.

→ ☑ RouterB will forward broadcast packets sent to the: Time, DNS, BOOTP, and TFTP ports.

Explanation

The **ip helper-address *a.b.c.d*** interface configuration command configures an interface to forward UPD broadcasts, including BOOTP and DHCP, to the specified DHCP server address via IP unicast.

- The ***a.b.c.d*** address can be a specific DHCP server address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables other servers to respond to DHCP requests.
- If you have multiple servers (such as DNS, TFTP, or DHCP servers), you can configure one helper address for each server.

By default, when an interface is configured as a relay agent, it forwards packets sent to all the well-known UDP ports that may be included in a UDP broadcast message. You can configure the relay agent to eliminate specific ports from the forwarding service. The well-known UDP broadcast ports include the following:

- 37: Time
- 49: TACACS

4.7.11 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)

Date: 2/12/2025, 4:36:20 PM • **Time Spent:** 02:15

Score: 100%

Passing Score: 80%

Question 1.

✓ Correct

Listed below are several DNS record types. Match the record type on the left with its function on the right.

Points a hostname to an IPv4 address.

✓ A

Provides alternate names to hosts that already have a host record.

✓ CNAME

Points an IP address to a hostname.

✓ PTR

Points a hostname to an IPv6 address.

✓ AAAA

Identifies servers that can be used to deliver mail.

✓ MX

Explanation

Records are used to store entries for hostnames, IP addresses, and other information in the zone database. Below are some common DNS record types:

- The A record maps an IPv4 (32-bit) DNS host name to an IP address. This is the most common resource record type.
- The AAAA record maps an IPv6 (128-bit) DNS host name to an IP address.
- The PTR record maps an IP address to a hostname and is referred to as a reverse lookup.
- The MX record identifies servers that can be used to deliver email and is referred to as a Mail eXchanger.
- The CNAME (Canonical NAME) record provides alternate names (or aliases) to hosts that already have a host record. Using a single A record with multiple CNAME records means that when the IP address changes, only the A record needs to be modified.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

4.7.1 DNS

4.7.2 Configure DNS

4.7.3 DNS Facts

4.7.4 Configure DNS on a Router

4.7.5 DNS Configuration Facts

resources\text\t_dns_ccna7\q_dns_01_ccna7.question.xml

Question 2

✓ Correct

If dynamic DNS is being used, which of the following events will cause a dynamic update of the host records? (Select two.)

□ A CNAME record is added to the DNS server.

→ ☑ The **ipconfig /registerdns** command is entered on a workstation.

→ ☑ The DHCP server renews an IP address lease.

□ The browser cache on a workstation is cleared.

□ An MX record is added to the DNS server.

Explanation

Dynamic DNS (DDNS) enables clients or the DHCP server to update records in the zone database automatically. Dynamic updates occur when:

- A network host's IP address is added, released, or changed.
- The DHCP server changes or renews an IP address lease.
- The client's DNS information is manually changed using the **ipconfig /registerdns** command.

Clearing a browser's cache has no effect on DNS records. Because MX records and CNAME records need to be manually added and created, they have no effect on DDNS.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

4.7.1 DNS

4.7.2 Configure DNS

4.7.3 DNS Facts

4.7.4 Configure DNS on a Router

4.7.5 DNS Configuration Facts

resources\text\t_dns_ccna7\q_dns_02_ccna7.question.xml

Question 3 ✓ Correct

Which of the following services automatically creates and deletes DNS host records when an IP address lease is created or released?

○ DHCP Relay

○ Forward lookup

○ Dynamic NAT

→ ● Dynamic DNS

Explanation

Dynamic DNS (DDNS) enables clients or the DHCP server to update records in the zone database automatically whenever an IP address lease is created or renewed.

A forward lookup is the process of resolving a hostname to an IP address. A DHCP relay is used to forward DHCP requests to a DHCP server in a different subnet. Dynamic NAT is used to automatically map internal IP addresses with a dynamic port assignment.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

4.7.1 DNS

4.7.2 Configure DNS

4.7.3 DNS Facts

4.7.4 Configure DNS on a Router

4.7.5 DNS Configuration Facts

resources\text\t_dns_ccna7\q_dns_03_ccna7.question.xml

Question 4 ✓ Correct

You want to implement a protocol on your network that allows computers to find the IP address of a host from a logical name. Which protocol should you implement?

○ Telnet

○ ARP

→ ● DNS

○ DHCP

Explanation

DNS is a system that is distributed throughout the internetwork to provide address/name resolution. For example, the name www.mydomain.com would be identified with a specific IP address.

ARP is a protocol for finding the IP address from a known MAC address. DHCP is a protocol used to assign IP addresses to hosts. Telnet is a remote management utility.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

4.7.1 DNS

4.7.2 Configure DNS

4.7.3 DNS Facts

4.7.4 Configure DNS on a Router

4.7.5 DNS Configuration Facts

resources\text\t_dns_ccna7\q_dns_04_ccna7.question.xml

Question 5 ✓ Correct

You are setting up a new branch office for your company. You would like to implement solutions to provide the following services:

- Hosts should be able to contact other hosts using names such as server1.westsim.com.
- IP address assignment should be centrally managed.

Which services should you implement on your network to meet the requirements? (Select two.)

☐ NAT

→ ☑ DHCP

☐ RARP

→ ☑ DNS

☐ ICS

☐ WINS

Explanation

Use the domain name system (DNS) to provide name resolution. Clients use logical names to identify computers. DNS maintains a list of logical names and their corresponding IP addresses.

