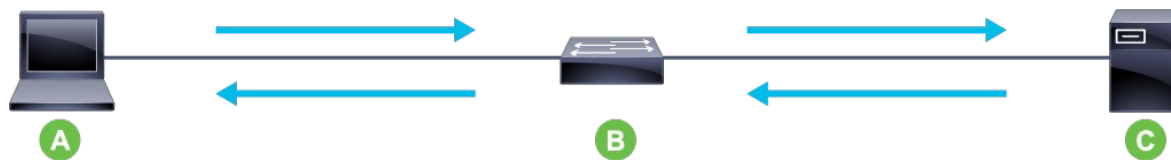


Test Questions I missed

When a router is calculating the network portion of an IPv4 address, which bitwise operation is performed on the IPv4 address and the subnet mask?

The correct answer is **AND**. In order to extract the network part of an IPv4 address, the ANDing logical operation is performed with the IPv4 address and the subnet mask as operands. When the binary digit 1 is ANDed with another digit, the value of the other digit is preserved. ANDing with 0 always results in a 0. Therefore, 1s in the subnet mask will preserve the value found in the IPv4 address. The logical operations NAND, OR, and XOR would not preserve the values found in the IPv4 address.

The correct answers are **RADIUS combines authentication and authorization, while TACACS+ implements two separate processes** and **RADIUS is a UDP based protocol. TACACS+ is a TCP based protocol.** RADIUS is an open standard that combines authentication and authorization services into a single process. TACACS+ is a Cisco proprietary security mechanism that can be used only for authorization and accounting while using another method of authentication. TACACS+ uses the Transmission Control Protocol (TCP) for all three services



The correct answer is **A: supplicant, B: authenticator, C: authentication server.**

supplicant is a workstation with 802.1X-compliant client software.

authenticator acts as a proxy between the supplicant and an authentication server.

authentication server authenticates supplicants connecting to a switch port.

Which three SNMP messages are sent from an SNMP agent to an SNMP manager?

The correct answers are **InformRequest**, **Response**, and **Trap**. GetRequest, GetNextRequest and SetRequest are SNMP messages that an SNMP manager sends to an SNMP agent.

A company needs to implement a secure VPN solution using IPsec. Which protocol and encryption algorithm should be used to guarantee VPN confidentiality?.

The correct answer is **ESP protocol with the 3DES encryption algorithm**. Of the two IPsec tunnel protocols, only the Encapsulating Security Payload (ESP) supports confidentiality. 3DES and AES are symmetric encryption algorithms, and both can be used in IPsec VPNs.

SHA-2 is a hash function

RSA is a public-key cryptosystem

Diffie-Hellman is a key exchange algorithm.

Options were

AH protocol with the AES encryption algorithms

AH protocol with the SHA-2 encryption algorithm

ESP protocol with the 3DES encryption algorithm

ESP protocol with the Diffie-Hellman Group 7 encryption algorithm

both ESP and AH protocols with the RSA encryption algorithm

When the store-and-forward switching method is in use, which part of the Ethernet frame is used to perform error checking using cyclic redundancy check (CRC)?

The correct answer is **All frame fields, except the FCS field in the trailer**. A cyclic redundancy check is used to generate a CRC value for the FCS field. The **FCS field value is computed as a function of the contents** of the *destination address, source address, type, and data and padding fields* of the Ethernet frame, **in other words, on all Ethernet frame fields except the FCS field**.

What are two field names corresponding to the IPv4 header field and the IPv6 header field that contain Differentiated Services Code Point (DSCP) markings? (Choose two.)

The correct answers are **traffic class** and **type of service (ToS)**.

In the original RFC definitions of the ToS field, IP precedence was a 3-bit sub-field. The initial definition of the ToS field has been changed to include the flow control field. The offset field is the IPv4 header field used when packets are fragmented. The flow label IPv6 header field can be used to label a set of packets belonging to the same flow and does not contain DSCP markings.