Lab 5.1.1b Access Control List Implementation

v1.1

Introduction

An Access List is a list of conditions that categorize packets, and are helpful when needing to control network traffic. Access Lists filter unwanted packets when implementing security policies. Once the lists are built, then they can be applied to either inbound, or outbound, traffic on any interface. Applying Access Lists causes the router to analyze every packet crossing that interface in the specified direction and take the appropriate action.

Objectives

In this project/lab the student will complete two labs: Standard IP Access List and Extended IP Access List

Part 1: Verify Network Connectivity
Part 2: Apply, Verify, and Remove a Standard ACL
Part 3: Configure, Apply and Verify Standard ACL
Part 4: Configure, Apply and Verify Extended ACL

Assignment

Create and apply a Standard IP Access List and an Extended IP Access List to permit/deny traffic.

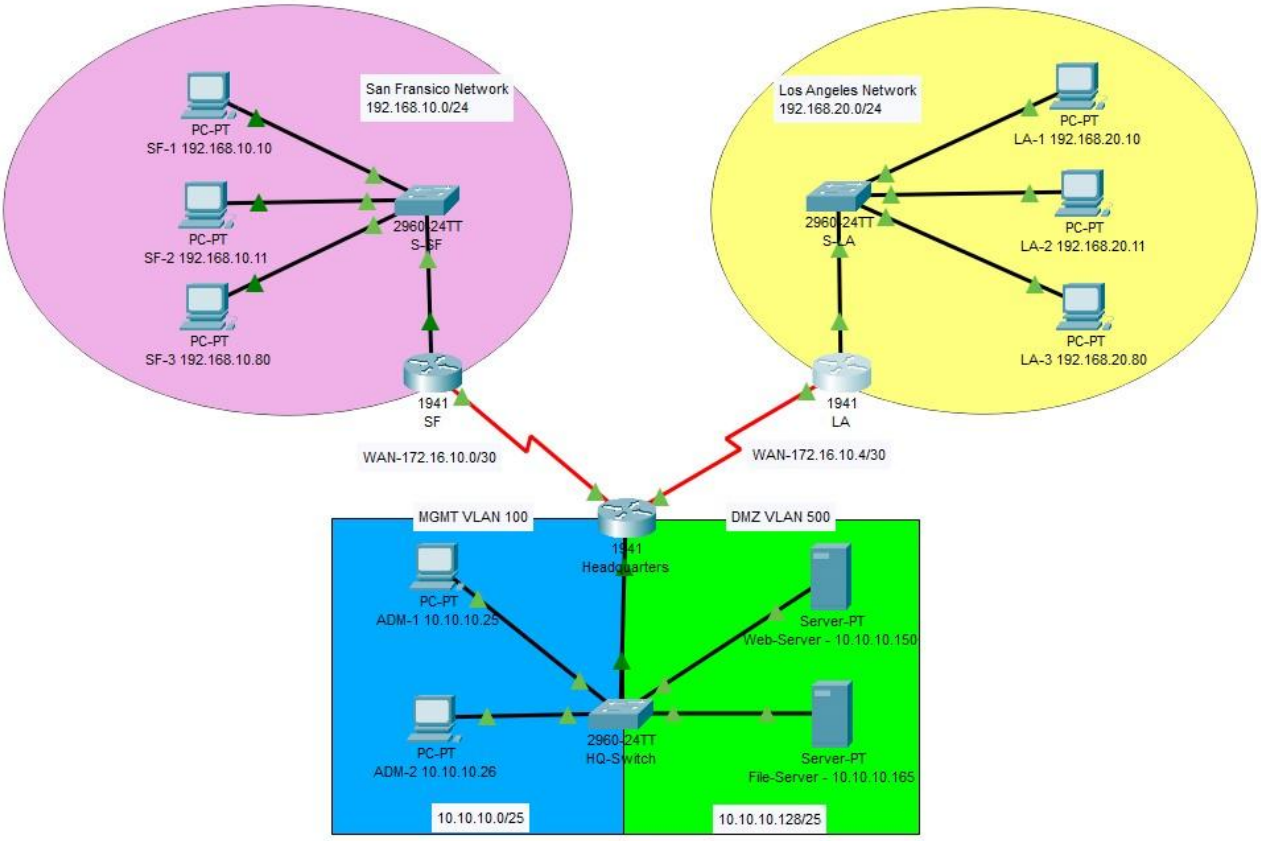
Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4) M3 universal image or comparable)
- 3 Cisco 2960 Switches (Software (C2960-LANBASE-M), Version 12.2)
- 8 Pc's and 2 servers
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

If working online:

- Your Computer workstation
- Cisco Packet Tracer (online)
- Provided Packet Tracer File

Topology



Addressing Table

Device	Interface	IP Address	Default Gateway
HQ	G0/0.100	10.10.10.1/25	n/a
	G0/0.500	10.10.10.129/25	n/a
	S0/0/0	172.16.10.1/30	n/a
	S0/0/1	172.16.10.5/30	n/a
SF	G0/0	192.168.10.1/24	n/a
	S0/0/0	172.16.10.2/30	n/a
LA	G0/0	192.168.20.1/24	n/a
	S0/0/1	172.16.10.6/30	n/a

ADMIN-1	NIC	10.10.10.25/25	10.10.10.1
ADMIN-2	NIC	10.10.10.26/25	10.10.10.1
Web Srvr	NIC	10.10.10.145/25	10.10.10.129
File Srvr	NIC	10.10.10.165/25	10.10.10.129
SF-1	NIC	192.168.10.10/24	192.168.10.1
SF-2	NIC	192.168.10.11/24	192.168.10.1
SF-3	NIC	192.168.10.150/24	192.168.10.1
LA-1	NIC	192.168.20.20/24	192.168.20.1
LA-2	NIC	192.168.20.21/24	192.168.20.1
LA-3	NIC	192.168.20.150/24	192.168.20.1

Procedure

Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information in a text file.