Use dynamic host configuration protocol (DHCP) to assign IP addresses to hosts. When a host system boots, it obtains an IP address from the DHCP server. DHCP can also be configured to provide additional IP configuration information, such as the default gateway and DNS server addresses.

WINS is a NetBIOS name resolution protocol. It is not a TCP/IP protocol. ARP is a protocol for obtaining the MAC address of a host from its IP address.

Network address translation (NAT) and internet connection service (ICS) are two methods of connecting a private network to the internet. While NAT might be required for the branch office, the scenario did not ask you to provide internet connectivity to the branch office.

References

4.6.1 DHCP Overview

📄 **4.6.2 DHCP Facts**

🖥 **4.6.3 Set Up DHCP**

📄 **4.6.4 DHCP Configuration Facts**

🎬 **4.7.1 DNS**

🖥 **4.7.2 Configure DNS**

📄 **4.7.3 DNS Facts**

🖥 **4.7.4 Configure DNS on a Router**

📄 **4.7.5 DNS Configuration Facts**

resources\text\t_dns_ccna7\q_dns_05_ccna7.question.xml

Question 6.

✓ **Correct**

Match the DNS components on the left with its function on the right.

Managed by the Internet Corporation of Assigned Names and Numbers (ICANN).

✓ Top-level domain

Includes the host name and all domain names separated by periods.

✓ Fully qualified domain name

The part of a domain name that represents a specific host.

✓ Hostname

Has a complete copy of all the records for a particular domain.

✓ Authoritative server

The last part of a domain name.

✓ Top-level domain

Denotes a fully qualified, unambiguous domain name.

✓ . (dot) domain

Explanation

The . (dot) domain, or root domain, denotes a fully qualified, unambiguous domain name.

A top-level domain (TDL) is the last part of a domain name (for example, .com, .edu, .gov). TDLs are managed by the Internet Corporation of Assigned Names and Numbers (ICANN).

The fully qualified domain name (FQDN) includes the hostname and all domain names separated by periods.

The hostname is the part of a domain name that represents a specific host.

An authoritative server is a DNS server that has a complete copy of all the records for a particular domain.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

4.7.1 DNS

4.7.2 Configure DNS

4.7.3 DNS Facts

4.7.4 Configure DNS on a Router

4.7.5 DNS Configuration Facts

resources\text\t_dns_ccna7\q_dns_06_ccna7.question.xml

Question 7 ✓ Correct

What is the difference between a forward lookup zone and a reverse lookup? (Select two.)

□ A forward lookup finds the host name from a given IP address.

→ ☑ A reverse lookup finds the host name from a given IP address.

□ A reverse lookup finds the IP address for a given host name.

□ A forward lookup finds the DNS server name from a given IP address.

→ ☑ A forward lookup finds the IP address for a given host name.

□ A reverse lookup finds the DNS server name from a given IP address.

Explanation

A forward lookup finds the IP address for a given hostname.

A reverse lookup finds the hostname from a given IP address.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

4.7.1 DNS

4.7.2 Configure DNS

4.7.3 DNS Facts

4.7.4 Configure DNS on a Router

4.7.5 DNS Configuration Facts

resources\text\t_dns_ccna7\q_dns_07_ccna7.question.xml

Question 8 ✓ Correct

You have a workstation configured with DNS server addresses as follows:

- Primary DNS server = 192.168.1.1
- Alternate DNS server = 192.168.1.155

While browsing the internet, you go to www.cisco.com. A few minutes later, you type **ping www.cisco.com** into a command prompt.

How will the workstation get the IP address for www.cisco.com?

○ By querying server 192.168.1.155

→ ● Out of its local DNS cache

○ By querying server 192.168.1.1

○ Out of the HOSTS file

Explanation

In this instance, because the workstation has recently resolved the DNS hostname, it retrieves the IP address from its local DNS cache. DNS name resolution looks for information in different locations in the in the following order:

1. Local DNS cache
2. HOSTS file
3. DNS server query

If the primary DNS server is unavailable, the secondary DNS servers are queried in order. If a name server responds that the name is unknown, no additional servers are consulted.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

4.7.1 DNS

4.7.2 Configure DNS

4.7.3 DNS Facts

4.7.4 Configure DNS on a Router

4.7.5 DNS Configuration Facts

resources\text\t_hostnames_ccna7\q_hostnames_01_ccna7.question.xml

Question 9. ✓ Correct

Listed below are several places that a workstation checks to resolve DNS hostnames.

- A. Primary DNS server
- B. Secondary DNS servers
- C. HOSTS file
- D. Local DNS cache

In a browser, you type the name of a website. In which order will these locations be checked during the name resolution process?

○ C, D, A, B

○ A, B, C, D

○ A, B, D, C

→ ● D, C, A, B

○ A, C, D, B

Explanation

DNS name resolution looks for information in the following locations in a certain order:

1. Local DNS cache
2. HOSTS file
3. DNS server query

If the primary DNS server is unavailable, the secondary DNS servers are queried in order. If a name server responds that the name is unknown, no additional servers are consulted.

References

4.6.1 DHCP Overview

4.6.2 DHCP Facts

4.6.3 Set Up DHCP

4.6.4 DHCP Configuration Facts

4.7.1 DNS

4.7.2 Configure DNS

4.7.3 DNS Facts

4.7.4 Configure DNS on a Router

4.7.5 DNS Configuration Facts

resources\text\t_hostnames_ccna7\q_hostnames_02_ccna7.question.xml

Question 10 ✓ Correct

For each operation on the right, match the appropriate command from the list on the left.

