ACL - Access Control List

SDC CNW (CSE 4541)

CSE, FET, ITER
SOA University, BBSR-30

References

Glen E. Clarke & Richard Deal

CCT/CCNA

Routing & Switching Exam Guide

McGrawHll

Todd Lammle

CCNA

Routing & Switching Study Guide

SYBEX, A Wiley Brand

Discussion Flow

- Introduction
- Types of ACL
- ACL Rules & Guideline
- Standard ACL
- Extended ACL
- Named ACL
- Exercise on ACL

Review Questions

Introduction

- An access list is essentially a list of conditions that categorize packets.
- It provides a way to exercise control over network traffic.
- Uses of access lists is to filter unwanted packets when implementing security policies.
- **For example**, ACL can be set to make very specific decisions about regulating traffic patterns so that they will allow only certain hosts to access web resources on the Internet while restricting others.
- Creating access lists is like programming a series of if-then statements: if a given condition is met, then a given action is taken. If the specific condition isn't met, nothing happens and the next statement is evaluated.
- Access-list statements are basically packet filters that packets are compared against, categorized by, and acted upon accordingly.
- Once the lists are built, they can be applied to either **inbound** or **outbound** traffic on any interface.

Types of ACL

There are two main types of access lists:

Standard access lists:

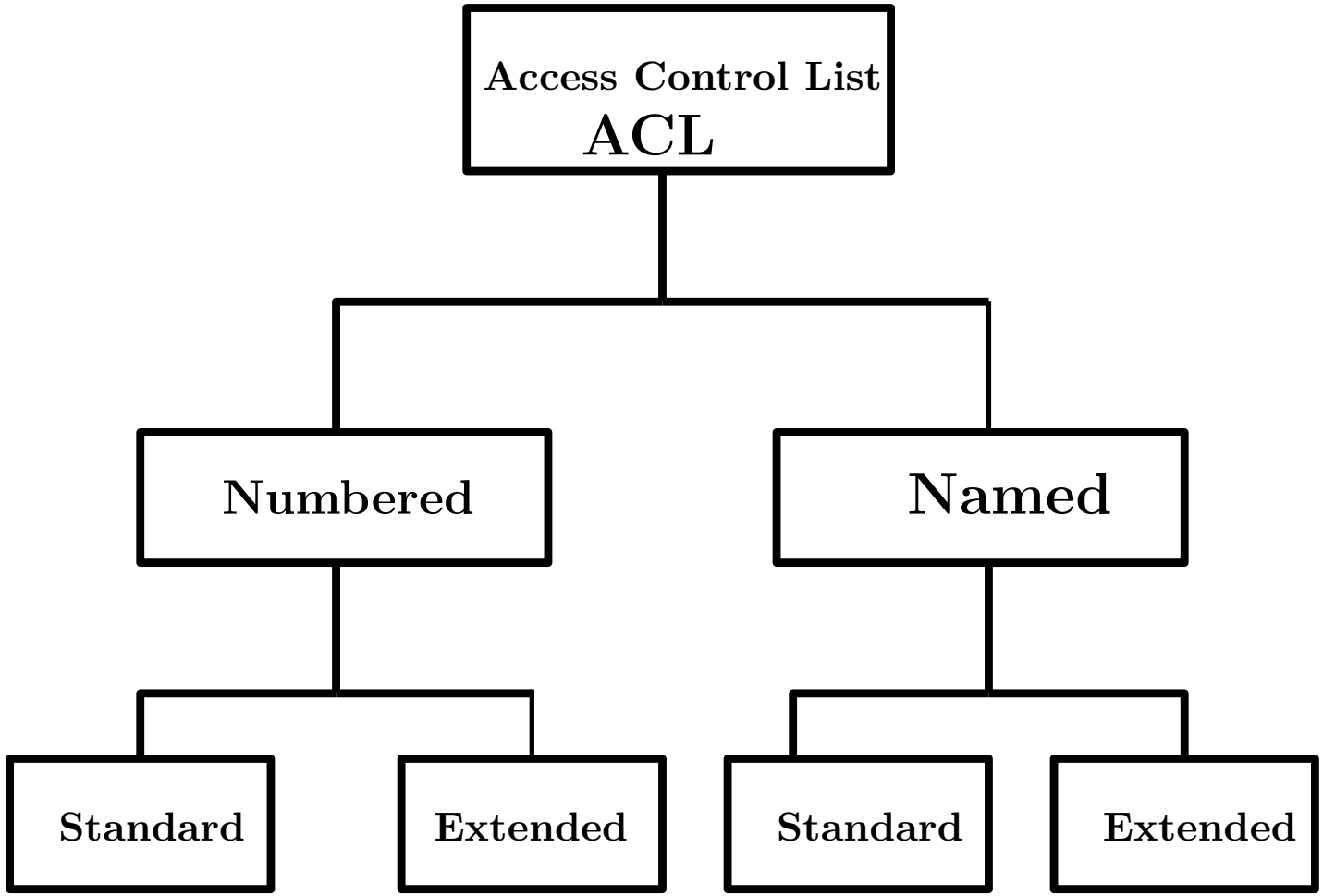
- These ACLs use only the source IP address in an IP packet as the condition test.
- All decisions are made based on the source IP address.
- Standard access lists basically **permit or deny** an entire suite of protocols.
- They do not distinguish between any of the many types of IP traffic such as 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.

