
Question: 1

[Cisco Equipment and Related Hardware]

What is the primary role of a switch in a local area network?

- A. to route data packets between different networks
- B. to encrypt data transmissions for security
- C. to divide the network into separate collision domains
- D. to provide wireless connectivity to LAN devices

Answer: C

Explanation:

In a local area network (LAN), the primary function of a switch is to operate at Layer 2 (Data Link Layer) of the OSI model. Switches use MAC addresses to forward frames to the appropriate destination ports. This targeted forwarding mechanism divides the network into separate collision domains for each switch port. By isolating collision domains, switches significantly reduce the chance of collisions, enhancing the performance and efficiency of the network.

Unlike hubs, which forward all traffic to all ports (thus creating a single collision domain), switches intelligently forward only the necessary traffic to the correct port. This capability allows multiple simultaneous conversations on different switch ports without interference.

Routers, which operate at Layer 3 (Network Layer), are used to route packets between different networks, not within the same LAN. Wireless connectivity is provided by wireless access points (WAPs), not switches. Encryption is typically handled by security protocols or devices such as firewalls and not by switches directly.

Reference: Supporting Cisco Devices for Field Technicians (FLDTEC) – Cisco Equipment and Related Hardware

Question: 2

[Cisco Equipment and Related Hardware]

Which Layer 2 technology extends to access layer devices, allowing individual switch ports to be

assigned for network and traffic management in an enterprise network?

- A. BGP
- B. VLANs
- C. OSPF
- D. MPLS

Answer: B

Explanation:

In an enterprise network, Virtual Local Area Networks (VLANs) are the key Layer 2 technology used to logically segment a network into multiple broadcast domains. VLANs allow network administrators to assign individual switch ports to specific VLANs, enabling effective network segmentation and traffic management.

This configuration extends to access layer devices, such as switches where end-user devices connect. By isolating traffic into VLANs, administrators can improve network performance, enhance security by separating sensitive departments (such as finance and HR), and simplify network management. Unlike routing protocols such as BGP and OSPF, which operate at Layer 3, or MPLS, which is a Layer 2.5 forwarding technology used primarily in service provider networks, VLANs are explicitly designed for Layer 2 segmentation within LAN environments.

Reference: Supporting Cisco Devices for Field Technicians (FLDTEC) – Cisco Equipment and Related Hardware

Question: 3

DRAG DROP

[Device Configuration and Verification]

Drag and drop the network connectivity and management tools used to ensure connectivity from the left onto the description on the right.

SSH	sends ICMP echo request packets to verify connectivity
Telnet	allows virtual terminal connections with unencrypted traffic
PING	provides secure, encrypted remote access to network devices
IP address configuration	requires the PC and Cisco device to be in the same subnet for direct connection

Answer:

PING → Sends ICMP echo request packets to verify connectivity

Telnet → Allows virtual terminal connections with unencrypted traffic

SSH → Provides secure, encrypted remote access to network devices

IP address configuration → Requires the PC and Cisco device to be in the same subnet for direct connection

These tools and their functions are covered under “Device Configuration and Verification” in the FLDTEC course:

PING: Utilized to test basic network connectivity using ICMP echo request/reply messages. It confirms whether a device is reachable and measures the round-trip time.

Telnet: A protocol that allows for remote device access but transmits data in plaintext, which makes it insecure. It's typically disabled by default on modern Cisco devices due to security concerns.

SSH (Secure Shell): Replaces Telnet as the preferred method for secure CLI access. It encrypts the session, protecting sensitive information such as login credentials.

IP Address Configuration: For direct device access via the same local network, both the PC and the Cisco device must be in the same subnet. This allows the use of tools like browser-based GUIs or terminal emulators when connecting directly.

Question: 4

[Troubleshooting Methodologies]

Which scenario would result in a speed mismatch when configuring Ethernet devices with different speed settings?

- A. One end is manually set to 1 Gbps, and the other end is manually set to 100 Mbps
- B. Both ends are manually set to the same speed
- C. One end is manually set to 100 Mbps, and the other end is set to auto-negotiation

D. Both ends are set to auto-negotiation and fail, reverting to their lowest speeds

Answer: A

Explanation:

A speed mismatch occurs when two connected Ethernet devices are configured to operate at different speeds. In scenario A, one device is manually set to 1 Gbps, while the other is set to 100 Mbps. Since both ends are hard-coded to different speeds, they cannot successfully negotiate a common speed, leading to a mismatch and resulting in a failed or unstable link.