Configure DNS server addresses for the router to use for resolving hostnames.

✓ **ip name-server**

Create static entries for hosts that associate each hostname with an IP address.

✓ **ip host**

Prevent the router from using DNS to resolve hostnames.

✓ **no ip domain-lookup**

Set the DNS name used by the router.

✓ **hostname**

Explanation

Use the **ip name-server** command to configure DNS server addresses for the router to use for resolving host names.

Use the **ip host** command to create static entries for hosts that associate a hostname with an IP address.

Use the **no ip domain-lookup** command to prevent the router from using DNS to resolve host names. Use **ip domain-lookup** to enable the router to use DNS.

Use the **hostname** command to set the DNS name used by the router.

Use **[no] ip hostname** strict (disabled by default) to ensure strict compliance with Section 2.1 of RFC 1123.

References

- 🎬 **4.6.1 DHCP Overview**
- 📄 **4.6.2 DHCP Facts**
- 🖥 **4.6.3 Set Up DHCP**
- 📄 **4.6.4 DHCP Configuration Facts**
- 🎬 **4.7.1 DNS**
- 🖥 **4.7.2 Configure DNS**
- 📄 **4.7.3 DNS Facts**
- 🖥 **4.7.4 Configure DNS on a Router**
- 📄 **4.7.5 DNS Configuration Facts**

resources\text\t_hostnames_ccna7\q_hostnames_03_ccna7.question.xml

5.1.10 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)

Date: 2/17/2025, 11:02:58 AM • **Time Spent:** 03:55

Score: 100%

Passing Score: 80%

Question 1 ✓ Correct

Which of the following describes the role of Access Switches and how they are implemented in the design of a local area network on a university or corporate campus? (Select three.)

- □ Not needed in a three-tier network design.
- → ☑ Connected to distribution switches using one or more ports or uplinks.
- □ Linked to each other via high-speed connections.
- → ☑ Give end users access to the local area network.
- □ Constitute the second tier in a two-tier network design.
- → ☑ Communicate with each other through distribution switches.
- □ Connected to high-speed core switches.

Explanation

An access switch, as its name suggests, gives end users access to the local area network. That is, end user devices are connected to access switches, and these switches send data to and from specific computers or nodes that are connected to them. In an office building, each floor will usually contain one or more access switches with cables that run from the switch to individual rooms or cubicles.

Each of these access switches communicate with each other through distribution switches. Typically, each access switch is connected to a distribution switch using one or more ports or uplinks. The multiple connections not only increase redundancy, but also the maximum bandwidth between the switches.

References

5.1.2 Switch Architecture Facts

resources\text\t_architecture_ccna7\q_architecture_01_ccna7.question.xml

Question 2 ✓ Correct

An Ethernet frame has just arrived on a switch port. The switch examines the destination MAC address of the frame. It is a unicast address, but no mapping exists in the CAM table for the destination address.

Assuming that no VLANs are configured, what happens next?

○ A new entry is added to the CAM table that maps the source device's MAC address to the port on which the frame was received.

→ ○ The switch sends a copy of the frame to all connected devices on all ports.

○ The switch sends the frame to the switch port specified in the CAM table.

○ The switch ignores the frame and does not forward it.

Explanation

When a frame arrives on a switch interface, the switch examines the frame's destination MAC address. If it is a unicast address, but no mapping exists in the CAM table for the destination address, the switch floods the frame to all ports that are members of the same VLAN. Connected devices to whom the frame is not addressed drop the frame. The device to which the frame is addressed receives and processes the frame.

Filtering occurs when a switch ignores a frame and does not forward it because the destination device is connected to the same port from which the frame was received. If the source MAC address is not in the switch's CAM table, a new entry is added to the table that maps the source device's MAC address to the port on which the frame was received. If the destination MAC address of the frame is a unicast address and a mapping exists in the CAM table for the destination address, the switch sends the frame to the switch port specified in the CAM table.

