TESTPASSPORT

練 習 問 題



高 品 質 な 学 習 リ ソ ー ス

https://www.testpassport.jp

1年間無料アップデート

Exam : **800-150**

Title : Supporting Cisco Devices for Field Technicians (FLDTEC)

Version : DEMO

1.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

2.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

3.DRAG DROP

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:

SSH	PING
Telnet	Telnet
PING	SSH
IP address configuration	IP address configuration

Explanation:

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.

4.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

5.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