

CCNA Exploration: Accessing the WAN (Version 4.0)

Chapter 5 – ACLs

1 Which benefit does an extended ACL offer over a standard ACL?

- ☐ Extended ACLs can be named, but standard ACLs cannot.
 - ☐ Unlike standard ACLs, extended ACLs can be applied in the inbound or outbound direction.
 - ☐ Based on payload content, an extended ACL can filter packets, such as information in an e-mail or instant message.
 - ☒ In addition to the source address, an extended ACL can also filter on destination address, destination port, and source port.
-

2 How do Cisco standard ACLs filter traffic?

- ☐ by destination UDP port
 - ☐ by protocol type
 - ☒ by source IP address
 - ☐ by source UDP port
 - ☐ by destination IP address
-

3 Which three parameters can ACLs use to filter traffic? (Choose three)

- ☐ packet size
 - ☒ protocol suite
 - ☒ source address
 - ☒ destination address
 - ☐ source router interface
 - ☐ destination router interface
-

4 Where should a standard access control list be placed?

- ☐ close to the source
 - ☒ close to the destination
 - ☐ on an Ethernet port
 - ☐ on a serial port
-

5 Which two statements are true regarding the following extended ACL? (Choose two)

access-list 101 deny tcp 172.16.3.0 0.0.0.255 any eq 20

access-list 101 deny tcp 172.16.3.0 0.0.0.255 any eq 21

access-list 101 permit ip any any

- ☒ FTP traffic originating from network 172.16.3.0/24 is denied.
 - ☐ All traffic is implicitly denied.
 - ☐ FTP traffic destined for the 172.16.3.0/24 network is denied.
 - ☐ Telnet traffic originating on network 172.16.3.0/24 is denied.
 - ☒ Web traffic originating from 172.16.3.0 is permitted.
-

6 Which statement about standard ACLs is true?

- ☐ Standard ACLs must be numbered and cannot be named.
 - ☒ They should be placed as close to the destination as possible.
 - ☐ They can filter based on source and destination address as well as on source and destination port.
 - ☐ When applied to an outbound interface, incoming packets are processed before they are routed to the outbound interface.
-

7 Which two statements are true regarding named ACLs? (Choose two)

- ☐ Only named ACLs allow comments.
- ☒ Names can be used to help identify the function of the ACL.
- ☐ Named ACLs offer more specific filtering options than numbered ACLs.
- ☒ Certain complex ACLs, such as reflexive ACLs, must be defined with named ACLs.
- ☐ More than one named IP ACL can be configured in each direction on a router interface.

8 Which three items must be configured before a dynamic ACL can become active on a router? (Choose three)

- ☒ extended ACL
- ☐ reflexive ACL
- ☐ console logging
- ☒ authentication
- ☒ Telnet connectivity
- ☐ user account with a privilege level of 15

9

```
Router# show ip access-lists
Extended IP access list Managers
deny tcp 192.168.1.0 0.0.0.255 any eq telnet
deny tcp 192.168.1.0 0.0.0.255 any eq www
deny tcp 192.168.1.0 0.0.0.255 any eq ftp
permit ip any any
```

Refer to the exhibit. How can a comment be added to the beginning of this ACL to identify its purpose?

- ☐ Use the **remark** command to add a remark to the beginning of the ACL.
- ☐ Use the **description** command to add a description to the beginning of the ACL.
- ☒ Recreate the ACL and use the **remark** command to add a remark to the beginning of the ACL.
- ☐ Recreate the ACL and use the **description** command to add a description to the beginning of the ACL.

10 Which three statements describe ACL processing of packets? (Choose three)

- ☒ An implicit **deny any** rejects any packet that does not match any ACL statement.
- ☒ A packet can either be rejected or forwarded as directed by the statement that is matched.
- ☐ A packet that has been denied by one statement can be permitted by a subsequent statement.
- ☐ A packet that does not match the conditions of any ACL statements will be forwarded by default.
- ☒ Each statement is checked only until a match is detected or until the end of the ACL statement list.
- ☐ Each packet is compared to the conditions of every statement in the ACL before a forwarding decision is made.

11 Which two statements are true regarding the significance of the access control list wildcard mask 0.0.0.7? (Choose two)

- ☐ The first 29 bits of a given IP address will be ignored.
- ☒ The last 3 bits of a given IP address will be ignored.
- ☐ The first 32 bits of a given IP address will be checked.
- ☒ The first 29 bits of a given IP address will be checked.
- ☐ The last 3 bits of a given IP address will be checked.