These lists are also called **numbered access list**

Putting ACL Types Altogether



Named ACL

Named access lists:

- Named access lists are either standard or extended and not actually a distinct type.
- They are created and referred to differently than standard and extended access lists are, but they are still functionally the same.

How to use access list:

- **Create the access list:** Once you create an access list, its not really going to do anything until you apply it.
- **Apply access list:** Yes, they are there on the router, but they are inactive until you tell that router what to do with them.
- **To use an access list as a packet filter:** (i) apply it to an interface on the router where traffic will be filtered (ii) specify the direction of the traffic (i.e. inbound and outbound traffic on a single interface).

Inbound and Outbound access lists

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 are discarded before the routing process is invoked.

Outbound access list:

- 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.

ACL Rules

There are three important rules that a packet follows when it's being compared with an access list:

- The packet is always compared with each line of the access list in sequential order: it will always start with the first line of the access list, move on to line 2, then line 3, and so on.

- The packet is compared with lines of the access list only until a match is made. Once it matches the condition on a line of the access list, the packet is acted upon and no further comparisons take place.

- There is an implicit **deny** at the end of each access list - this means that if a packet does not match the condition on any of the lines in the access list, the packet will be **discarded**.

Access-list Guidelines During Create and Apply

- Only one access list can be assigned per interface per protocol per direction. This means that when applying IP access lists, you can have only one inbound access list and one outbound access list per interface.
- Organize the access lists so that the more specific tests are at the top.
- Anytime a new entry is added to the access list, it will be placed at the bottom of the list.
- One line can not be removed from an access list. If you try to do this, you will remove the entire list. (Exeption: Line can be edited, added, or deleted a single line from a named access list).
- Create access lists and then apply them to an interface. Any access list applied to an interface without access-list test statements present will not filter traffic.
- Access lists are designed to filter traffic going through the router. They will not filter traffic that has originated from the router.
- Place IP standard access lists as close to the destination as possible. you can only filter based on source address and all destinations would be affected as a result.
- Place IP extended access lists as close to the source as possible. By placing this list as close to the source address as possible, you can filter traffic before it uses up precious bandwidth.
- Unless your access list ends with a `permit any` command, all packets will be discarded if they do not meet any of the list's tests.

Mitigating Security Issues with ACLs

A list of security threats that can mitigate with ACLs:

- IP address spoofing, inbound
- IP address spoofing, outbound
- Denial of service (DoS) TCP SYN attacks, blocking external attacks
- DoS TCP SYN attacks, using TCP Intercept
- DoS smurf attacks
- Denying/filtering ICMP messages, inbound
- Denying/filtering ICMP messages, outbound
- Denying/filtering Traceroute

The most common attack is a denial of service (DoS) attack. Although ACLs can help with a DoS, you really need an intrusion detection system (IDS) and intrusion prevention system (IPS) to help prevent these common attacks. Cisco sells the Adaptive Security Appliance (ASA), which has IDS/IPS modules, but lots of other companies sell IDS/IPS products too.

Standard Access Lists

- This lists filter network traffic by examining the source IP address in a packet.
- This list is created by using the access-list numbers 1- 99 or numbers in the expanded range of 1300- 1999.
- Based on the number used when the access list is created, the router knows which type of syntax to expect as the list is entered.
- By using numbers 1-99 or 1300-1999, it is told to the router that a standard IP access list is created, so the router will expect syntax specifying only the source IP address in the test lines.

Standard access list command

```
Router(config)#access-list ?
Router(config)#access-list 10 ?


...(config)#access-list deny ?
```

Example :

```
Router(config)#access-list 10 deny host
172.16.30.2
```

OR cab be

```
Router(config)#access-list 10 deny
172.16.30.2
```

The list 10 to deny any packets from host 172.16.30.2.

Description:

➡ Displays access-list number ranges to be used to filter traffic.

➡

deny	Specify packets to reject
permit	Specify packets to forward
remark	Access list entry comment

➡

Hostname or A.B.C.D	Address to match
any	Any source host
host	A single host address

- Use an IP address to specify either a single host or a range of them.
- The `any` parameter used to permit or deny any source host or network.
- Use the `host` command to specify a specific host only.

Wildcard Masking

- Wildcards are used with access lists to specify an individual host, a network, or a specific range of a network or networks.
- Wildcards are used with the host or network address to tell the router a range of available addresses to filter.
- The block sizes used to specify a range of IP addresses are key to understanding wildcards.

Wildcard Mask

- **Exact match:** Put 0 in against of the reference octet in an IP.
- **Octet to have any value:** Put 255 in against of the reference octet in an IP .
- **Octet for network range IP:** Wildcard mask for that reference octet will be block size - 1.