References

5.1.3 Switch Operations

5.1.4 Unicast, Broadcast, and Multicast Frames

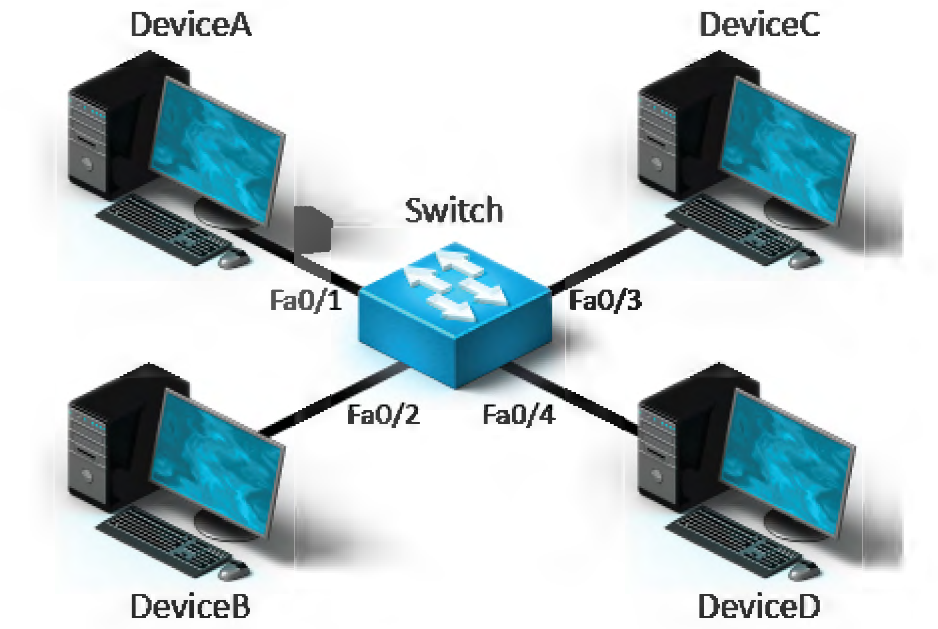
5.1.5 Switch Operations Facts

resources\text\t_frametype_ccna7\q_frametype_01_ccna7.question.xml

✓ Correct

Device B sends a frame to Device A on the network shown. The switch has an entry in its CAM table for Device A in its database, but not for Device B.

Which of the following best describes what the switch does with the message?



○ The switch records the address and port for Device B in its database. It sends the frame out all ports except Fa0/2.

○ The switch sends the frame out port Fa0/1.

○ The switch sends the frame out all ports except Fa0/2.

→ ○ The switch records the address and port for Device B in its database. It sends the frame out port Fa0/1.

Explanation

If an entry for the sending device does not currently exist in the switch's database, it records the device address and its port. If it knows the destination device's location, it sends the frame out that port.

If the switch does not know the destination device's location, it sends the frame out all ports except for the port on which the frame was received.

References

5.1.3 Switch Operations

5.1.4 Unicast, Broadcast, and Multicast Frames

5.1.5 Switch Operations Facts

resources\text\t_frametype_ccna7\q_frametype_02_ccna7.question.xml

✓ Correct

You have a switch connected to a small network as shown. A hub connects Wrk1 and Wrk5 to the switch. The switch has the following information in its CAM table:

Port	**Device**
Fa0/1	Wrk1 Wrk5
Fa0/2	--
Fa0/3	Wrk3
Fa0/4	--

Wrk1 sends a frame addressed to Wrk5. What will the switch do with the frame? (Select two.)

☐ Record the location of Wrk1 in its database.

□ Forward the frame out port Fa0/1.

→ ☑ Not record the location of any device.

□ Forward the frame out all ports.

□ Forward the frame out all ports except Fa0/1.

□ Record the location of Wrk5 in its database.

→ ☑ Drop the frame.

Explanation

Because the switch knows the location of both the sending device (Wrk1) and the location of the destination device (Wrk5), it will not record any information in its database. Because the destination port is the same as the source port, it will drop the frame and not forward it out any other port.

References

5.1.3 Switch Operations

5.1.4 Unicast, Broadcast, and Multicast Frames

5.1.5 Switch Operations Facts

resources\text\t_frametype_ccna7\q_frametype_03_ccna7.question.xml

✓ Correct

You have a network consisting of a switch, a router, a hub, and several workstations connected as shown in the graphic. No VLANs have been configured.

How many collision domains exist on the network shown?

Router
Switch

○ 1

○ 2

○ 3

→ ● 4

○ 5

○ 7

Explanation

The network has four collision domains. Each switch port is in its own collision domain. All computers connected to a hub share the same collision domain.

References

4.5.9 IPv6 Implementation Strategy Facts

5.1.6 Collision and Broadcast Domains

5.1.7 Broadcast and Collision Domain Facts

5.1.8 Switching Methods

5.1.9 Switching Method Facts

resources\text\t_lanseg_ccna7\q_lanseg_01_ccna7.question.xml

Question [illegible]

✓ Correct

You administer a network that uses bridges to connect network segments. The network is currently suffering from serious broadcast storms.

What can you do to solve the problem?

○ Install a central gateway to absorb broadcast storms.

○ Install a repeater at the end of each segment.

○ Replace the bridges with gateways.

→ ● Replace the bridges with routers.

Explanation

Broadcast messages are sent to every computer on the network. Too many broadcast messages can degrade system performance. A broadcast storm occurs when there are so many broadcast messages on the network that they approach or exceed the network bandwidth. Bridges, which operate at the Data Link layer, forward broadcasts. You can use routers to segment the network, which prevents broadcast storms because routers do not forward broadcasts from network to network.

