WILEY

SYBEX
A Wiley Brand

CCENT Study Guide

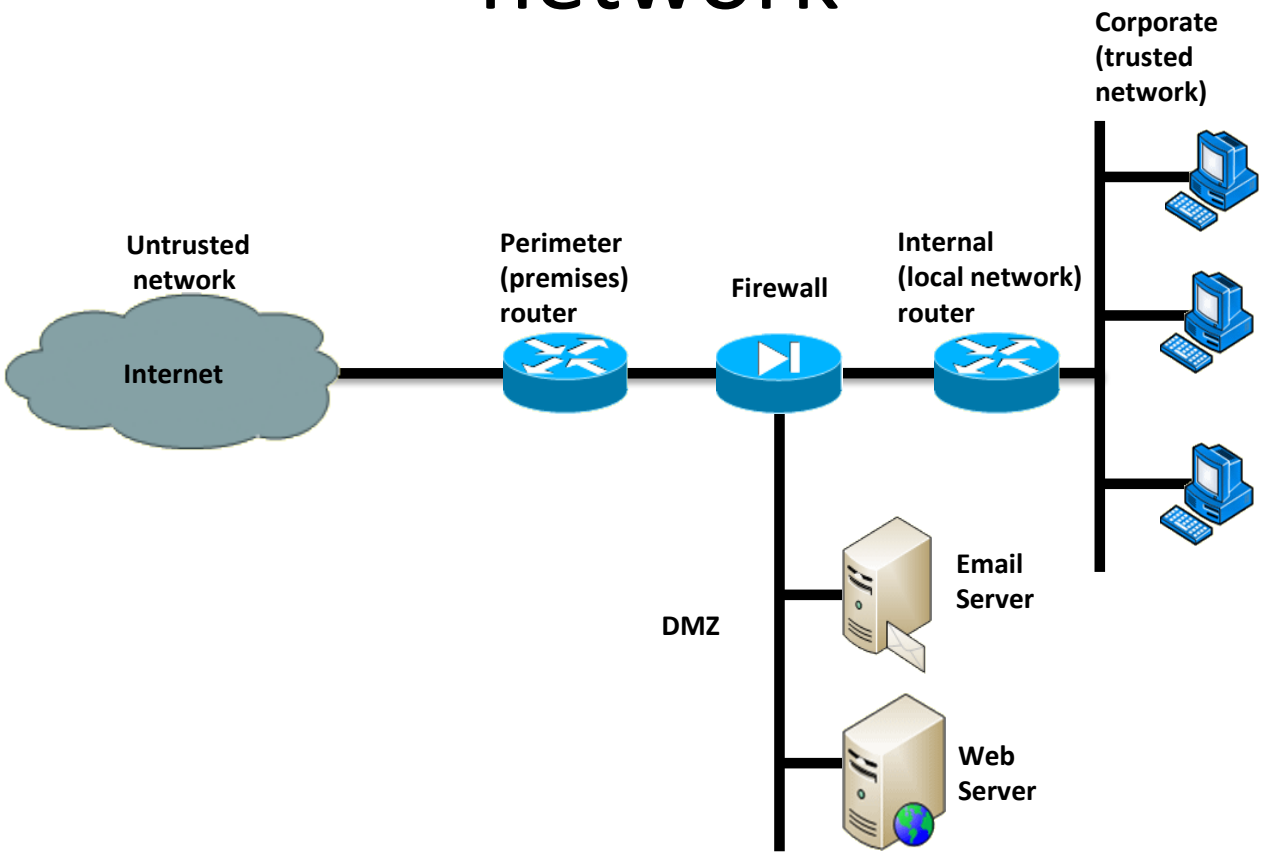
Chapter 12

Security

Chapter 12 Objectives

- The CCENT Topics Covered in this chapter include:
- **4.0 Infrastructure Services**
- 4.6 Configure, verify, and troubleshoot IPv4 standard
- numbered and named access list for routed interfaces.

Figure 12.1: A typical secured network



The demilitarized zone (DMZ) can be global (real) Internet addresses or private addresses, depending on how you configure your firewall, but this is typically where you'll find the HTTP, DNS, email, and other Internet-type corporate servers.