In contrast, scenario B, where both ends are manually set to the same speed, ensures compatibility and stable communication. Scenario C can lead to a duplex mismatch rather than a speed mismatch; the auto-negotiating end may default to half-duplex if it cannot determine the duplex setting of the manually configured end. Scenario D is less common; if auto-negotiation fails, devices may revert to their lowest common speed, but this typically results in reduced performance rather than a complete mismatch.

Reference: Supporting Cisco Devices for Field Technicians (FLDTEC) – Troubleshooting Methodologies
=====

Question: 5

[Cisco IOS Software Basics]

Which layer of the OSI model provides error detection and defines how access to the media is controlled?

- A. Presentation layer
- B. Physical layer
- C. Network layer
- D. Data link layer

Answer: D

Explanation:

The Data Link Layer (Layer 2) of the OSI model is responsible for node-to-node data transfer and plays a crucial role in error detection and media access control. It ensures that data frames are transmitted to the correct device on a local network segment.

This layer is divided into two sublayers:

Logical Link Control (LLC): Manages frame synchronization, flow control, and error checking.

Media Access Control (MAC): Controls how devices on the network gain access to the medium and permission to transmit data.

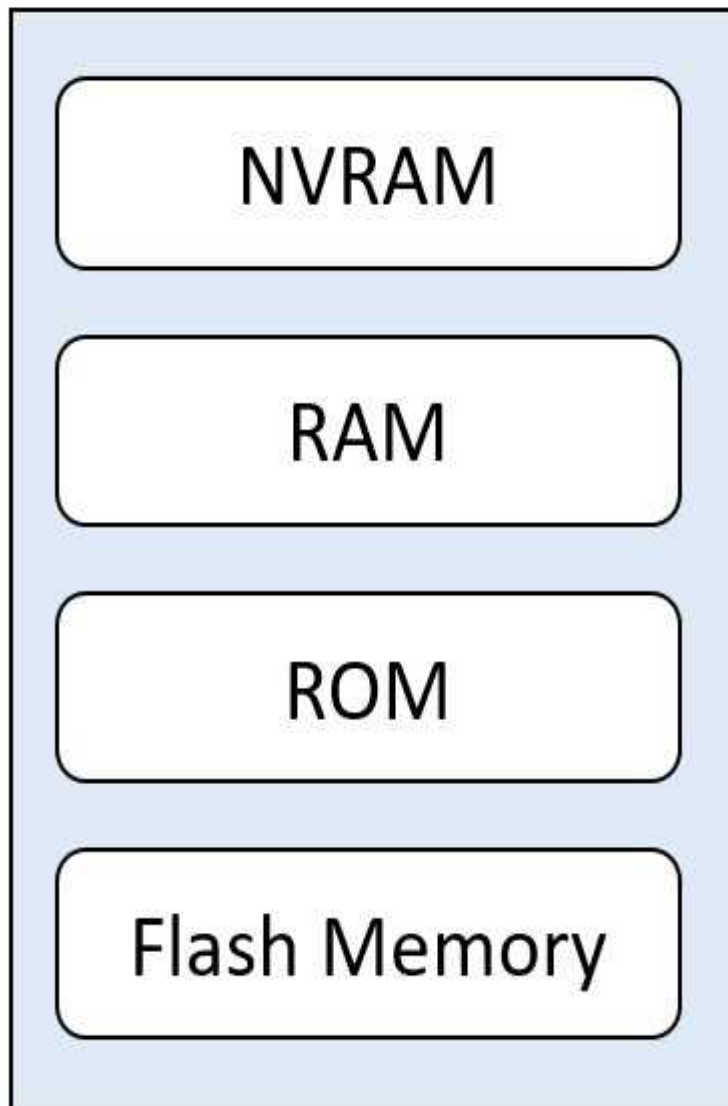
Together, these sublayers ensure reliable data transmission by detecting and possibly correcting errors that may occur in the Physical Layer. They also manage how devices share the transmission medium, preventing collisions and ensuring orderly communication.

Reference: Supporting Cisco Devices for Field Technicians (FLDTEC) – Cisco IOS Software Basics

Question: 6

DRAG DROP

[Cisco Equipment and Related Hardware]



Refer to the exhibit. Drag and drop the functions from the left onto the corresponding internal memory components on the right.

bootstrap code, post code, ROM monitor	NVRAM
startup configuration	RAM
running configuration	ROM
Cisco IOS software, backup configuration	flash memory

Answer:

Explanation:

bootstrap code, post code, ROM monitor	startup configuration
startup configuration	running configuration
running configuration	bootstrap code, post code, ROM monitor
Cisco IOS software, backup configuration	Cisco IOS software, backup configuration

NVRAM → Startup configuration

RAM → Running configuration

ROM → Bootstrap code, POST code, ROM monitor

Flash memory → Cisco IOS software, backup configuration

Each memory type in a Cisco device serves a specific function in the boot process and runtime operation. NVRAM retains configuration across reboots, RAM is volatile and holds active configs, ROM handles initial boot tasks, and flash stores the operating system.