12 By default, how is IP traffic filtered in a Cisco router?

- ☐ blocked in and out of all interfaces
- ☐ blocked on all inbound interfaces, but permitted on all outbound interfaces
- ☒ permitted in and out of all interfaces
- ☐ blocked on all outbound interfaces, but permitted on all inbound interfaces

13 R2# show ip access-list
Standard IP access list WEBSERVER
10 permit 192.168.10.11 0.0.255.255
20 permit host 192.168.10.13

Refer to the exhibit. How does this access list process a packet with the source address 10.1.1.1 and a destination of 192.168.10.13?

- ☐ It is allowed because of the implicit deny any.
- ☒ It is dropped because it does not match any of the items in the ACL.
- ☐ It is allowed because line 10 of the ACL allows packets to 192.168.0.0/16.
- ☐ It is allowed because line 20 of the ACL allows packets to the host 192.168.10.13.

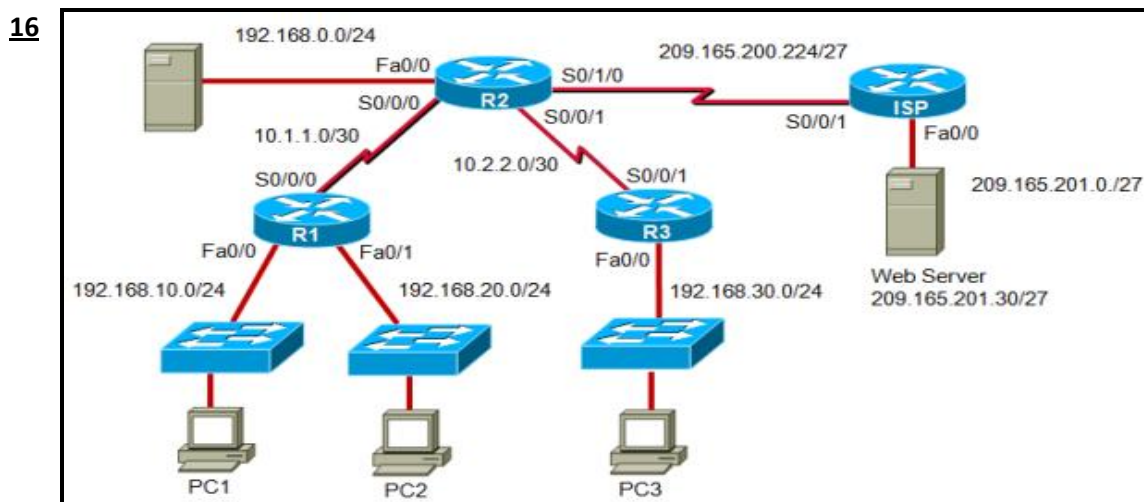
14 Router1 (config)# time-range EVERYOTHERDAY
Router1 (config-time-range)# periodic Monday Wednesday Friday 8:00 to 17:00
Router1 (config)# access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eg telnet time-range EVERYOTHERDAY
Router1 (config)# interface fa0/0
Router1 (config-if)# ip address 10.1.1.1 255.255.255.0
Router1 (config-if)# ip access-group 101 in

Refer to the exhibit. How will Router1 treat traffic matching the time-range requirement of EVERYOTHERDAY?

- ☐ TCP traffic entering fa0/0 from 172.16.1.254/24 destined to the 10.1.1.0/24 network is permitted.
- ☐ TCP traffic entering fa0/0 from 10.1.1.254/24 destined to the 172.16.1.0/24 network is permitted.
- ☐ Telnet traffic entering fa0/0 from 172.16.1.254/24 destined to the 10.1.1.0/24 network is permitted.
- ☒ Telnet traffic entering fa0/0 from 10.1.1.254/24 destined to the 172.16.1.0/24 network is permitted.

15 A network administrator needs to allow traffic through the firewall router for sessions that originate from within the company network, but the administrator must block traffic for sessions that originate outside the network of the company. What type of ACL is most appropriate?

- ☐ dynamic
- ☐ port-based
- ☒ reflexive
- ☐ time-based



Refer to the exhibit. When creating an extended ACL to deny traffic from the 192.168.30.0 network destined for the Web server 209.165.201.30, where is the best location for applying the ACL?