Access Lists

There are two main types of access lists:

Standard access lists

These ACLs use only the source IP address in an IP packet as the condition test. All decisions are made based on the source IP address. This means that standard access lists basically permit or deny an entire suite of protocols. They don't distinguish between any of the many types of IP traffic such as Web, Telnet, UDP, and so on.

Extended access lists

Extended access lists can evaluate many of the other fields in the layer 3 and layer 4 headers of an IP packet. They can evaluate source and destination IP addresses, the Protocol field in the Network layer header, and the port number at the Transport layer header. This gives extended access lists the ability to make much more granular decisions when controlling traffic.

Named access lists

Hey, wait a minute—I said there were only two types of access lists but listed three! Well, technically there really are only two since *named access lists* are either standard or extended and not actually a distinct type. I'm just distinguishing them because they're created and referred to differently than standard and extended access lists are, but they're still functionally the same.

Direction

Once you create an access list, it's not really going to do anything until you apply it.

By specifying the direction of traffic, you can and must use different access lists for inbound and outbound traffic on a single interface:

Inbound access lists

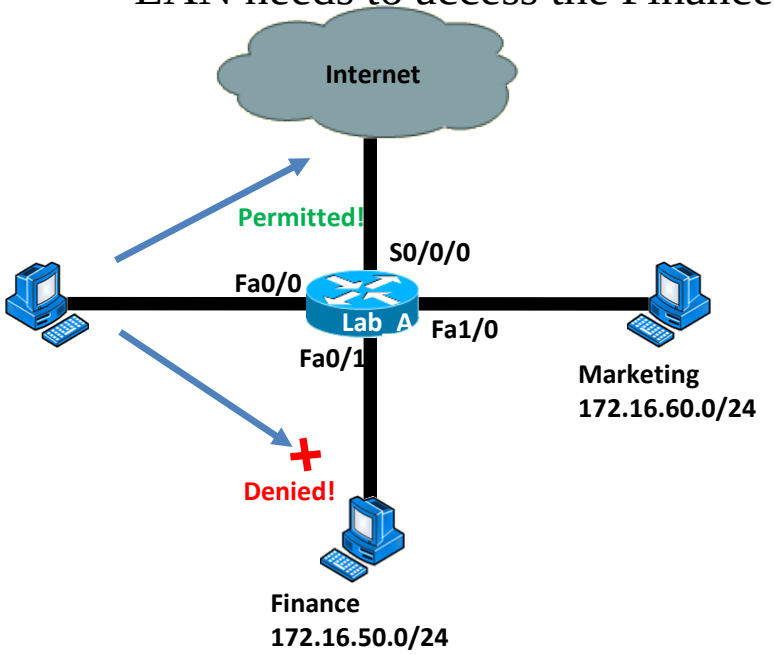
When an access list is applied to inbound packets on an interface, those packets are processed through the access list before being routed to the outbound interface. Any packets that are denied won't be routed because they're discarded before the routing process is invoked.

Outbound access lists

When an access list is applied to outbound packets on an interface, packets are routed to the outbound interface and then processed through the access list before being queued.

Figure 12.2: IP access list example with three LANs and a WAN connection

In Figure 12.2, a router has three LAN connections and one WAN connection to the Internet. Users on the Sales LAN should not have access to the Finance LAN, but they should be able to access the Internet and the marketing department files. The Marketing LAN needs to access the Finance LAN for application services.



