

CERTPARK



QUESTION & ANSWER



CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



<https://www.certpark.com>

Exam : **100-490**

Title : Supporting Cisco Routing
and Switching Network
Devices v3.0

Version : DEMO

1.Which protocol does TFTP typically use for transport?

- A. RSVP
- B. TCP
- C. HTTP
- D. UDP

Answer: D

Explanation:

TFTP, or Trivial File Transfer Protocol, is a simple protocol used for transferring files. Unlike other file transfer protocols, TFTP operates on top of the User Datagram Protocol (UDP), which is a connectionless protocol. This means that TFTP does not establish a persistent connection between the client and server, and it does not guarantee reliable delivery of packets, error checking, or correction. TFTP is typically used in scenarios where simplicity and minimal memory footprint are more critical than the need for reliable delivery, such as when booting a device over a network¹²³.

Reference: = Wikipedia, GeeksforGeeks, PyNet Labs

2.What is the correct IPv6 address notation?

- A. 2001:0DB8::/128
- B. 2001:0DB8:0::
- C. 2001:0DB8::1:1:1:1:1
- D. 2001:0DB8:130F:0000:0000:7000:0000:140B

Answer: D

Explanation:

The correct IPv6 address notation follows the format of eight groups of four hexadecimal digits, separated by colons. The address must have exactly eight groups unless it uses the double colon (::) to represent consecutive groups of zero value. The double colon can only appear once in an address to avoid ambiguity.

Option A is incorrect because it includes a subnet mask (/128) which is not part of the actual address notation. Option B is incomplete as it does not contain enough groups and ends with a single colon. Option C has too many groups (nine instead of eight) and is therefore not a valid IPv6 address. Option D is the correct notation with eight groups of four hexadecimal digits, where necessary leading zeros are included.

Reference: = IPv6 Address Types, Notation, and Structure Explained¹. IPv6 address formats - IBM².

3.Which two statements about Telnet and SSH are true? (Choose two.)

- A. SSH is a protocol that provides a secure remote access connection to network devices.
- B. SSH uses the well-known TCP port 23 for its communication.
- C. A Telnet network management connection is dropped when a router reboots.
- D. Telnet is a protocol that provides a secure remote access connection to network devices.
- E. Telnet is preferred over SSH for security reasons.

Answer: AC

Explanation:

A. Correct. SSH, or Secure Shell, is indeed a protocol that provides a secure remote access connection to network devices. It encrypts the data to ensure secure transmission over insecure networks like the internet¹.

C. Correct. Telnet connections are not secure and are terminated when a router reboots. This is because Telnet does not have any mechanism to maintain the connection in case of network interruptions or device reboots¹.

B, D, and E are incorrect because:

B. SSH uses TCP port 22 by default, not port 23, which is used by Telnet¹. D. Telnet does not provide a secure connection; it transmits data in plain text, which can be intercepted easily¹.

E. SSH is preferred over Telnet for security reasons because it provides encrypted connections and authentication mechanisms, which Telnet does not¹.

Reference: = 1: GeeksforGeeks - Difference between SSH and Telnet 2: phoenixNAP - Telnet vs. SSH: How Is SSH Different From Telnet? 3: Guru99 - Telnet vs SSH – Difference Between Them 4: Difference Between - Difference Between Telnet and SSH

4. Which address facilitates the routing of packets over an IP network?

- A. physical
- B. transport
- C. network
- D. MAC

Answer: C

Explanation:

The address that facilitates the routing of packets over an IP network is the network address. In the context of IP networking, this refers to the IP address, which is used to identify each host on a network and to determine the best path for data packets to travel from their source to their destination. Routers use IP addresses to make decisions about where to forward packets so that they reach the correct destination. The network layer of the OSI model, where IP operates, is responsible for this routing process¹²³.

The other options listed do not facilitate routing in the same way:

Physical (A) and MAC (D) addresses are used at the data link layer to deliver packets on the same local network.

Transport (B) refers to the transport layer, which is responsible for end-to-end communication and data flow control but does not route packets over an IP network.

5. Which two IPv4 addresses can be assigned to a host computer? (Choose two.)

- A. 255.255.255.255
- B. 10.1.1.20
- C. 0.0.0.0
- D. 192.168.10.15
- E. 292.10.3.4

Answer: BD

Explanation:

IPv4 addresses consist of four octets, each ranging from 0 to 255. The addresses are used to uniquely identify devices on a network.

A. 255.255.255.255 is reserved for broadcast messages to all hosts on the local network, so it cannot be assigned to a single host.

B. 10.1.1.20 falls within the range of private IP addresses (10.0.0.0 to 10.255.255.255) and can be

assigned to a host within a private network.

C. 0.0.0.0 is used to denote an unknown or non-applicable target address, often used as a default route, and cannot be assigned to a host.

D. 192.168.10.15 is also within the range of private IP addresses (192.168.0.0 to 192.168.255.255) and can be assigned to a host within a private network.

E. 292.10.3.4 is not a valid IPv4 address because the first octet exceeds the maximum value of 255.

Reference: =

IPv4 Addressing

Valid IP Address

IP Address Validation