Evaluation:

- To specify a host with IP- 172.16.30.5
  The wildcard mask - 0.0.0.0
- To specify /24 subnet of IP 172.16.30.0
  The wildcard mask:0.0.0.255
- Network ranges: from 172.16.8.0 through 172.16.15.0.
  wildcard mask, Here block size is 8:
  0.0.16.(blocksize-1).255 = 0.0.(8-1).255 = 0.0.7.255

Example: Wildcard Masking

ACL configuration with wildcard mask

- Router to match the first three octets exactly but that the fourth octet can be anything:
  `Router(config)#access-list 10 deny 172.16.10.0 0.0.0.255`
- Router to match the first two octets and that the last two octets can be any value:
  `Router(config)#access-list 10 deny 172.16.0.0 0.0.255.255`
- This configuration tells the router to start at network 172.16.16.0 and use a block size of 4: The range would then be 172.16.16.0 through 172.16.19.255. So, the access list configuration:
  `Router(config)#access-list 10 deny 172.16.16.0 0.0.3.255`
- Wildmask for the access list starting at 172.16.16.0 going up a block size of 8 to 172.16.23.255.:
  `Router(config)#access-list 10 deny 172.16.16.0 0.0.7.255`
- Wildmask for the access list begins at network 172.16.32.0 and goes up a block size of 16 to 172.16.47.255:
  `Router(config)#access-list 10 permit 172.16.32.0 0.0.15.255`
- Wildmask for the access list begins at network 172.16.64.0 and goes up a block size of 64 to 172.16.127.255:
  `Router(config)#access-list 10 permit 172.16.64.0 0.0.63.255`
- Wildmask for the access list begins at network 192.168.160.0 and goes up a block size of 32 to 192.168.191.255:
  `Router(config)#access-list 10 deny 192.168.160.0 0.0.31.255`

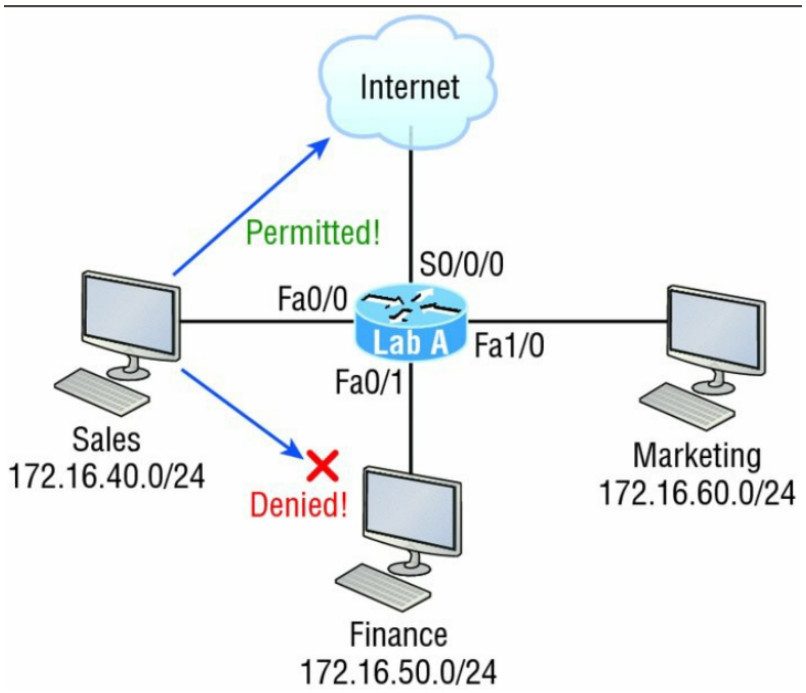
Note: while working with block sizes and wildcards

- **Each block size must start at 0 or a multiple of the block size**. For example, you can't say that you want a block size of 8 and then start at 12. You must use 0-7, 8-15, 16-23, etc. For a block size of 32, the ranges are 0-31, 32-63, 64-95, etc.
- The command **`any`** is the same thing as writing out the wildcard; 0.0.0.0 255.255.255.255.

Standard Access List Example 1

Use a standard access list to stop specific users from gaining access to the Finance department LAN.

Standard access list topology



Standard access list configuration

In Figure, router **Lab_A** 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.

The standard IP access list configuration on the router:

```
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
```

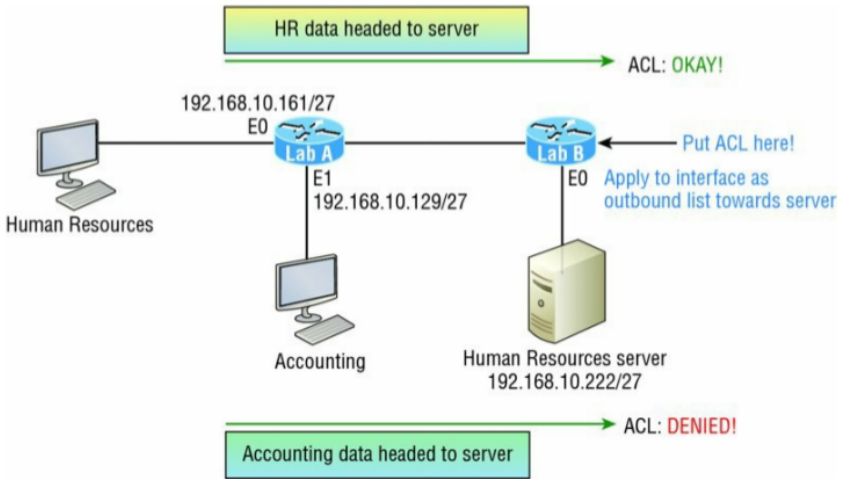
Applying standard access list at the interface

