MODULE 5 : ACCESS LIST LISTS(ACLs)

1 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

---

2 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.

---

3 Interface s0/0/0 already has an IP ACL applied inbound. What happens when the network administrator attempts to apply a second inbound IP ACL?

- **The second ACL is applied to the interface, replacing the first.**
- Both ACLs are applied to the interface.
- The network administrator receives an error.
- Only the first ACL remains applied to the interface.

---

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

---

5 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.

6

```
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?

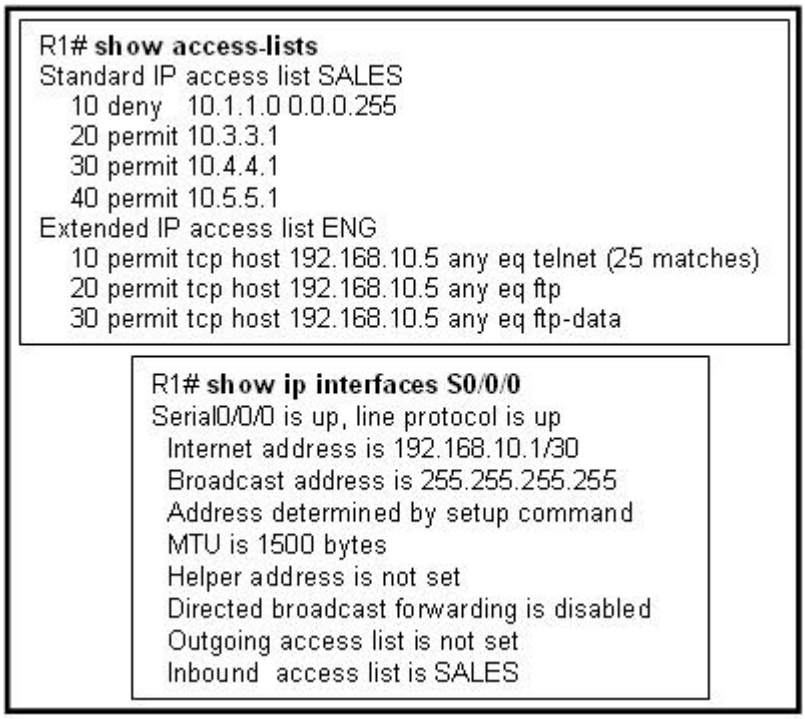
- **Use the remark command to add a remark to the beginning of the ACL.**
- Use the **description** command to add a description to the beginning of the ACL.
- Recreate the ACL and use the **remark** command to add a remark to the beginning of the ACL.
- Recreate the ACL and use the **description** command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

---

7 If all the statements in an ACL are unmatched, what happens to the packet?

- The packets will be placed in a buffer and forwarded when the ACL is removed.
- The packets will be sent to the source with an error notification message.
- The implicit **permit any** statement placed at the end of the list will allow the packets to flow through uninhibited.
- **The implicit deny any statement placed at the end of the list will cause the packets to be dropped.**

8



Refer to the exhibit. Which three conclusions can be derived from the output that is shown? (Choose three.)

- [ ] **All traffic, except for three host addresses, will be denied coming into interface S0/0/0.**
- [ ] **No traffic is permitted out interface S0/0/0.**
- [ ] Telnet and FTP traffic from 192.168.10.5 to any host is permitted in from interface S0/0/0.
- [ ] Telnet and FTP traffic have been received at R1 from 192.168.10.5.
- [ ] Permitted traffic from 192.168.10.5 came through an interface other than S0/0/0.
- [ ] **Access list SALES has not yet permitted any traffic.**

---

9 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

---

10 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.

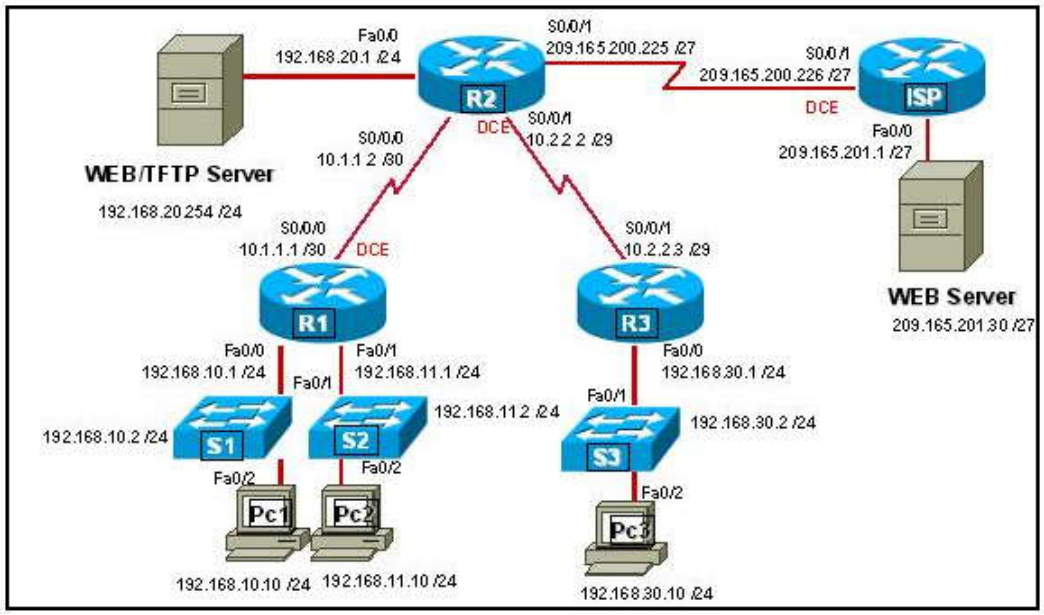