- ☐ ISP Fa0/0 outbound
- ☐ R2 S0/0/1 inbound
- ☒ R3 Fa0/0 inbound
- ☐ R3 S0/0/1 outbound

17 The following commands were entered on a router:

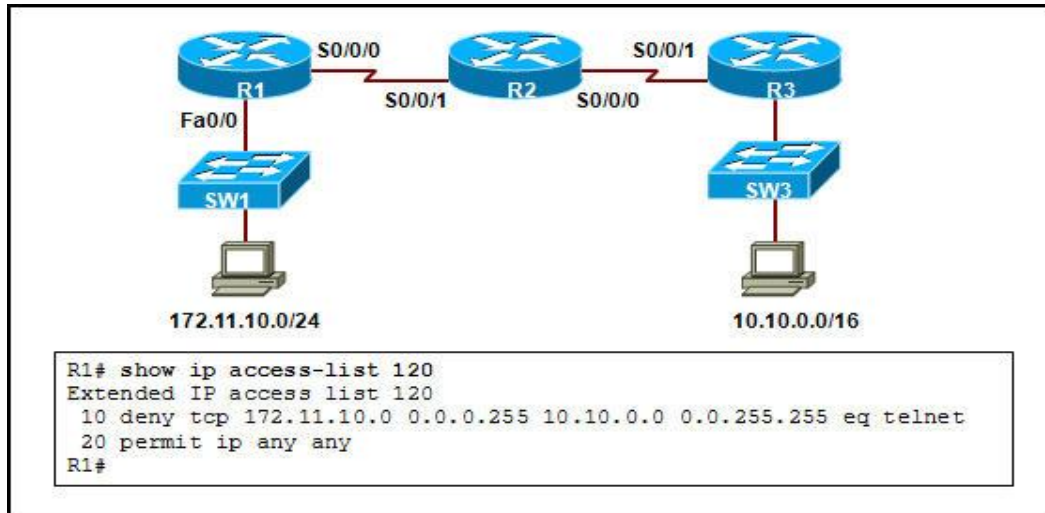
Router(config)# access-list 2 deny 172.16.5.24

Router(config)# access-list 2 permit any

The ACL is correctly applied to an interface. What can be concluded about this set of commands?

- ☒ The wildcard mask 0.0.0.0 is assumed.
- ☐ The access list statements are misconfigured.
- ☐ All nodes on the 172.16.0.0 network will be denied access to other networks.
- ☐ No traffic will be allowed to access any nodes or services on the 172.16.0.0 network.

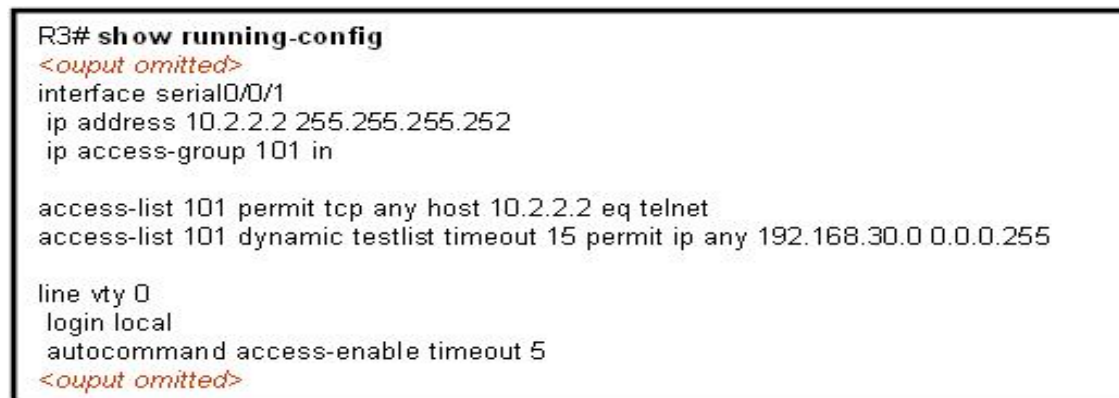
18



Refer to the exhibit. ACL 120 is configured inbound on the serial0/0/0 interface on router R1, but the hosts on network 172.11.10.0/24 are able to telnet to network 10.10.0.0/16. On the basis of the provided configuration, what should be done to remedy the problem?