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

Standard Access List Example 2

The below Figure shows an internetwork of two routers with four LANs. Write a standard ACL 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.

Standard access list topology



Standard access list configuration

```
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
```

Ethernet 0 (**E0**) is the outbound interface on the **Lab_B** router and here's the access list that should be placed on it:

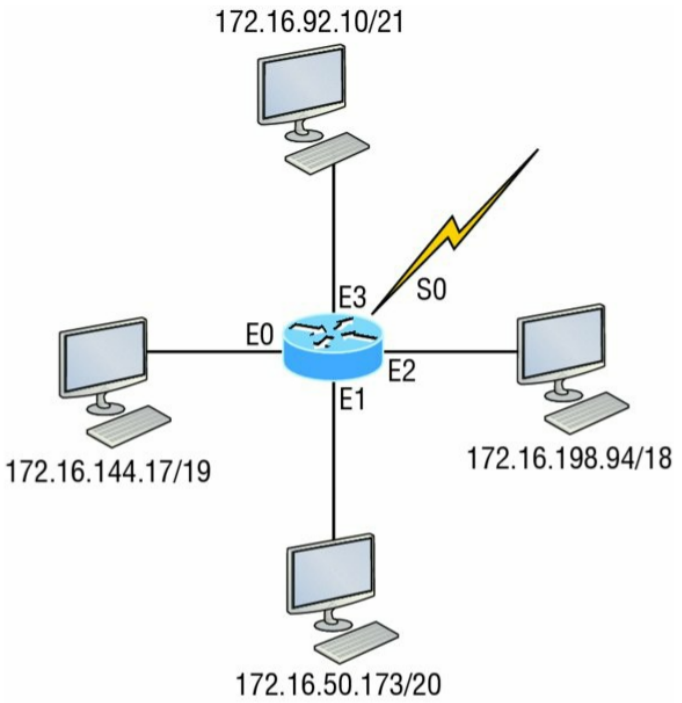
```
Lab_B(config)#interface Ethernet 0
Lab_B(config-if)#ip access-group 10 out
```

The accounting subnet is 192.168.10.128/27 with subnet mask 255.255.255.224 and a block size of 32 in the fourth octet.

Standard Access List Example 3

In the below Figure, a router with four LAN connections and one WAN connection to the Internet. Write an access list that will stop access from each of the four LANs shown in the diagram to the Internet. Each of the LANs reveals a single host's IP address, which is needed to use to determine the subnet and wildcards of each LAN to configure the access list.

Standard ACL topology



Standard ACL at Router R

```
R#config t
R(config)#access-list 1 deny 172.16.128.0 0.0.31.255
R(config)#access-list 1 deny 172.16.48.0 0.0.15.255
R(config)#access-list 1 deny 172.16.192.0 0.0.63.255
R(config)#access-list 1 deny 172.16.88.0 0.0.7.255
R(config)#access-list 1 permit any
```

Serial 0 (**S0**) is the outbound interface on the router, **R**,

and he access list is applied on it:

```
R(config)#interface serial 0
R(config-if)#ip access-group 1 out
```

Extended Access Lists

- Extended ACLs allow us to specify source and destination addresses as well as the protocol and port number that identify the upper-layer protocol or application.
- Extended access-list range from 100-199 or 2000-2699.
- Based on the number used when the access list is created, the router knows which type of syntax to expect as the list is entered.
- After choosing a number in the extended range, you need to decide what type of list entry to be made.

Standard access list command

```
Router(config)#access-list ?
Router(config)#access-list 110 ?
..#access-list 110 deny ?
..#access-list 110 deny tcp ?
..#access-list 110 deny tcp any host 172.16.30.2 ?
..#access-list 110 deny tcp any host 172.16.30.2
eq ?
..#access-list 110 deny tcp any host 172.16.30.2
eq 23
..#access-list 110 permit ip any any
```

Apply:

```
..#ip access-group 110 in
```

or `..#ip access-group 110 out`

Description:

➡ Displays access-list number ranges to be used to filter traffic.