This content is covered thoroughly in "Cisco Equipment and Related Hardware" in the FLDTEC curriculum. Here's the breakdown:

ROM (Read-Only Memory)

Stores bootstrap code, POST (Power-On Self-Test), and ROM Monitor.

These are essential for the device's initial power-on operations and recovery modes.

NVRAM (Non-Volatile RAM)

Holds the startup configuration file, which is loaded during the boot process.

Content remains intact after a reboot or power cycle.

RAM (Random Access Memory)

Stores the running configuration and current operational state of the router or switch.

Also used for routing tables, ARP cache, and packet buffers.

Data is lost when the device is powered off or rebooted.

Flash Memory

Contains the Cisco IOS image, system files, and can store backup configurations.

It is a non-volatile storage, so it retains data after reboots.

Question: 7

[Cisco Equipment and Related Hardware]

Which two devices are most commonly used in a WAN environment? (Choose two.)

- A. Hubs
- B. Optical fiber converters
- C. Modems
- D. Network interface cards
- E. Wireless access points

Answer: BC

Explanation:

In the context of Wide Area Networks (WANs), the key objective is to connect geographically separated networks using service provider infrastructure. The FLDTEC course emphasizes that WAN environments typically involve devices that can handle different physical transmission mediums and protocols.

Modems:

Modulate and demodulate analog signals to digital signals.

Used in WAN environments to connect over analog lines like DSL or leased lines.

Essential for interfacing between digital routers and analog telephone networks.

Optical Fiber Converters:

Also known as media converters, they are used to convert electrical signals to optical signals (and vice versa) for fiber transmission.

Common in WAN scenarios where long-distance high-speed transmission over fiber is required.

Incorrect Options:

A . Hubs: Obsolete Layer 1 devices used in LANs, not suitable for WANs.

D . Network Interface Cards (NICs): Used in end devices for LAN connectivity.

E . Wireless Access Points: Typically used in WLANs within local premises, not WAN infrastructure.

This aligns with Cisco's WAN architecture fundamentals as highlighted in FLDTEC under "Cisco Equipment and Related Hardware."

Question: 8

[Cisco IOS Software Basics]

What is the purpose of a subnet mask?

- A. Distinguishes the network and host segments
- B. Provides encryption for network traffic
- C. Determines the next-hop router
- D. Aids in route prioritization

Answer: A

Explanation:

A subnet mask is a 32-bit number used in IP networking to divide an IP address into network and host portions. This division is crucial for routing traffic within and between networks. The subnet mask works in tandem with the IP address to identify which part of the address refers to the network and which part refers to the host. This distinction allows for efficient IP address allocation and routing.

For example, in the IP address 192.168.1.10 with a subnet mask of 255.255.255.0, the first three octets (192.168.1) represent the network portion, while the last octet (10) identifies the specific host within that network.

Reference: Supporting Cisco Devices for Field Technicians (FLDTEC) – Cisco IOS Software Basics

Question: 9

DRAG DROP

[Device Configuration and Verification]

Drag and drop the descriptions from the left onto the corresponding IPv4 addressing modes on the right.

address used for testing and troubleshooting on the local device	unicast
address used for one-to-everyone communication on the subnet	broadcast
address that identifies the unique node on the network	multicast
address used for single packet of one-to-many delivery	loopback

Answer:

Explanation:

address used for testing and troubleshooting on the local device	address that identifies the unique node on the network
address used for one-to-everyone communication on the subnet	address used for one-to-everyone communication on the subnet
address that identifies the unique node on the network	address used for single packet of one-to-many delivery
address used for single packet of one-to-many delivery	address used for testing and troubleshooting on the local device

This content is aligned with IPv4 Addressing Fundamentals, detailed in the FLDTEC course under Device Configuration and Verification:

Unicast: A unicast address uniquely identifies a single host on a network. This is the most common address type used for standard communication between two devices.

Broadcast: Broadcast addresses (e.g., 255.255.255.255 or subnet-specific broadcast) send traffic to all hosts in the network segment. Used for ARP requests and DHCP discovery.

Multicast: Used to deliver a packet to a group of hosts interested in the data, without flooding the network like a broadcast. Multicast uses addresses from the range 224.0.0.0 to 239.255.255.255.

Loopback: The loopback address (127.0.0.1) is reserved for local testing, ensuring that the TCP/IP stack is working properly without needing to access the network.