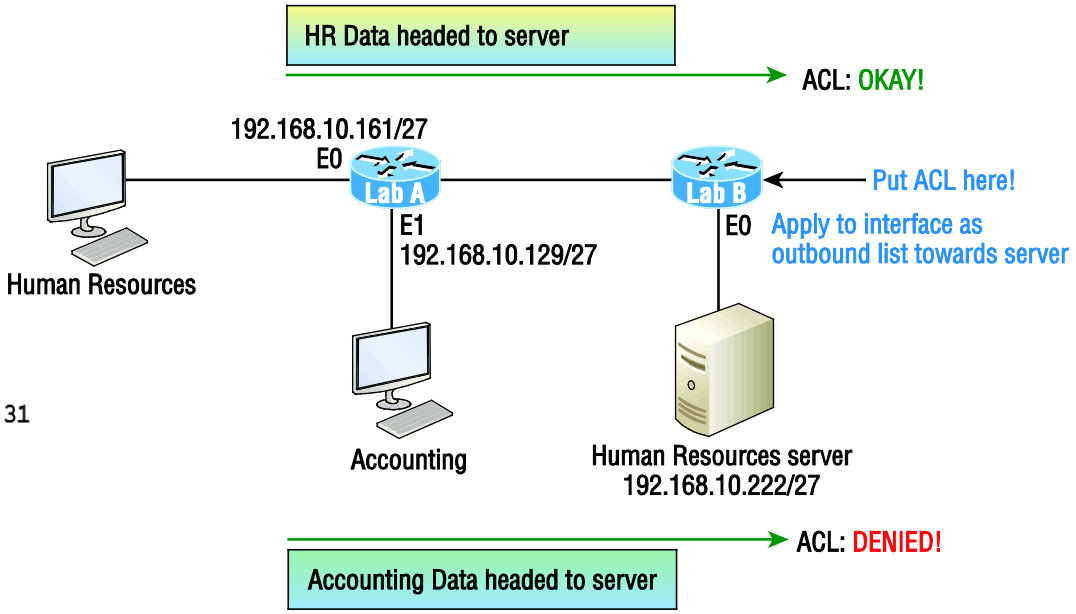

```
Lab_A#config t
Lab_A(config)#access-list 10 deny 172.16.40.0 0.0.0.255
Lab_A(config)#access-list 10 permit any
```

```
Lab_A(config)#int fa0/1
Lab_A(config-if)#ip access-group 10 out
```

Doing this completely stops traffic from 172.16.40.0 from getting out FastEthernet0/1. It has no effect on the hosts from the Sales LAN accessing the Marketing LAN and the Internet because traffic to those destinations doesn't go through interface Fa0/1.

Figure 12.3: IP standard access list example 2

Now we're going to stop the Accounting users from accessing the Human Resources server attached to the Lab B router but allow all other users access to that LAN using a standard ACL.

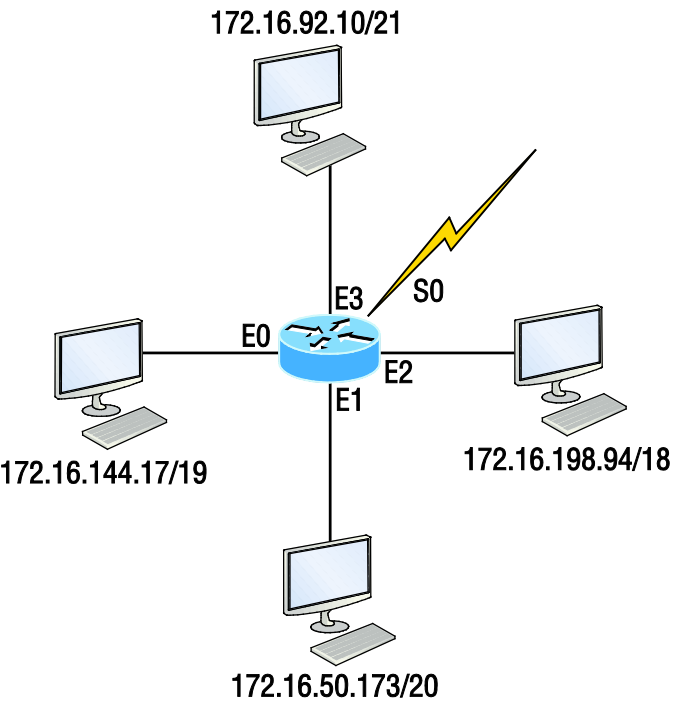



```
Lab_B#config t
Lab_B(config)#access-list 10 deny 192.168.10.128 0.0.0.31
Lab_B(config)#access-list 10 permit any
Lab_B(config)#interface Ethernet 0
Lab_B(config-if)#ip access-group 10 out
```

Keep in mind that to be able to answer this question correctly, you really need to understand subnetting, wildcard masks, and how to configure and implement ACLs. The accounting subnet is the 192.168.10.128/27, which is a 255.255.255.224, with a block size of 32 in the fourth octet.