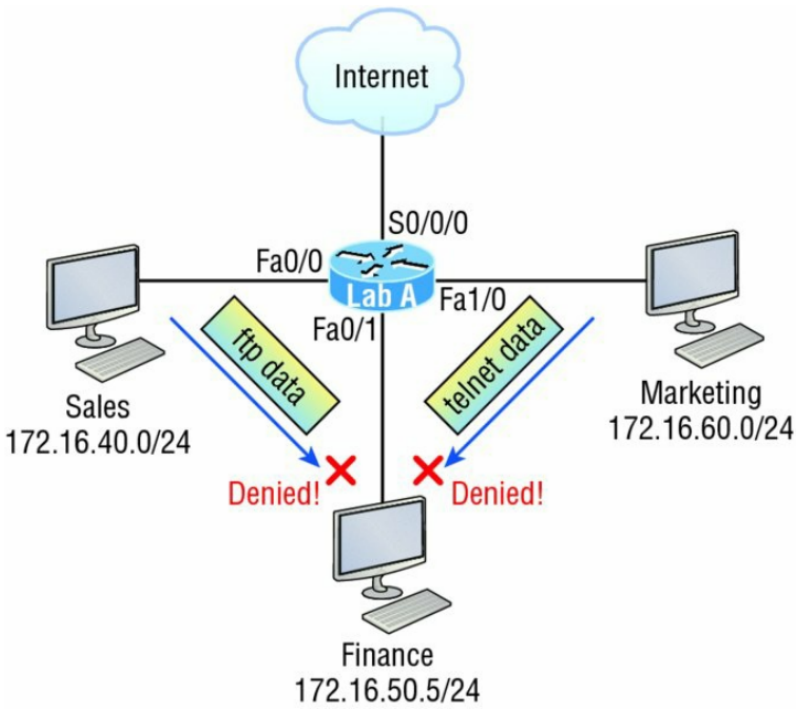
```
➡deny        Specify packets to reject
  dynamic    Specify a DYNAMIC list of
             PERMITs or DENYs
  permit     Specify packets to forward
  remark     Access list entry comment

➡tcp   Transmission Control Protocol
  udp   User Datagram Protocol
  icmp  Internet Control Message Protocol
  ip    Any Internet Protocol
  ..............................
```

➡ purpose to block Telnet (port 23) to host 172.16.30.2 only.

Extended Access List Example 1

We need 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.

Extended access list topology



Extended access list configuration

Configuration on the router Lab_A:

```
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
```

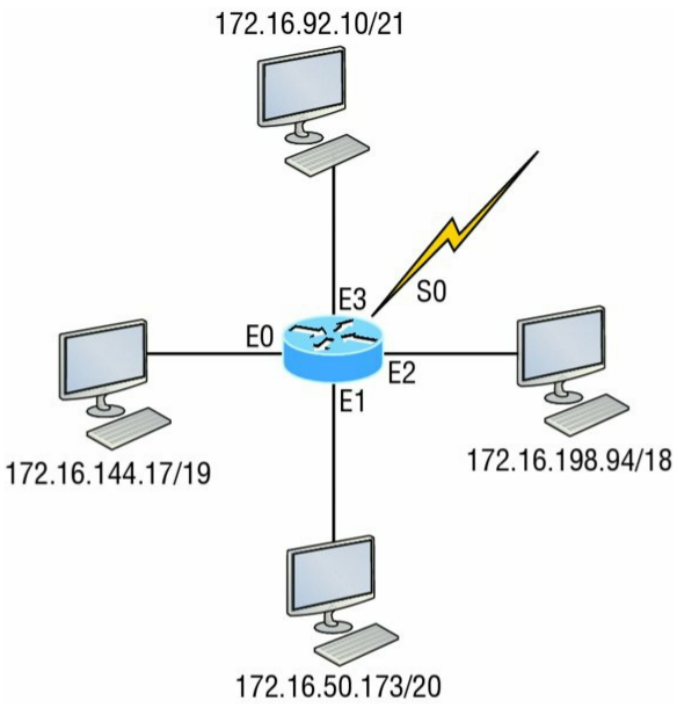
Applying Extended access list at the interface:

```
Lab_A(config)#int fa0/1
Lab_A(config-if)#ip access-group 110 out
```

Extended Access List Example 2

Consider the below Fgure, which has four LANs and a serial connection. We need to prevent Telnet access to the networks attached to the E1 and E2 interfaces.

Extended access list topology



Extended access list configuration

Configuration on the router R:

```
R#config t
R(config)#access-list 110 deny tcp any 172.16.48.0
0.0.15.255 eq 23
R(config)#access-list 110 deny tcp any 172.16.192.0
0.0.63.255 eq 23
R(config)#access-list 110 permit ip any any
```

