Free Questions for SSCP

Shared by Ryan on 03-03-2025

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What ISO/OSI layer do switches primarily operate at?

Do take note that this question makes reference to a plain vanilla switch and not one of the smart switches that is available on the market today.

Options:

A- Physical layer

B- Network layer

C- Data link layer

D- Session layer

Answer:

C

Explanation:

Switches primarily operate at the data link layer (layer 2), although intelligent, extremely fast Layer 3 switching techniques are being more frequently used.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 111).

Question 2

Question Type: MultipleChoice

Which xDSL flavour, appropriate for home or small offices, delivers more bandwidth downstream than upstream and over longer distance?

Options:

A- VDSL

B- SDSL

C- ADSL
D- HDSL

Answer:

C

Explanation:

Asymmetric digital subscriber line (ADSL) is designed to provide more bandwidth downstream (1 to 8 Mbps) than upstream (16 to 800Kb).

DSL (Digital Subscriber Line) is a modem technology for broadband data access over ordinary copper telephone lines (POTS) from homes and businesses. xDSL refers collectively to all types of DSL, such as ADSL (and G.Lite), HDSL, SDSL, IDSL and VDSL etc. They are sometimes referred to as last-mile (or first mile) technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.

xDSL is similar to ISDN in as much as both operate over existing copper telephone lines (POTS) using sophisticated modulation schemes and both require the short runs to a central telephone office

Graphic below from: http://computer.howstuffworks.com/vdsl3.htm

DSL Type	Max. Send Speed	Max. Receive Speed	Max. Distance	Lines Required	Phone Support
ADSL	800 Kbps	8 Mbps	18,000 ft (5,500 m)	1	Yes
HDSL	1.54 Mbps	1.54 Mbps	12,000 ft (3,650 m)	2	No
IDSL	144 Kbps	144 Kbps	35,000 ft (10,700 m)	1	No
MSDSL	2 Mbps	2 Mbps	29,000 ft (8,800 m)	1	No
RADSL	1 Mbps	7 Mbps	18,000 ft (5,500 m)	1	Yes
SDSL	2.3 Mbps	2.3 Mbps	22,000 ft (6,700 m)	1	No
VDSL	16 Mbps	52 Mbps	4,000 ft (1,200 m)	1	Yes

DSL speed chart

The following are incorrect answers:

Single-line Digital Subscriber Line (SDSL) deliver 2.3 Mbps of bandwidth each way.

High-rate Digital Subscriber Line (HDSL) deliver 1.544 Mbps of bandwidth each way.

Very-high data-rate Digital Subscriber Line (VDSL) can deliver up to 52 Mbps downstream over a

single copper twisted pair over a relatively short distance (1000 to 4500 feet).
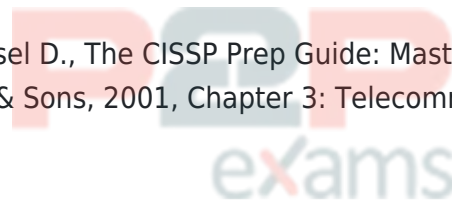
Reference used for this

question;

http ://computer.howstuffworks.com/vdsl3.htm

and

http://www.javvin.com/protocolxDSL.html

and

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 115).

Question 3

Question Type: MultipleChoice

Which of the following technologies has been developed to support TCP/IP networking over low-speed serial interfaces?

Options:

A- ISDN

B- SLIP

C- xDSL

D- T1

Answer:

B

Explanation:

Serial Line IP (SLIP) was developed in 1984 to support TCP/IP networking over low-speed serial interfaces.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network

Security (page 114).

Question 4

Question Type: MultipleChoice

Which of the following IEEE standards defines the token ring media access method?

Options:

A- 802.3

B- 802.11

C- 802.5

D- 802.2

Answer:

D

Explanation:

The IEEE 802.5 standard defines the token ring media access method. 802.3 refers to Ethernet's CSMA/CD, 802.11 refers to wireless communications and 802.2 refers to the logical link control.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 109).

Question 5

Question Type: MultipleChoice

Which of the following standards is concerned with message handling?