Figure 12.4: IP standard access list example 3

Okay—you need to write an access list that will stop access from each of the four LANs shown in the diagram to the Internet.



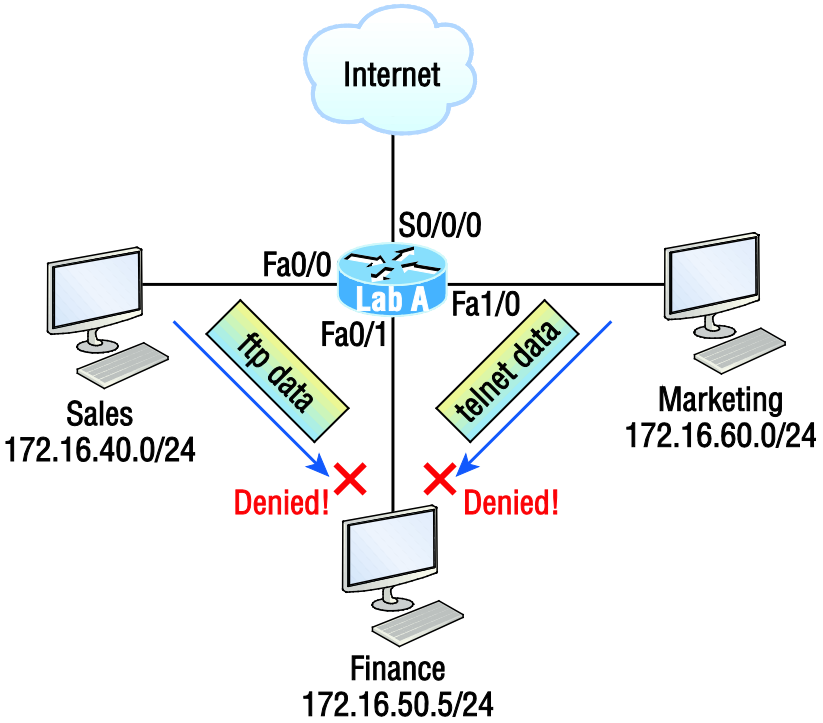
Here is an example of what your answer should look like, beginning with the network on E0 and working through to E3:

```
Router(config)#access-list 1 deny 172.16.128.0 0.0.31.255
Router(config)#access-list 1 deny 172.16.48.0 0.0.15.255
Router(config)#access-list 1 deny 172.16.192.0 0.0.63.255
Router(config)#access-list 1 deny 172.16.88.0 0.0.7.255
Router(config)#access-list 1 permit any
Router(config)#interface serial 0
Router(config-if)#ip access-group 1 out
```

Figure 12.5: Extended ACL example 1

What do we need to do to deny access to a host at 172.16.50.5 on the finance department LAN for both Telnet and FTP services? All other services on this and all other hosts are acceptable for the sales and marketing departments to access.

```
Lab_A#config t
Lab_A(config)#access-list 110 deny tcp any host
172.16.50.5 eq 21
Lab_A(config)#access-list 110 deny tcp any host
172.16.50.5 eq 23
Lab_A(config)#access-list 110 permit ip any any
Lab_A(config)#int fa0/1
Lab_A(config-if)#ip access-group 110 out
```



The `access-list 110` tells the router we're creating an extended IP ACL. The `tcp` is the protocol field in the Network layer header. If the list doesn't say `tcp` here, you cannot filter by TCP port numbers 21 and 23 as shown in the example.

Table 12.1: Commands used to verify access-list configuration

Command	Effect
show access-list	Displays all access lists and their parameters configured on the router. Also shows statistics about how many times the line either permitted or denied a packet. This command does not show you which interface the list is applied on.
show access-list 110	Reveals only the parameters for the access list 110. Again, this command will not reveal the specific interface the list is set on.
show ip access-list	Shows only the IP access lists configured on the router.
show ip interface	Displays which interfaces have access lists set on them.
show running-config	Shows the access lists and the specific interfaces that have ACLs applied on them.

Written Labs and Review Questions

- Read through the Exam Essentials section together in class.
- Open your books and go through all the written labs and the review questions.
- Review the answers in class.