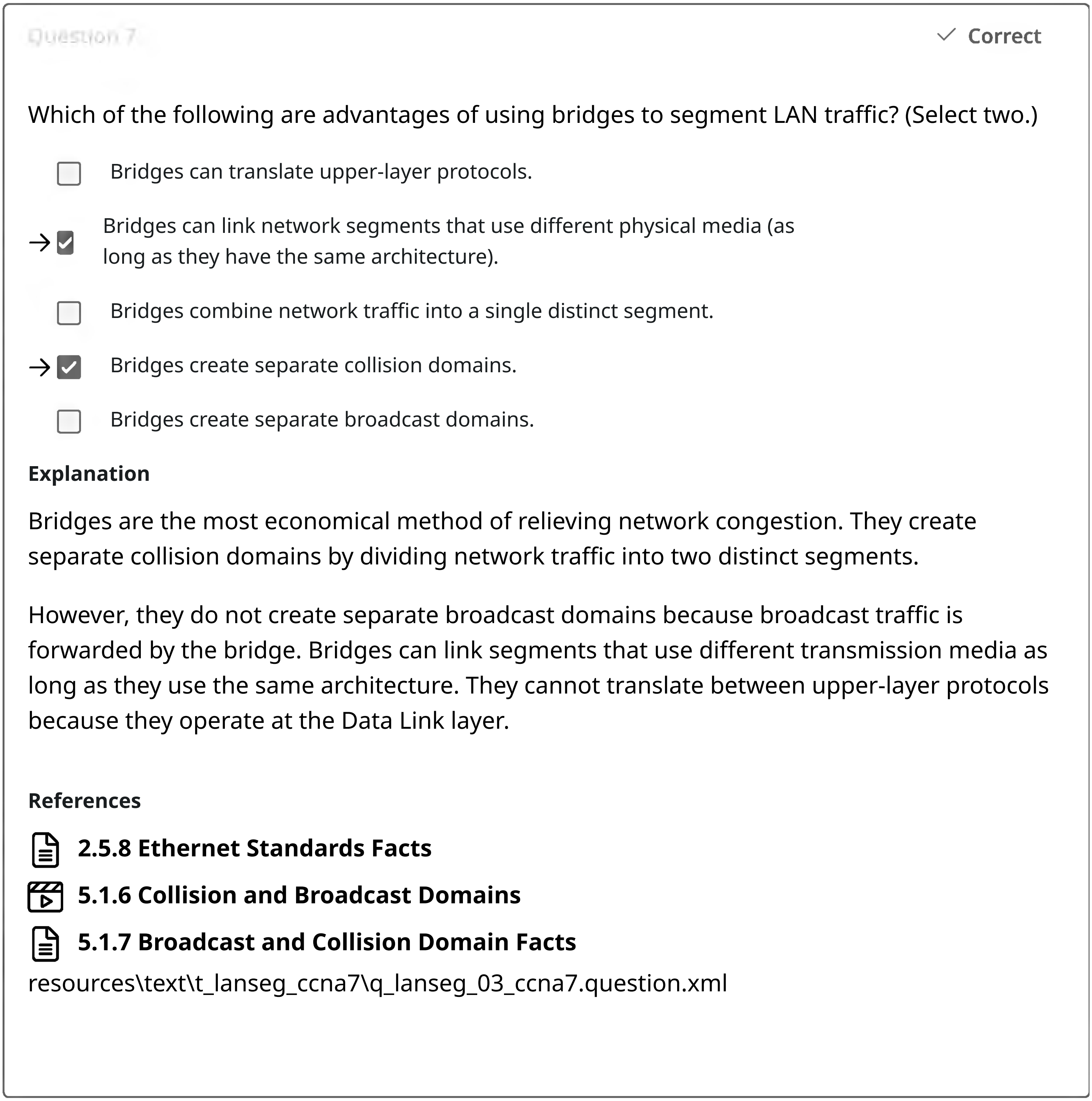
References

2.5.8 Ethernet Standards Facts

5.1.6 Collision and Broadcast Domains

5.1.7 Broadcast and Collision Domain Facts

resources\text\t_lanseg_ccna7\q_lanseg_02_ccna7.question.xml



Question 7

✓ Correct

Which of the following are advantages of using bridges to segment LAN traffic? (Select two.)

- □ Bridges can translate upper-layer protocols.
- → ☑ Bridges can link network segments that use different physical media (as long as they have the same architecture).
- □ Bridges combine network traffic into a single distinct segment.
- → ☑ Bridges create separate collision domains.
- □ Bridges create separate broadcast domains.

Explanation

Bridges are the most economical method of relieving network congestion. They create separate collision domains by dividing network traffic into two distinct segments.

However, they do not create separate broadcast domains because broadcast traffic is forwarded by the bridge. Bridges can link segments that use different transmission media as long as they use the same architecture. They cannot translate between upper-layer protocols because they operate at the Data Link layer.

References

2.5.8 Ethernet Standards Facts

5.1.6 Collision and Broadcast Domains

5.1.7 Broadcast and Collision Domain Facts

resources\text\t_lanseg_ccna7\q_lanseg_03_ccna7.question.xml

Question 8 ✓ Correct

You are the network administrator for a rapidly growing company with a 100BaseT network. Users have recently complained about slow file transfers. In a check of network traffic, you discover a high number of collisions.

Which connectivity device would best reduce the number of collisions and prepare for future growth?

○ Router

→ ● Switch

○ Hub

○ Bridge

Explanation

A switch would be the best choice in this situation. Switches can provide benefits at a lower cost per port, and they offer more administration options.

A bridge segments traffic and reduces collisions, but it would be harder to maintain and to add new bridges as the network grows.

A router would prepare for growth and reduce collisions.

References

4.5.9 IPv6 Implementation Strategy Facts

5.1.6 Collision and Broadcast Domains

5.1.7 Broadcast and Collision Domain Facts

5.1.8 Switching Methods

5.1.9 Switching Method Facts

resources\text\t_lanseg_ccna7\q_lanseg_04_ccna7.question.xml

Question 9.

✓ Correct

Which frame processing method causes a switch to wait until the first 64 bytes of the frame have been received before forwarding the frame to the destination device?

