Chapter 5 - QUIZ – ACLs
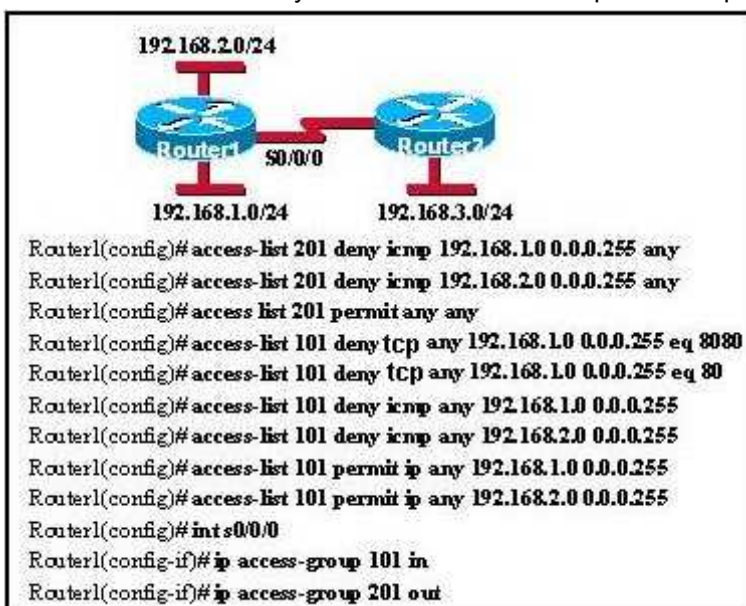
1. Which two statements correctly describe Cisco access control lists? (Choose two.)
   A. Extended ACL's are created in interface configuration mode.
   B. Extended ACL's filter traffic based on source and destination IP, port number, and protocol.
   C. Standard IP ACL's are numbered 1 to 99, and extended IP ACL's are numbered 100 to 199.
   D. Standard ACL's permit or deny traffic to specific IP addresses.
   E. Standard ACL's do not permit the use of wildcard masks.

2. Which statement is correct regarding applying an access list to an interface?
   A. Access lists are applied in global configuration mode.
   B. Named access lists are applied using the **ip access-name** command.
   C. Standard access lists should be applied to an interface as close as possible to the destination.
   D. The command for applying access list 101 inbound is **ip access-list 101**.

3. Which statement is a guideline to be followed when designing access control lists?
   A. Since ACL tests are executed in order, they should be organized from the most general condition to the most specific.
   B. Since ACL tests are executed in order, they should be organized from the most specific condition to the most general.
   C. Since all statements in an ACL are evaluated before they are executed, an explicit **deny any** statement must be written for an ACL to function properly.
   D. Since all statements in an ACL are evaluated before they are executed, an explicit **permit any** statement must be written in order for an ACL to function properly.

4. Which two solutions can be implemented with ACL's? (Choose two.)
   A. Segment the network to increase available bandwidth.
   B. Create a firewall on a router to filter inbound traffic from an external network.
   C. Control traffic entering or exiting different areas of a local network.
   D. Distribute DHCP traffic to allow easier network availability.
   E. Allow or deny traffic into the network based on the MAC address.

5. Match the following commands used with ACL's to their descriptions:

   A. ANY ➔ Represents an IP address and mask pair of 0.0.0.0 255.255.255.255.
   B. show running-config ➔ Reveals the ACL's and interface assignments on a router.
   C. show access-list ➔ Displays the contents of all ACL's on the router.
   D. HOST ➔ Substitutes for the 0.0.0.0 mask.
   E. show ip interface ➔ Indicates whether any ACL's are set on an interface.

6. Which IP address and wildcard mask will test for hosts from an entire subnet of network 192.168.12.0 using a 29-bit mask?
   A. 192.168.12.56 0.0.0.15
   B. 192.168.12.56 0.0.0.8
   C. 192.168.12.56 0.0.0.31
   D. 192.168.12.84 0.0.0.7
   E. 192.168.12.84 0.0.0.3
   F. 192.168.12.84 0.0.0.255

7. What kind of access list is created with the command ip **access-list standard fastaccess**?
   A. Turbo ACL
   B. Reflexive ACL
   C. Named ACL
   D. Dynamic ACL