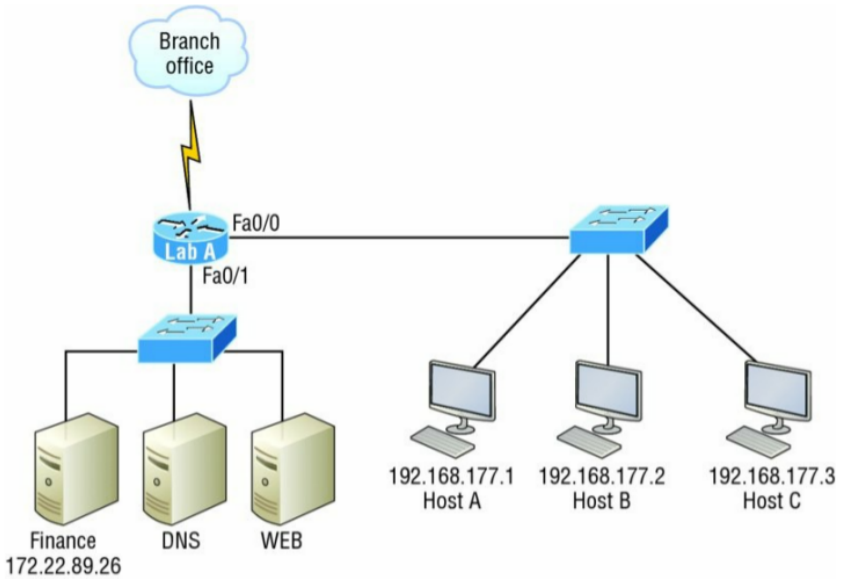
Applying Extended access list at the interface:

```
R(config)#interface Ethernet 1
R(config-if)#ip access-group 110 out
R(config)#interface Ethernet 2
R(config-if)#ip access-group 110 out
```

Extended Access List Example 3

In this case, configre the extended ACL to allow **HTTP** access to the **Finance server** from source **Host B** only. All other traffic will be permitted.

Extended access list topology



Extended access list configuration

Configuration on the router Lab_A:

```
R#config t
Lab_A(config)#access-list 110 permit tcp host
192.168.177.2 host 172.22.89.26 eq 80
Lab_A(config)#access-list 110 deny tcp any host
172.22.89.26 eq 80
Lab_A(config)#access-list 110 permit ip any any
```

Applying Extended access list at the interface:

```
Lab_A(config)#interface fastethernet 0/1
Lab_A(config-if)#ip access-group 110 out
```

NOTE: Generally extended access list is applied closest to the source. In this case it is required to allow only HTTP traffic to the Finance server from Host B. If the ACL is applied to inbound on Fa0/0 interface, then the branch office would be able to access the Finance server and perform HTTP. So it is needed to place the ACL closest to the destination.

Named ACLs

- Named access lists are just another way to create standard and extended access lists.
- This allow us to use names for creating and applying either standard or extended access lists.
- Lines can be added or deleted to named ACLs.

Named ACLs Synatx

```
Router(config)#ip access-list ?
Router(config)#ip access-list standard ?
Router#ip access-list standard <ACL_name>
Router(config-std-nacl)#
Router(config-std-nacl)#?
Router(config-std-nacl)#deny ?
Router(config-std-nacl)#permit ?
```

Apply:

```
Router#config t
Router(config)#interface fa0/1
...(config-if)#ip access-group <ACL_name> in|out
```

Description:

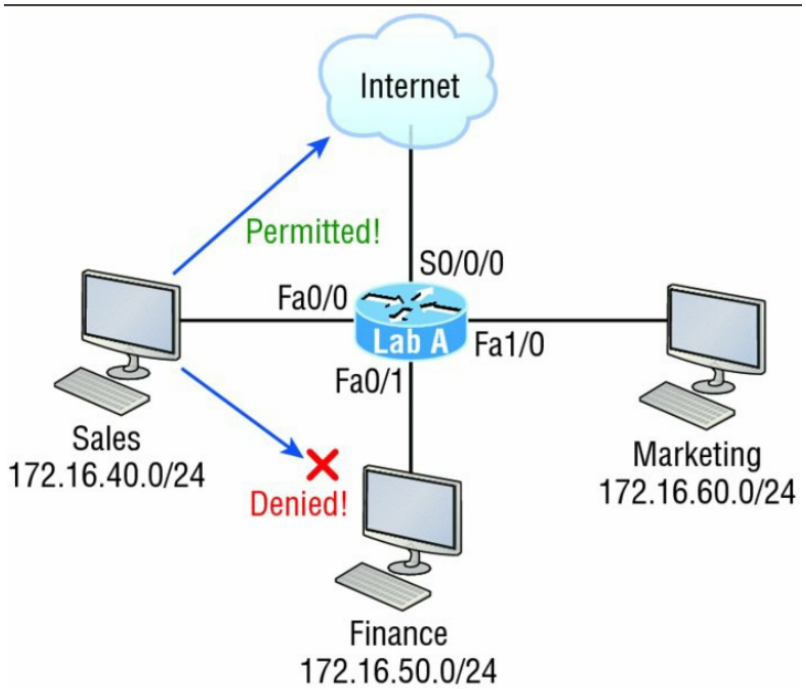
➡ Command ***ip access list*** allows to enter a named acl.

```
➡   extended      Extended Access List
    standard      Standard Access List
    ..........................

➡  <1-99>       Standard IP access-list no
   <1300-1999>  Expanded range ACls
   WORD         Access-list name
  ..........................

➡  Standard Access List configuration cmds:
deny      Specify packets to reject
permit    Specify packets to forward
no        Negate a command
default   Set a command to its defaults
exit      Exit from acl configuration mode
  ..........................
```

Named ACLs Example 1

Create a named access list to stop specific users from gaining access to the Finance department LAN.