- ○ Store-and-forward
- ○ Adaptive
- ○ Cut-through
- → ● Fragment-free

Explanation

When using fragment-free processing, the switch starts to forward a frame before the entire the frame has arrived. The switch waits until the first 64 bytes of the frame are received before forwarding the frame to the destination device. Typically, a collision is detected within the first 64 bytes of a frame transmission. By waiting until the first 64 bytes have arrived, it is assumed that any frames corrupted by a collision are detected by the switch.

When using store-and-forward processing, the switch fully buffers frames and checks their integrity before forwarding them. When using cut-through processing, the switch starts to forward a frame as soon as its header is received, but before the rest of the frame has arrived. As a result, corrupt frames are forwarded before they can be detected. The adaptive frame processing option automatically selects a processing method (store-and-forward, cut-through, or fragment-free).

References

4.5.9 IPv6 Implementation Strategy Facts

5.1.6 Collision and Broadcast Domains

5.1.7 Broadcast and Collision Domain Facts

5.1.8 Switching Methods

5.1.9 Switching Method Facts

resources\text\t_switchmethod_ccna7\q_switchmethod_01_ccna7.question.xml

Question 10 ✓ Correct

Which of the following are true of store-and-forward switches? (Select three.)

- □ Frames with errors are forwarded.
- → ☑ Frames with errors are dropped.
- □ Latency is less than with cut-through switches.
- □ Frames are forwarded without being checked for errors.
- □ All frames are forwarded, regardless of whether they contain errors.
- → ☑ Frames are checked for errors before being forwarded.
- → ☑ Latency is greater than with cut-through switches.

Explanation

Store-and-forward switches receive the entire frame, verify its integrity (check for errors), and then forward it to the correct port. Frames with errors are dropped.

Cut-through switches do not check for errors. They forward frames regardless of their integrity. Because store-and-forward switches check for errors, latency (delay time) is greater than with cut-through switches.

References

4.5.9 IPv6 Implementation Strategy Facts

5.1.6 Collision and Broadcast Domains

5.1.7 Broadcast and Collision Domain Facts

5.1.8 Switching Methods

5.1.9 Switching Method Facts

resources\text\t_switchmethod_ccna7\q_switchmethod_02_ccna7.question.xml

5.2.13 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)

Date: 2/17/2025, 1:54:23 PM • **Time Spent:** 02:39

Score: 100%

Passing Score: 80%

Question 1. ✓ Correct

A workstation is connected to a switch on the Gi0/2 interface using a straight-through cable. The Ethernet interface in the workstation has been manually configured to use a 100 Mbps link speed and full duplexing.

Which of the following are true in this scenario? (Select three.)

→ ☑ If the link speed is 1000 Mbps or faster, full-duplex is used.

→ ☑ The switch attempts to sense the link speed. If it can't, the slowest link speed supported on the interface is selected.

☐ If the link speed is 10 Mbps or 100 Mbps, full-duplex is used.

☐ If the link speed is 100 Mbps or slower, autonegotiation is disabled.

☐ The switch interface will display as administratively down.

→ ☑ If the link speed is 10 Mbps or 100 Mbps, half-duplex is used.

☐ If the link speed is 1000 Mbps or faster, half-duplex is used.

Explanation

By default, the link speed and duplex configuration for Ethernet interfaces in Cisco devices are set using IEEE 802.3u autonegotiation. The interface negotiates with remote devices to determine the correct settings. However, autonegotiation can be disabled on the Cisco device and/or other Ethernet network hosts. When this happens, devices with autonegotiation enabled try to negotiate link speed and duplexing, but get no response. When autonegotiation fails, Cisco devices that have autonegotiation enabled default to the following:

- The interface will attempt to sense the link speed. If it can't, the slowest link speed supported on the interface is used, which is usually 10 Mbps.
- If the link speed selected is 10 Mbps or 100 Mbps, half-duplex is used. If it is 1000 Mbps or faster, full-duplex is used.

In this situation, link speed and duplex mismatches are likely to occur between network devices on the same link. When this happens, the link will probably be established, and the interface will be in an up/up state, but it will perform very poorly.

References

5.2.3 Switch Configuration Facts

resources\text\t_swi_cfg_ccna7\q_swi_cfg_01_ccna7.question.xml

Question 2 ✓ Correct

You are the only network administrator for your company. You are planning for an upcoming vacation, and you need to ensure that you can administer your switches remotely while you are gone. What must you configure to allow remote administration? (Select two.)

- □ The management VLAN name must match the local workgroup name.
- □ Use VNC on port 5900 to remotely access the switch.
- → ☑ The switch must be configured with a valid IP address and default gateway.
- □ CDP must be enabled on the switch so that other devices on the network can locate it.
- → ☑ Use Telnet, Secure Shell, or Web protocols to remotely access the switch.

Explanation

For the switch to communicate with remote workstations, the switch must have a valid IP address and default gateway. You can connect to a Cisco device directly with a console cable or remotely using applications like Telnet or Secure Shell.

References

5.2.3 Switch Configuration Facts

resources\text\t_swi_cfg_ccna7\q_swi_cfg_02_ccna7.question.xml

Question 3 ✓ Correct

During the initial setup of a new switch, which of the following configuration tasks should be performed? (Select three.)

→ ☑ Set the default gateway for remote management.

→ ☑ Set an IP address for remote management.

□ Configure trunking.

□ Configure the Spanning Tree Protocol.

→ ☑ Set passwords for the console, virtual terminal (TTY) ,and enable mode.

□ Attach a rollover console cable and set VTP mode to server.

□ Set duplex to full for remote access ports.