8. Refer to the ACL 101 statements listed below to answer the question. This ACL already exists on the router. The network administrator wants to insert the command **access-list 101 deny tcp any 192.168.1.0 0.0.0.255 eq ftp** as the third line in the ACL shown. The network administrator enters the command in global configuration mode on the router. What effect does this have?

```
access-list 101 deny tcp any 192.168.1.0 0.0.0.255 eq 8080
access-list 101 deny tcp any 192.168.1.0 0.0.0.255 eq 80
access-list 101 deny icmp any 192.168.1.0 0.0.0.255
access list 101 deny icmp any 192.168.2.0 0.0.0.255
access-list 101 permit tcp any 192.168.1.0 0.0.0.255
access-list 101 permit tcp any 192.168.1.2.0 0.0.0.255
```

   A. It inserts the line in the desired position in the ACL.
   B. It inserts the line as the first statement in the ACL.
   C. It inserts the line as the last statement in the ACL.
   D. It deletes the entire list and replaces it with the new line only.

9. Refer to the topology description and ACL statements listed below to answer the question.
Which statement correctly describes how Router1 processes packets with the configuration shown?


```
192.168.2.0/24

Router1    S0/0/0    Router2

192.168.1.0/24        192.168.3.0/24
Router1(config)# access-list 201 deny icmp 192.168.1.0 0.0.0.255 any
Router1(config)# access-list 201 deny icmp 192.168.2.0 0.0.0.255 any
Router1(config)# access list 201 permit any any
Router1(config)# access-list 101 deny tcp any 192.168.1.0 0.0.0.255 eq 8080
Router1(config)# access-list 101 deny tcp any 192.168.1.0 0.0.0.255 eq 80
Router1(config)# access-list 101 deny icmp any 192.168.1.0 0.0.0.255
Router1(config)# access-list 101 deny icmp any 192.168.2.0 0.0.0.255
Router1(config)# access-list 101 permit ip any 192.168.1.0 0.0.0.255
Router1(config)# access-list 101 permit ip any 192.168.2.0 0.0.0.255
Router1(config)# int s0/0/0
Router1(config-if)# ip access-group 101 in
Router1(config-if)# ip access-group 201 out
```

   A. Traffic exiting interface s0/0/0 is filtered by both ACL 101 and ACL 201.
   B. If a packet entering interface s0/0/0 matches a condition in ACL 101, the router continues comparing the packet to the rest of the statements in ACL 101 to make sure that no other statements might also apply.
   C. Router1 compares packets entering interface s0/0/0 first to all the ACL 101 statements for the IP protocol and then to all the ACL 101 statements for the ICMP protocol.
   D. A packet entering interface s0/0/0 is compared to each statement in ACL 101 until one statement matches the packet. Then the router drops or forwards the packet without considering the remaining statements in ACL 101.

10. An administrator wants to implement lock-and-key access to a host within the company network for specific users who are connecting from outside the company network. What type of ACL would best suit the situation?
   A. Dynamic
   B. Reflexive
   C. Extended
   D. Time-based

11. What type of ACL should the network administrator implement to limit Internet traffic during peak hours of the day?
   A. Dynamic
   B. Policy-based
   C. Reflexive
   D. Time-based

12. Which statement correctly describes a reflexive access list?
    A. An ACL that allows IP traffic for sessions originating from inside the network, while denying traffic for sessions originating from the outside.
    B. An ACL that controls traffic based on the time.
    C. An ACL that uses an extended list to block users from traversing a router until they are authenticated.
    D. An ACL that only identifies the source of traffic.

13. Categorize the following descriptions with the appropriate ACL type.

Description		ACL Type
A. Only checks source address.	➜	Standard IP ACL
B. Access list numbers 100 to 199.	➜	Extended IP ACL
C. Checks protocol and port numbers.	➜	Extended IP ACL
D. Only permits or denies entire protocols based on the network address.	➜	Standard IP ACL
E. Access list numbers 1- to 99.	➜	Standard IP ACL
F. Checks source and destination addresses.	➜	Extended IP ACL

14. Assuming the following ACL is correctly applied to a router interface, which two statements describe traffic on the network? (Choose two.)

    access-list 199 deny tcp 178.15.0.0 0.0.255.255 any eq 23
    access-list 199 permit i p any any?

    A. All FTP traffic from network 178.15.0.0 will be permitted.
    B. All Telnet traffic destined for network 178.15.0.0 will be denied.
    C. Telnet and FTP will be permitted from all hosts on network 178.15.0.0 to any destination.
    D. Telnet will not be permitted from any hosts on network 178.15.0.0 to any destination.
    E. Telnet will not be permitted to any host on network 178.15.0.0 from any destination.