Standard access list topology



Standard access list configuration

Named ACLs configuration on the router:

```
Lab_A#config t
Lab_A(config)#ip access-list standard BlockSales
Lab_A(config-std-nacl)#deny 172.16.40.0
0.0.0.255
Lab_A(config-std-nacl)#permit any
Lab_A(config-std-nacl)#exit
```

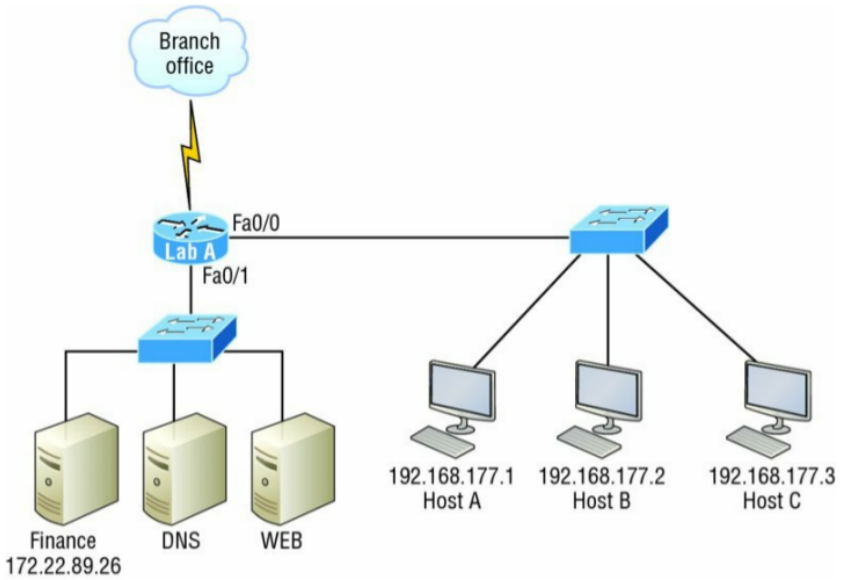
Applying Extended access list at the correct interface:

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

Named ACLs Example 2

In this case, configre the named ACL to allow **HTTP** access to the **Finance server** from source **Host B** only. All other traffic will be permitted.

Extended access list topology



Extended access list configuration

Configuration on the router Lab_A:

```
Lab_A#config t
Lab_A(config)#ip access-list extended 110
Lab_A(config-ext-nacl)#permit tcp host
192.168.177.2 host 172.22.89.26 eq 80
Lab_A(config-ext-nacl)#deny tcp any host
172.22.89.26 eq 80
Lab_A(config-ext-nacl)#permit ip any any
```

Applying Extended access list at the interface:

```
Lab_A(config)#int fa0/1
Lab_A(config-if)#ip access-group 110 out
```

Remarks

- It arms the ability to include comments regarding the entries made in both IP standard and extended ACLs.
- They efficiently increase the ability to examine and understand ACLs.
- It cab be placed either before or after a `permit` or `deny` statement.

Remarks in ACLs

```
Router#config t
Router(config)#access-list 110 remark Permit Bob from Sales Only To Finance
Router(config)#access-list 110 permit ip host 172.16.40.1 172.16.50.0 0.0.0.255
Router(config)#access-list 110 deny ip 172.16.40.0 0.0.0.255 172.16.50.0 0.0.0.255
Router(config)#ip access-list extended No_Telnet
Router(config-ext-nacl)#remark Deny all of Sales from Telnetting to Marketing
Router(config-ext-nacl)#deny tcp 172.16.40.0 0.0.0.255 172.16.60.0 0.0.0.255 eq 23
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#do show run
```

```
[output cut]
!
ip access-list extended No_Telnet
  remark Stop all of Sales from Telnetting to Marketing
  deny tcp 172.16.40.0 0.0.0.255 172.16.60.0 0.0.0.255 eq telnet
  permit ip any any
!
access-list 110 remark Permit Bob from Sales Only To Finance
access-list 110 permit ip host 172.16.40.1 172.16.50.0 0.0.0.255
access-list 110 deny
ip 172.16.40.0 0.0.0.255 172.16.50.0 0.0.0.255
access-list 110 permit ip any any
!
```