Explanation

After you plug in a switch, you should always configure the following:

- Passwords (console, virtual terminal, or VTY, and enable mode)
- IP addresses
- Default gateway

Other configurations are optional depending on the purpose of the device.

References

5.2.3 Switch Configuration Facts

resources\text\t_swi_cfg_ccna7\q_swi_cfg_03_ccna7.question.xml

Question 4. ✓ Correct

The FastEthernet 0/0 interface on a switch is currently disabled. You need to enable it so a workstation can be connected to it.

Drag each command on the left to the associated configuration step on the right to accomplish this task. Not all of the commands will be used.

Enter global configuration mode.

✓ **config terminal**

Enter interface configuration mode.

✓ **interface fa0/0**

Enable the interface.

✓ **no shutdown**

Verify the interface is up.

✓ **show interface status**

Explanation

To complete the requirements of this scenario, you need to use the following commands:

- Enter global configuration mode: **config terminal**
- Enter interface configuration mode: **interface fa0/0**
- Enable the interface: **no shutdown**
- Verify the interface status: **show interface status**

References

5.2.4 Switch Configuration Mode Facts

resources\text\t_swi_mode_ccna7\q_swi_mode_01_ccna7.question.xml

Question 5

✓ Correct

The following graphic illustrates some of the configuration modes of the switch.

What is one difference between the VLAN interface configuration and config-vlan?

○ VLAN interface configuration mode is used to perform all VLAN configuration tasks.

○ Config-vlan mode is used to configure all management functions and is a logical management interface.

→ ○ VLAN interface configuration mode is used to configure the switch IP address.

○ Config-vlan mode is used to configure all physical interfaces.

Explanation

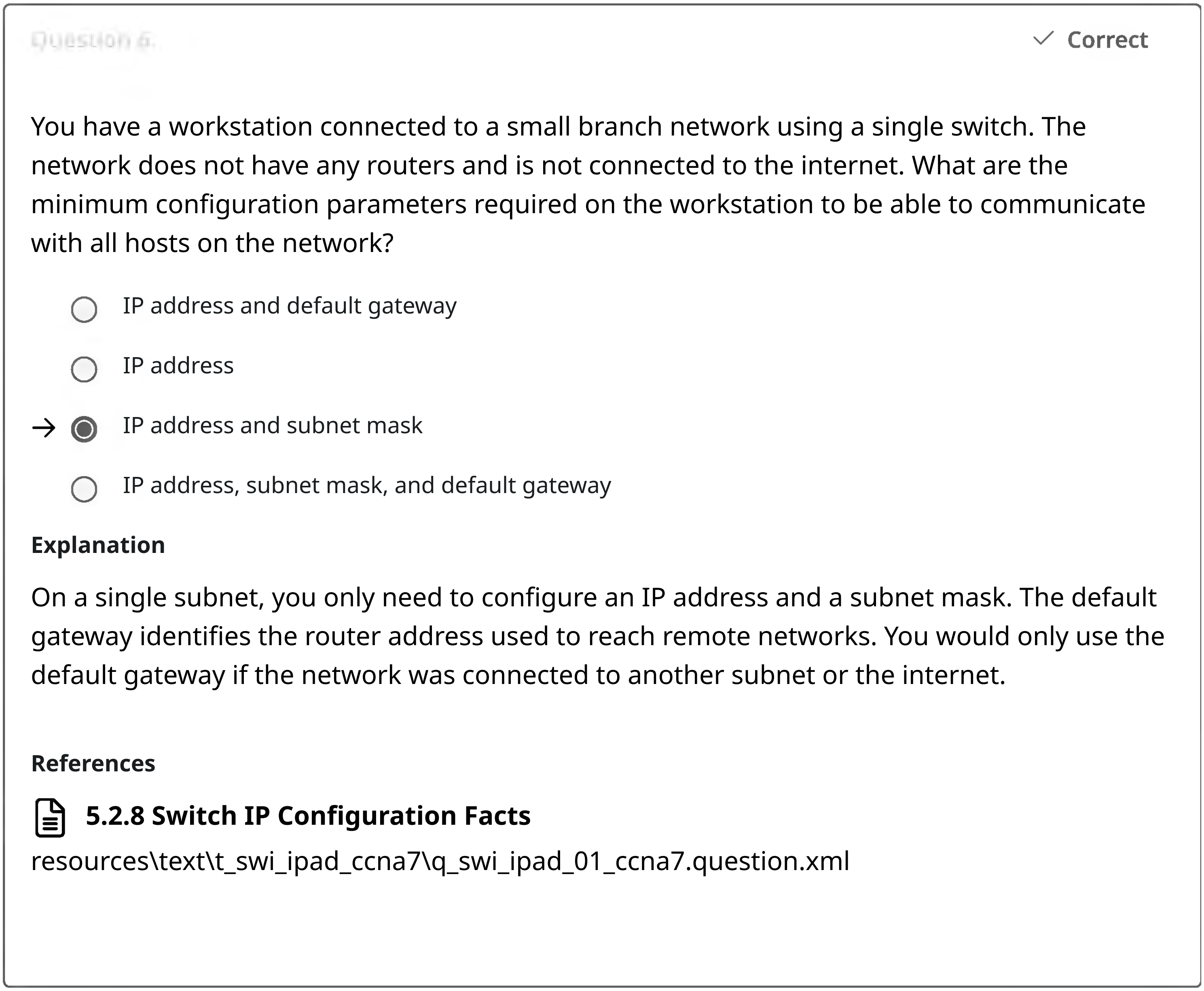
The VLAN interface configuration mode is used to configure the switch IP address and other management functions. It is a logical management interface configuration mode instead of a physical interface configuration mode, as is used for the FastEthernet and GigabitEthernet ports.

