CCNA 640-802 Bible - Describe the Purpose and Types of ACLs

1. What are the general recommendations regarding the placement of access control lists? (Choose two) A. Standard ACLs should be placed as close as possible to the source of traffic to be denied. B. Extended ACLs should be placed as close as possible to the source of traffic to be denied . C. Standard ACLs should be placed as close as possible to the destination of traffic to be denied . D. Extended ACLs should be placed as close as possible to the destination of traffic to be denied . Answer: B, C Explanation: **Standard Access Lists:** Access-list list# {permit/deny} source IP [wildcard mask] interface [router port] ip access-group [list#] in|out (out is the default) If a match is made, the action defined in this access list statement is performed. If no match is made with an entry in the access list, the deny action is performed (implicit deny) Should be put close to the destination address because you can not specify the destination address, only the source information is looked at. **Extended Access List:** Access-list list# {permit/deny} protocol source [source mask] destination [destination mask] operator [port] Should be put close to the source Since extended ACLs have destination information, you want to place it as close to the source as possible. Place an extended ACL on the first router interface the packet enters and specify inbound in the access-group command. 2. What three pieces of information can be used in an extended access list to filter traffic? (Choose three.) A:protocol B:VLAN number C:TCP or UDP port numbers D:source switch port number E:source IP address and destination IP address F:source MAC address and destination MAC address **Correct Answers: A, C, E** 3. What are two reasons that a network administrator would use access lists? (Choose two.) A:to control vty access into a router B:to control broadcast traffic through a router C:to filter traffic as it passes through a router D:to filter traffic that originates from the router E:to replace passwords as a line of defense against security incursions **Correct Answers: A, C** Explanation: Access lists are used to process data received by a router can be divided into two broad categories: 1. traffic that passes through the router via the forwarding path (choice C) 2. traffic destined for the router via the receive path for route processor handling, such as ssh/telnet vty access (Choice A) In normal operations, the vast majority of traffic simply flows through a router en route to its ultimate destination. 4. When are packets processed by an inbound access list? A: before they are routed to an outbound interface B: after they are routed to an outbound interface C: before and after they are routed to an outbound interface D: after they are routed to an outbound interface but before being placed in the outbound queue **Correct Answers: A** Explanation: When a packet is received on an interface with an inbound access list configured, the packets are matched against the access list to determine if they should be permitted or denied. After this check, the packets are processed by the routing function. The access list check is always done first. **Incorrect Answers:** B, D. The packets are always processed by the inbound access list prior to being routed. C. All packets are always checked against a specific access list only once. While packets traversing through a router may be checked against different access lists for each interface and in each direction (inbound and outbound), each access list is always only consulted once.