CCNA Quick Notes ? Access Lists

1.Besides named access lists, what are the two types of IP access lists? The two types of IP access lists are standard and extended. What criteria do standard IP access lists use to filter packets? Standard IP access lists filter packets by the source address. This results in the packet's being permitted or denied for the entire protocol suite based on the source network IP address. 2.What criteria do extended IP access lists use to filter packets? Extended IP access lists filter packets by source address, destination address, protocols, and port numbers. 3.In what two ways can IP access lists be applied to an interface? Access lists can be applied as inbound or outbound access lists. Inbound access lists process packets as they enter a router's interface and before they are routed. Outbound access lists process packets as they exit a router's interface and after they are routed. 4.How many access lists can be applied to an interface on a Cisco router? Only one access list per protocol, per direction, per interface can be applied on a Cisco router. Multiple access lists are permitted per interface, but they must be for a different protocol. 5.How are access lists processed? Access lists are processed in sequential, logical order, evaluating packets from the top down, one statement at a time. As soon as a match is made, the permit or deny option is applied, and the packet is not applied to any more access list statements. Because of this, the order of the statements within any access list is significant. 6.What is at the end of each access list? At the end of each access list, an implicit deny statement denies any packet not filtered in the access list. 7.What are the number ranges used to define standard and extended IP access lists? The number ranges used to define standard and extended IP access lists are as follows: · Standard IP access lists 1 to 99 and 1300 to 1999· Extended IP access lists 100 to 199 and 2000 to 2699 8.When implementing access lists, what are wildcard masks? Wildcard masks define the subset of the 32 bits in the IP address that must be matched. Wildcards are used with access lists to specify a host, network, or part of a network. Wildcard masks work exactly the opposite of subnet masks. In subnet masks, 1 bits are matched to the network portion of the address, and 0s are wildcards that specify the host range. In wildcard masks, when 0s are present, the octet address must match. Mask bits with a binary value of 1 are wildcards. For example, if you have an IP address 172.16.0.0 with a wildcard mask of 0.0.255.255, the first two portions of the IP address must match 172.16, but the last two octets can be in the range 1 to 255. 9.What is the IOS command syntax used to create a standard IP access list? Here is the command syntax to create a standard IP access list: access-list access-list-number {permit deny} source-address [wildcard mask]access-list-number is a number from 1 to 99. For example: RouterA(config)#access-list 10 deny 192.168.0.0 0.0.0.255 10.After you create a standard or extended IP access list, how do you apply it to an interface on a Cisco router? To apply an access list to an interface on a Cisco router, use the ip access-group interface command: ip access-group access-list-number {in out}For example:RouterA(config)#int s0RouterA(config-if)#ip access-group 10 in Create a standard access list that permits the following networks: 192.168.200.0192.168.216.0192.168.232.0192.168.248.0 There are two ways to do this. First, you can create one access list that contains an entry for each network: access-list 10 permit 192.168.200.0 0.0.0.255access-list 10 permit 192.168.216.0 0.0.0.255access-list 10 permit 192.168.232.0 0.0.0.255access-list 10 permit 192.168.248.0 0.0.0.255 A second way to do this is to create a single entry with wildcard masks: access-list 10 permit 192.168.200.0 0.0.48.255 To see how this one statement denies all the networks, you must look at it in binary: .200= 11001000.216= 11011000.232= 11101000.248= 11111000 All the bits match except the third and fourth bits. With wildcard masks, these are the bits you want to match. Therefore, your wildcard mask would be 00110000 in binary, which is 48. 11.What is the Cisco IOS command syntax used to create an extended access list? Here is the Cisco IOS command syntax to create an extended access list: access-list access-list-number {permit deny} protocol source-address source-wildcard [operator port] destination-address destination-wildcard [operator port] protocol examples include IP, TCP, UDP, ICMP, GRE, and IGRP. operator port can be lt (less than), gt (greater than), eq (equal to), or neg (not equal to) and a protocol port number. Create an extended access list denying web traffic to network 192.168.10.0. The following commands deny web traffic to network 192.168.10.0: access-list 101 deny tcp any 192.168.10.0 0.0.0.255 eq wwwaccess-list 101 permit ip any any 12.What IOS command can you use to see whether an IP access list is applied to an interface? The IOS command to see whether an IP access list is applied to an interface is show ip interface interface-type interface-number For example: RouterA#show ip interface s0 Serial0 is up, line protocol is up Internet address is 192.168.1.2/24 Broadcast address is 255.255.255.255 Address determined by non-volatile memory MTU is 1500 bytes Helper address is not set Directed broadcast forwarding is enabled Multicast reserved groups joined: 224.0.0.9 Outgoing access list is not set Inbound access list is 10 Proxy ARP is enabled Security level is default Split horizon is enabled ICMP redirects are always sent ICMP unreachables are always sent ICMP mask replies are never sent IP fast switching is enabled IP fast switching on the same interface is enabled IP Feature Fast switching turbo vector IP multicast fast switching is disabled IP multicast distributed fast switching is disabled IP route-cache flags are Fast Router Discovery is disabled IP output packet accounting is disabled IP access violation accounting is disabled TCP/IP header compression is disabled RTP/IP

header compression is disabled Probe proxy name replies are disabled Policy routing is disabled Network address translation is disabled Web Cache Redirect is disabled BGP Policy Mapping is disabled 13.How can you display all access lists on a Cisco router? To display all access lists on a Cisco router, use the show access-list command: RouterA#show access-listStandard IP access list 10 deny 192.168.0.0, wildcard bits 0.0.0.255Extended IP access list 101 permit tcp any any eq www permit udp any any eq domain permit udp any eq domain any permit icmp any any deny tcp 192.168.10.0 0.0.0.255 any eq wwwRouterA# 14.How do you figure out wildcard questions? Identify the class192.68.12.0 - Class C24 bits for networks/29 tells us that we need an additional 5 bits29 - 24 = 5 bits5 bits = 128 + 64 + 32 + 16 + 8 = 248Default subnet mask for Class C network = 255.255.255.0New subnet mask for /29 network = 255.255.255.248To find the wildcard value:255.255.255.255 255.255.255.248 - ----------0.0.0.7 Same logic for Class B172.31.0.0 /1916 bits for networks/19 tells us we need an additional 3 bits19 - 16 = 3 bits3 bits = 128 + 64 + 32 = 224Default subnet mask for Class B network = 255.255.0.0New subnet mask for /19 network = 255.255.224.0To find the wildcard value:255.255.255.255255.255.224.0 ----------0.0.31.255 PDF Version | Download