Do not confuse the config-vlan mode with the VLAN interface configuration mode.

References

5.2.4 Switch Configuration Mode Facts

resources\text\t_swi_mode_ccna7\q_swi_mode_02_ccna7.question.xml



Question 6. ✓ Correct

You have a workstation connected to a small branch network using a single switch. The network does not have any routers and is not connected to the internet. What are the minimum configuration parameters required on the workstation to be able to communicate with all hosts on the network?

- ○ IP address and default gateway
- ○ IP address
- → ● IP address and subnet mask
- ○ IP address, subnet mask, and default gateway

Explanation

On a single subnet, you only need to configure an IP address and a subnet mask. The default gateway identifies the router address used to reach remote networks. You would only use the default gateway if the network was connected to another subnet or the internet.

References

5.2.8 Switch IP Configuration Facts

resources\text\t_swi_ipad_ccna7\q_swi_ipad_01_ccna7.question.xml

Question [illegible]

✓ Correct

You have a small network connected to the internet as shown. You need to configure the default gateway address on Wrk1 so that it can communicate with hosts on the internet.

Which address would you use for the default gateway address?

○ The IP address assigned to Fa0/1 on Router2.

○ The IP address assigned to SwitchA.

→ ● The IP address assigned to Fa0/0 on Router1.

○ The IP address assigned to Fa0/1 on Router1.

○ The IP address assigned to Fa0/0 on Router2.

Explanation

When assigning the default gateway address, use the address of the router interface connected to the same network that is used to reach remote networks. In this scenario, the workstation must be configured with the IP address assigned to the Fa0/0 interface on Router1. This default gateway configuration allows the workstation to communicate with hosts on the other internal subnet as well as with hosts on the network.

The IP address assigned to the switch is only used for remote management of the switch. Packets sent to remote networks are not processed by the switch, but the frames are simply forwarded to the correct destination device. The Fa0/1 interface on Router1 is not on the same network as Wrk1, so it cannot be used as its default gateway address. The Fa0/0 interface on Router2 would be the default gateway address for hosts connected to SwitchB.

References

5.2.8 Switch IP Configuration Facts

resources\text\t_swi_ipad_ccna7\q_swi_ipad_02_ccna7.question.xml

✓ Correct

You have a small network with a single subnet connected to the internet as shown in the Exhibit. The router has been assigned the two addresses shown.

You need to manually configure the workstation to connect to the network. The workstation should use RouterA as the default gateway, and DNS1 as the DNS server address.

From the drop-down lists, select the appropriate parameters to configure the workstation's TCP/IP settings.

IP Address

192.168.12.46 ✓

Subnet Mask

255.255.255.240 ✓

Default Gateway

192.168.12.34 ✓

DNS Server

198.162.1.22 ✓

Explanation

Use the following values:

- Use 192.168.12.46 for the IP address. With a 28-bit mask, the router is on subnet 192.168.12.32, and valid addresses are 192.168.12.33 to 192.168.12.46. You cannot use 192.168.12.32 because that is the subnet address. You cannot use 192.168.12.47 because that is the broadcast address.
- A 28-bit mask is 255.255.255.240 in binary.
- For the default gateway address, use the address assigned to the router interface that is on the same subnet as the workstation (in this example, 192.168.12.34).
- For the DNS server address, use the IP address assigned to the DNS server (198.162.1.22).

References

5.2.8 Switch IP Configuration Facts

resources\text\t_swi_ipad_ccna7\q_swi_ipad_03_ccna7.question.xml

Question 9. ✓ Correct

Which command(s) would you use to configure a default-gateway on a Catalyst 2950XL switch?

→ ● **Switch(config)#ip default-gateway 192.168.10.1**

○ **Switch(config)#interface fa0/1**
Switch(config-if)ip default-gateway 192.168.10.1 255.255.255.0

○ **Switch(config)#ip default-gateway 192.168.10.1 255.255.255.0**

○ **Switch(config)#interface fa0/1**
Switch(config-if)#ip default-gateway 192.168.10.1

Explanation

The **default-gateway** command requires that you be in global configuration mode. Only the IP address is defined, not the subnet mask.

References

5.2.8 Switch IP Configuration Facts

resources\text\t_swi_ipad_ccna7\q_swi_ipad_04_ccna7.question.xml

Question 10. ✓ Correct

You must configure an IP address on a Catalyst 2950XL switch using the default management switch port. From global configuration mode, which commands would you enter to configure the correct management port?

○ **int fa0/1**
ip address 192.168.10.2 255.255.255.0

○ **int vlan 2**
ip address 192.168.10.2 255.255.255.0

○ **int fa0/3**
ip address 192.168.10.2 255.255.255.0

→ ● **int vlan 1**
ip address 192.168.10.2 255.255.255.0

Explanation

The default management switch port on a Catalyst 2950XL switch is VLAN1. The IP address must be assigned to VLAN1.

The management IP address cannot be assigned to an interface. The IP address identifies the entire switch, not a specific switch port.

References

5.2.8 Switch IP Configuration Facts
resources\text\t_swi_ipad_ccna7\q_swi_ipad_05_ccna7.question.xml