Options:

A- X.400

B- X.500

C- X.509

D- X.800

X- 400 is used in e-mail as a message handling protocol. X.500 is used in directory services.
X.509 is used in digital certificates and X.800 is used a network security standard.

Answer:

A

Question 6

Question Type: MultipleChoice

Which of the following is an example of a connectionless communication protocol?

Options:

A- UDP

B- X.25

C- Packet switching

D- TCP

Answer:

A

Explanation:

UDP is an example of connectionless communication protocol, wherein no connection needs to be established before data can be exchanged.

In telecommunications, connectionless describes communication between two network end points in which a message can be sent from one end point to another without prior arrangement. The device at one end of the communication transmits data addressed to the other, without first ensuring that the recipient is available and ready to receive the data. Some protocols allow for error correction by requested retransmission. Internet Protocol (IP) and User Datagram Protocol (UDP) are connectionless protocols.

Connectionless protocols are also described as stateless because the endpoints have no protocol-defined way to remember where they are in a 'conversation' of message exchanges.

List of connectionless protocols

Hypertext Transfer Protocol

IP

UDP

ICMP

IPX

TIPC

NetBEUI

References:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 86).

and

https://secure.wikimedia.org/wikipedia/en/wiki/Connectionless_protocol

Question 7

Question Type: MultipleChoice

What is also known as 10Base5?

Options:

A- Thinnet

B- Thicknet

C- ARCnet

D- UTP

Answer:

B

Explanation:

Thicknet is a coaxial cable with segments of up to 500 meters, also known as 10Base5. Thinnet is

a coaxial cable with segments of up to 185 meters. Unshielded twisted pair (UTP) has three variations: 10 Mbps (10BaseT), 100 Mbps (100BaseT) or 1 Gbps (1000BaseT). ARCnet is a LAN media access method.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 108).

Question 8

Question Type: MultipleChoice

Which of the following LAN topologies offers the highest availability?

Options:

A- Bus topology

B- Tree topology

C- Full mesh topology

D- Partial mesh topology

Answer:

C

Explanation:

In a full mesh topology, all network nodes are individually connected with each other, providing the highest availability. A partial mesh topology can sometimes be used to offer some redundancy.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 106).

Question 9

Question Type: MultipleChoice

Which of the following is a LAN transmission method?

Options:

A- Broadcast

B- Carrier-sense multiple access with collision detection (CSMA/CD)

C- Token ring

D- Fiber Distributed Data Interface (FDDI)

Answer:

A

Explanation:

LAN transmission methods refer to the way packets are sent on the network and are either unicast, multicast or broadcast.

CSMA/CD is a common LAN media access method.

Token ring is a LAN Topology.

LAN transmission protocols are the rules for communicating between computers on a LAN.

Common LAN transmission protocols are: polling and token-passing.

A LAN topology defines the manner in which the network devices are organized to facilitate communications.

Common LAN topologies are: bus, ring, star or meshed.

LAN transmission methods refer to the way packets are sent on the network and are either unicast, multicast or broadcast.

LAN media access methods control the use of a network (physical and data link layers). They can be Ethernet, ARCnet, Token ring and FDDI.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 103).

HERE IS A NICE OVERVIEW FROM CISCO:

LAN Transmission Methods

LAN data transmissions fall into three classifications: unicast, multicast, and broadcast.

In each type of transmission, a single packet is sent to one or more nodes.

In a unicast transmission, a single packet is sent from the source to a destination on a network. First, the source node addresses the packet by using the address of the destination node. The package is then sent onto the network, and finally, the network passes the packet to its destination.

A multicast transmission consists of a single data packet that is copied and sent to a specific subset of nodes on the network. First, the source node addresses the packet by using a multicast address. The packet is then sent into the network, which makes copies of the packet and sends a copy to each node that is part of the multicast address.

A broadcast transmission consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address. The packet is then sent on to the network, which makes copies of the packet and sends a copy to every node on the network.