Monitoring Access Lists

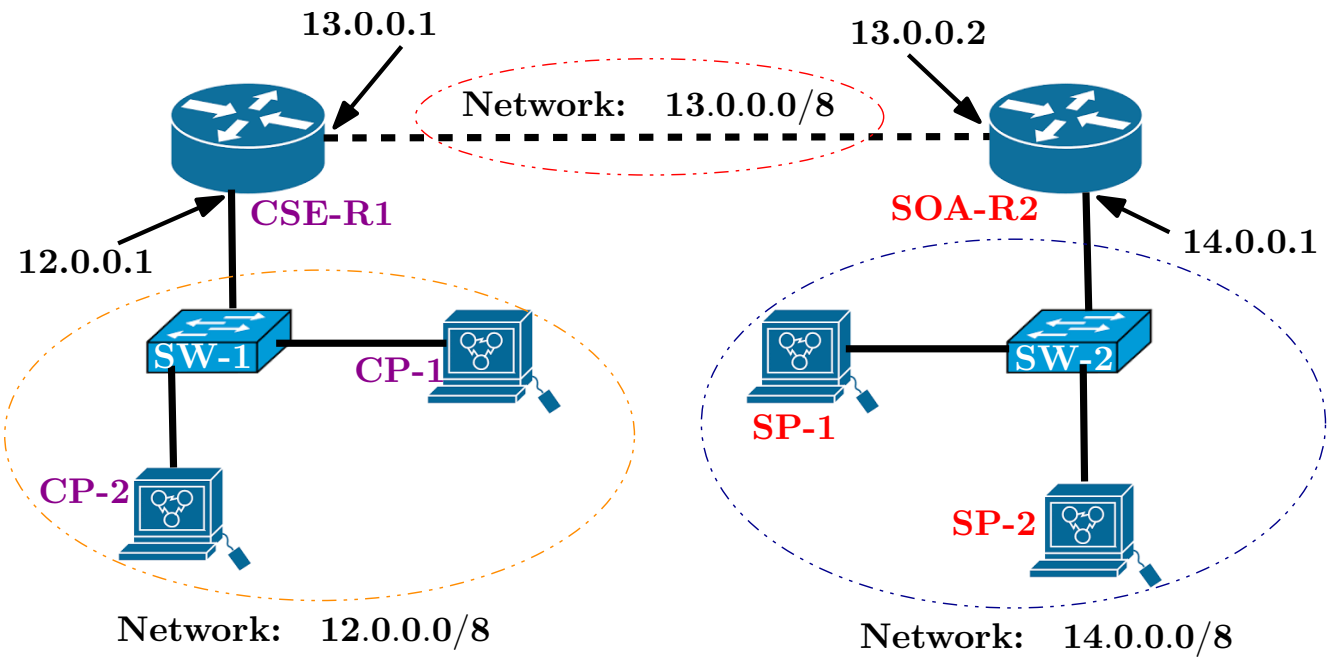
Command	Effect
`show access-list`	Displays all access lists and their parameters configured on the router. Also shows statistics about how many times the line either permitted or denied a packet. This command does not show you which interface the list is applied on.
`show access-list 110`	Reveals only the parameters for 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.

Example Monitor ACL

```
Lab_A#show access-list
Standard IP access list 10
  10 deny 172.16.40.0, wildcard bits 0.0.0.255
  20 permit any
Standard IP access list BlockSales
  10 deny 172.16.40.0, wildcard bits 0.0.0.255
  20 permit any
;;;;;;;;;;;;
```

Exercise on ACLs

ACLs Configuration



- Create a standard access list to block the network 12.0.0.0 to gain access 14.0.0.0 network.
- Create an extended access list to block the host **CP-2** to telnet **SW-2**.
- Create a named access list to block the network 12.0.0.0 to gain access 14.0.0.0 network.

Review Questions

1. Which of the following statements is false when a packet is being compared to an access list?
   (A) It's always compared with each line of the access list in sequential order.
   (B) Once the packet matches the condition on a line of the access list, the packet is acted upon and no further comparisons take place.
   (C) There is an implicit deny at the end of each access list.
   (D) Until all lines have been analyzed, the comparison is not over.

2. You need to create an access list that will prevent hosts in the network range of 192.168.160.0 to 192.168.191.0. Which of the following lists will you use?
   (A) access-list 10 deny 192.168.160.0 255.255.224.0
   (B) access-list 10 deny 192.168.160.0 0.0.191.255
   (C) access-list 10 deny 192.168.160.0 0.0.31.255
   (D) access-list 10 deny 192.168.0.0 0.0.31.255

3. You have created a named access list called BlockSales. Which of the following is a valid command for applying this to packets trying to enter interface Fa0/0 of your router?
   (A) (config)#ip access-group 110 in
   (B) (config-if)#ip access-group 110 in
   (C) (config-if)#ip access-group Blocksales in
   (D) (config-if)#BlockSales ip access-list in

4. Which access list statement will permit all HTTP sessions to network 192.168.144.0/24 containing web servers?
   (A) access-list 110 permit tcp 192.168.144.0 0.0.0.255 any eq 80
   (B) access-list 110 permit tcp any 192.168.144.0 0.0.0.255 eq 80
   (C) access-list 110 permit tcp 192.168.144.0 0.0.0.255 192.168.144.0 0.0.0.255 any eq 80
   (D) access-list 110 permit udp any 192.168.144.0 eq 80

5. What router command allows you to determine whether an IP access list is enabled on a particular interface?
   (A) show ip port
   (B) show access-lists
   (C) show ip interface
   (D) show access-lists interface

THANK YOU