- [ ] **The first 29 bits of a given IP address will be checked.**
- [ ] The last 3 bits of a given IP address will be checked.

---

11 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

12



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?

- ● **R3 Fa0/0 inbound**
- ● R3 S0/0/1 outbound
- ● R2 S0/0/1 inbound
- ● ISP Fa0/0 outbound

---

13 Which three statements are true regarding named ACLs? (Choose three.)

- [ ] **Names can be used to help identify the function of the ACL.**
- [ ] Named ACLs offer more specific filtering options than numbered ACLs.

- [ ] **Named ACLs can be modified without re-entering the entire ACL.**
- [ ] More than one named IP ACL can be configured in each direction on a router interface.
- [ ] **Certain complex ACLs, such as reflexive ACLs, must be defined with named ACLs.**
- [ ] Only named ACLs allow comments.

---

14 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

15

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

---

16 A network administrator needs to allow traffic through the firewall router for sessions originating from within the company network, but block traffic for sessions that originate outside the netowrk of the company. What type of ACL is most appropri

- Dynamic
- **Reflexive**
- time-based
- port-based

17

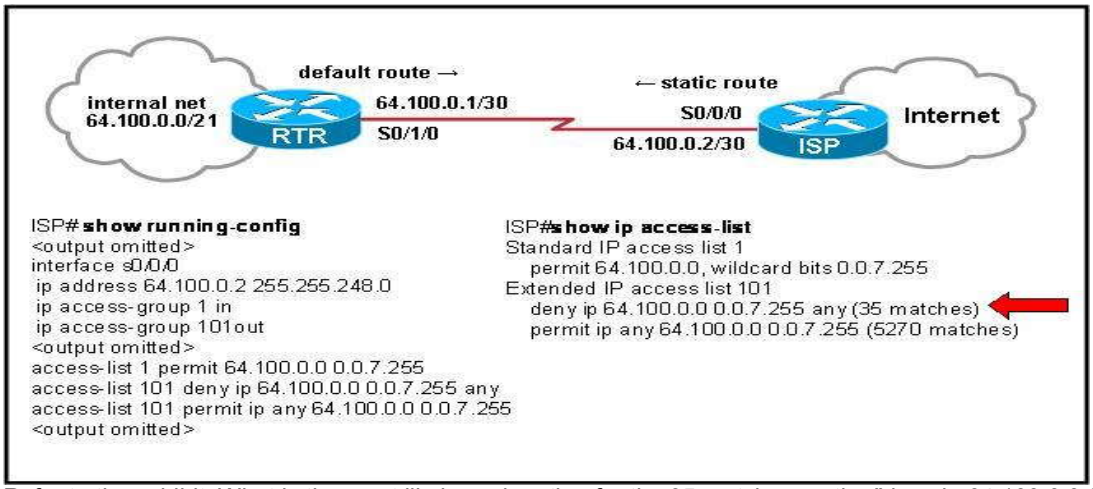
```
Router1 (config)# time-range EVERYOTHERDAY
Router1 (config-time-range)# periodic Monday Wednesday Friday 8:00 to 17:00
Router1 (config)# access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range EVERYOTHERDAY
Router1 (config)# interface fa0/0
Router1 (config-if)# ip 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.**

18



Refer to the exhibit. What is the most likely explanation for the 35 matches on the "deny ip 64.100.0.0 0.0.7.255 any" statement for ACL 101?

- A user on the internal network has spoofed a host from the Internet and is sending traffic to that host, which is respondin
- A user on the Internet has spoofed a host address from the internal network and is trying to send packets toward the inte network.
- **An Internet host is looping traffic from the internal network.**
- A host on the internal network is looping traffic from the Internet.

---

19 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.**

---

20 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