LAN Topologies

LAN topologies define the manner in which network devices are organized. Four common LAN topologies exist: bus, ring, star, and tree. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies, for example, are commonly organized physically as a star. A bus topology is a linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations. Of the three

most widely used LAN implementations, Ethernet/IEEE 802.3 networks---including 100BaseT---implement a bus topology

Sources:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 104).

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introlan.htm

Question 10

Question Type: MultipleChoice

What is defined as the rules for communicating between computers on a Local Area Network (LAN)?

Options:

A- LAN Media Access methods
B- LAN topologies
C- LAN transmission methods
D- Contention Access Control

Answer:

A

Explanation:

Media contention occurs when two or more network devices have data to send at the same time. Because multiple devices cannot talk on the network simultaneously, some type of method must be used to allow one device access to the network media at a time.

This is done in two main ways: carrier sense multiple access collision detect (CSMA/CD) and token passing.

In networks using CSMA/CD technology such as Ethernet, network devices contend for the network media. When a device has data to send, it first listens to see if any other device is currently using the network. If not, it starts sending its data. After finishing its transmission, it listens again to see if a collision occurred. A collision occurs when two devices send data simultaneously. When a collision happens, each device waits a random length of time before resending its data. In most cases, a collision will not occur again between the two devices. Because of this type of network contention, the busier a network becomes, the more collisions occur. This is why performance of Ethernet degrades rapidly as the number of devices on a single network increases.

In token-passing networks such as Token Ring and FDDI, a special network frame called a token is passed around the network from device to device. When a device has data to send, it must wait until it has the token and then sends its data. When the data transmission is complete, the token is released so that other devices may use the network media. The main advantage of token-passing networks is that they are deterministic. In other words, it is easy to calculate the maximum time that will pass before a device has the opportunity to send data. This explains the popularity of token-passing networks in some real-time environments such as factories, where machinery must be capable of communicating at a determinable interval.

For CSMA/CD networks, switches segment the network into multiple collision domains. This reduces the number of devices per network segment that must contend for the media. By creating smaller collision domains, the performance of a network can be increased significantly without requiring addressing changes.

The following are incorrect answers:

LAN topologies: Think of a topology as a network's virtual shape or structure. This shape does not necessarily correspond to the actual physical layout of the devices on the network. For example, the computers on a home LAN may be arranged in a circle in a family room, but it would be highly unlikely to find a ring topology there. Common topologies are: bus, ring, star or meshed. See THIS LINK for more information.

LAN transmission methods: refer to the way packets are sent on the network and are either unicast, multicast or broadcast. See THIS LINK for more information.

Contention Access Control: This is a bogus detractor.

Contention is a real term but Contention Access Control is just made up. Contention methods is very closely related to Media Access Control methods. In communication networks, contention is a media access method that is used to share a broadcast medium. In contention, any computer in the network can transmit data at any time (first come-first served). This system breaks down when two computers attempt to transmit at the same time. This is a case of collision. To avoid collision, carrier sensing mechanism is used. Here each computer listens to the network before attempting to transmit. If the network is busy, it waits until network quiets down. In carrier detection, computers continue to listen to the network as they transmit. If computer detects another signal that interferes with the signal it is sending, it stops transmitting. Both computers then wait for random amount of time and attempt to transmit. Contention methods are most popular media access control method on LANs.

Reference(s) used for this question:

http:// docwiki.cisco.com/wiki/Introduction_to_LAN_Protocols#LAN_Media-Access_Methods

http:// docwiki.cisco.com/wiki/Introduction_to_LAN_Protocols#LAN_Media-Access_Methods

http://en.wikipedia.org/wiki/Contention_%28telecommunications%29

Question 11

Question Type: MultipleChoice

How would an IP spoofing attack be best classified?

Options:
A- Session hijacking attack

B- Passive attack

C- Fragmentation attack

D- Sniffing attack

Answer:

A

Explanation:

IP spoofing is used to convince a system that it is communicating with a known entity that gives an intruder access. IP spoofing attacks is a common session hijacking attack.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 77).

To Get Premium Files for SSCP Visit

https://www.p2pexams.com/products/sscp

For More Free Questions Visit

https://www.p2pexams.com/isc2/pdf/sscp