- ☒ Apply the ACL outbound on the serial0/0/0 interface on router R1.
- ☐ Apply the ACL outbound on the FastEthernet0/0 interface on router R1.
- ☐ Include the established keyword at the end of the first line in the ACL.
- ☐ Include a statement in the ACL to deny the UDP traffic that originates from 172.11.10.0/24 network.

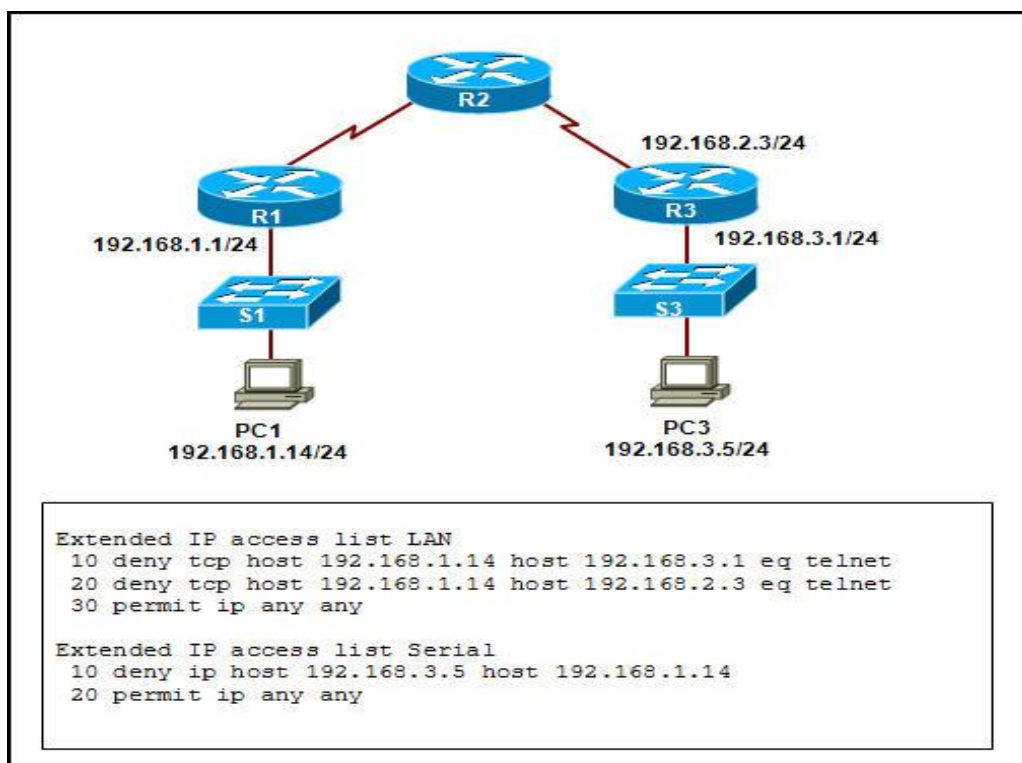
19



Refer to the exhibit. What will be the effect of the configuration that is shown?

- ☒ Users attempting to access hosts in the 192.168.30.0/24 network will be required to telnet to R3.
- ☐ Hosts connecting to resources in the 191.68.30.0/24 network have an idle timeout of 15 minutes.
- ☐ Anyone attempting to telnet into R3 will have an absolute time limit of five minutes.
- ☐ Telnet access to R3 will only be permitted on Serial 0/0/1.

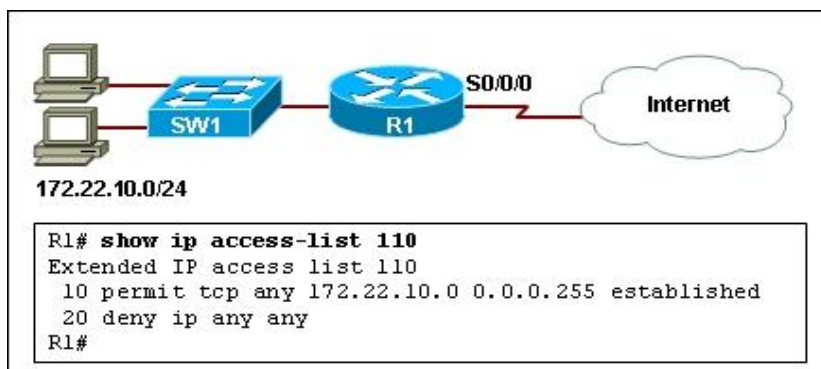
20



Refer to the exhibit. An administrator has configured two access lists on R1. The list inbound on the serial interface is named **Serial** and the list inbound on the LAN interface is named **LAN**. What affect will be produced by the access control lists?

- ☐ PC1 will be able to telnet to PC3.
- ☐ R3 will not be able to communicate with PC1 and PC3.
- ☐ PC3 cannot telnet to R3 and cannot communicate with PC1.
- ☒ PC1 will not be able to telnet to R3 and PC3 will not be able to communicate with PC1.

21



Refer to the exhibit. Which statement is true about ACL 110 if ACL 110 is applied in the inbound direction on S0/0/0 of R1?

- ☐ It will deny TCP traffic to the Internet if the traffic is sourced from the 172.22.10.0/24 network.
- ☐ It will not allow TCP traffic coming from the Internet to enter the network 172.22.10.0/24.
- ☐ It will allow any TCP traffic from the Internet to enter the network 172.22.10.0/24.
- ☒ It will permit any TCP traffic that originated from network 172.22.10.0/24 to return inbound on the S0/0/0 interface.

22 Which feature will require the use of a named ACL rather than a numbered ACL?

- ☐ the ability to filter traffic based on a specific protocol
- ☐ the ability to filter traffic based on an entire protocol suite and destination
- ☐ the ability to specify source and destination addresses to use when identifying traffic
- ☒ the ability to edit the ACL and add additional statements in the middle of the list without removing and re-creating the list

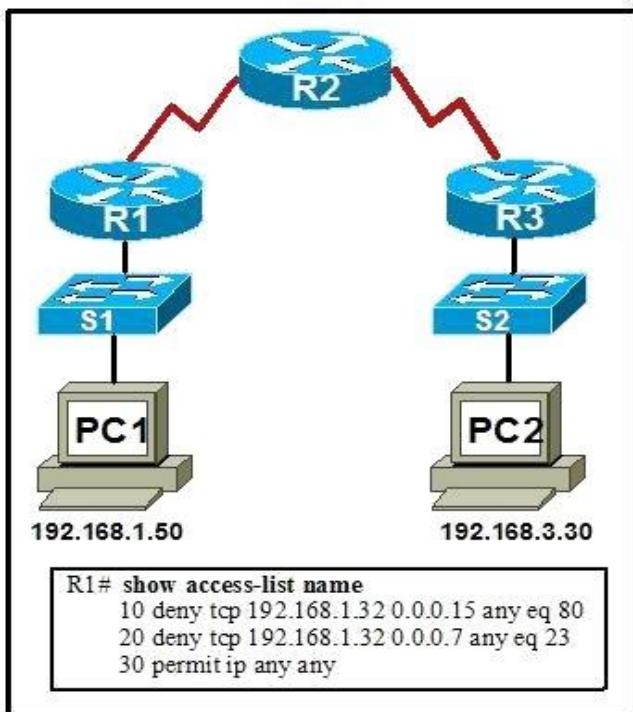
23 A technician is creating an ACL and needs a way to indicate only the subnet 172.16.16.0/21. Which combination of network address and wildcard mask will accomplish the desired task?

- ☐ 172.16.0.0 0.0.255.255
- ☐ 127.16.16.0 0.0.0.255
- ☒ 172.16.16.0 0.0.7.255
- ☐ 172.16.16.0 0.0.15.255
- ☐ 172.16.16.0 0.0.255.255

24 Which two statements are correct about extended ACLs? (Choose two)

- ☐ Extended ACLs use a number range from 1-99.
- ☐ Extended ACLs end with an implicit permit statement.
- ☒ Extended ACLs evaluate the source and destination addresses.
- ☒ Port numbers can be used to add greater definition to an ACL.
- ☐ Multiple ACLs can be placed on the same interface as long as they are in the same direction.

25



Refer to the exhibit. The administrator wishes to block web traffic from 192.168.1.50 from reaching the default port of the web service on 192.168.3.30. To do this, the access control list name is applied inbound on the router R1 LAN interface. After testing the list, the administrator has noted that the web traffic remains successful. Why is web traffic reaching the destination?

- ☐ Web traffic does not use port 80 by default.
- ☐ The access list is applied in the wrong direction.
- ☐ The access list needs to be placed closer to the destination, on R3.
- ☒ The range of source addresses specified in line 10 does not include host 192.168.1.50