Part 1: Verify Network Connectivity

Step 1:Ping devices to verify full connectivity between the networks. Ping to and from the stated networks below using any end device in each network.

Pink Network to **Blue** Network

Pink to **Green**

Pink to **Yellow**

Blue to **Green**

Blue to **Yellow**

Green to **Yellow**

Congrats! You have now verified layer 1 through 3 are fully functional ***and*** there is no policy currently filtering ICMP messages blocking connectivity between the two networks

Part 2: Apply, Verify and Remove a Standard ACL.

Step 1: Use show commands to investigate the ACL configuration.

Use the **show run** and **show access-lists** commands to view the currently configured ACLs. To quickly view the current ACLs, use **show access-lists**.

a. Enter the **show access-lists** command, followed by a space and a question mark (?) to view the available options:

```
LA#show access-lists ?

<1-199>  ACL number
WORD     ACL name
<cr>
```

If you know the ACL number or name, you can filter the **show** output further. However, **LA** has only one ACL; therefore, the **show access-lists** command will suffice.

```
LA#show access-lists

Standard IP access list 11
        10 deny 192.168.10.0 0.0.0.255
        20 permit any
```

The first line of the ACL prevents any packets originating in the **192.168.10.0/24** network, which includes Internet Control Message Protocol (ICMP) echoes (ping requests). The second line of the ACL allows all other **ip** traffic from **any** source to transverse the router.

b. For an ACL to impact router operation, it must be applied to an interface in a specific direction. In this scenario, the ACL is used to filter traffic exiting an interface. Therefore, all traffic leaving the specified interface of R1 will be inspected against ACL 11. **c.**

Note: Although you can view IP information with the **show ip interface** command, it may be more efficient in some situations to simply use the **show run** command.

Step 2: Apply the standard ACL to a specified interface

For the ACL to actually filter traffic, it must be applied to some router operation. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.

```
LA(config)# interface GigabitEthernet0/0
LA(config-if)# ip access-group 11 out
```

Although you can view IP information with the **show ip interface** command, it may be more efficient in some situations to simply use the **show run** command.

Using one or both of these commands, to which interface and direction is the ACL applied? Int g0/0 out

Step 3: Ping devices on remote networks to test ACL functionality.

a. From the command prompt of any PC in the **Pink** network, ping the **Yellow** network.

b. From the command prompt of any PC in the **Blue** network, ping the **Yellow** network.

Why did the first pings fail? We are denying access from network 192.168.10.0 to our 192.168.20.0 network using ACL (**Hint:** Use simulation mode or view the router configurations to investigate.)

The pings fail because the LA router is configured with an ACL to deny any ping from the 192.168.10.0 network exiting the G0/0 interface.

Step 4: Remove access list 11 from the configuration, and repeat the test.

You can remove ACLs from the configuration by issuing the **no access list** [*number of the ACL*] command. The **no access-list** command deletes all ACLs configured on the router. The **no access-list** [*number of the ACL*] command removes only a specific ACL.

a. Under the Gigabitethernet 0/0 interface, remove access-list 11 previously applied to the interface as an **outgoing** filter:

```
LA(config)# int G0/0
LA(config-if)#no ip access-group 11 out
```

b. In global configuration mode, remove the ACL by entering the following command:

```
LA(config)# no access-list 11
```

c. Verify that the **Pink** network can now ping the **Yellow** network.

If the pings fails, troubleshoot the issue and verify the ACL was removed from the LA router.

Part 3: Configure, Apply and Verify Standard ACL

Step 1: Evaluate two network policies and planned ACL implementations.

a. The following network policies need to be implemented on **HQ(Headquarters)** router:

- The Office Manager PC's in both the San Francisco 192.168.10.150 **Pink** location and Los Angeles 192.168.20.150 **Yellow** location, as well as the Admin PCs on 10.10.10.0/25 **Blue** are the only devices allowed to access the DMZ 10.10.10.128/25 **(Green)** network. ● All other access is denied.

To allow access from the above stated device to the **DMZ** at 10.10.10.165 without interfering with other traffic, an ACL must be created on **HQ** router. The access list must be placed on the outbound interface to the **FileServer**. A second rule must be created on **HQ** to permit all other traffic.

b. The following network policies need to be implemented on **all routers**:

Only the admin network is allowed to log into company routers.

- The 10.10.10.0/25 network is allowed to log into the **LA**,**SF** and **HQ** routers
- All other access is denied

To allow access from the 10.10.10.0/25 network to each router.. The ACL must be placed inbound on the vty lines.

Step 2: Configure and apply a numbered standard ACL on the HeadQuarters router.

a. Create an ACL using the number 30 on the **HQ** router with a statement that allows access to the **DMZ** from the office manager PC's in both the San Francisco 192.168.10.150 **Pink** location and Los Angeles 192.168.20.150 **Yellow** location, as well as the Admin PC's on 10.10.10.0/25 **Blue**, these are the only devices allowed to access the **DMZ** 10.10.10.128/25 **Green** network.

By default, an access list denies all traffic that does not match any rules. To permit all other traffic, configure the following statements:

```
HQ(config)#access-list 30 permit host 192.168.20.150
HQ(config)#access-list 30 permit host 192.168.10.150
HQ(config)#access-list 30 permit 10.10.10.0 0.0.0.127
```

For the ACL to actually filter traffic, it must be applied to some router operation. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.

```
HQ(config)# interface G0/0.500
HQ(config-if)# ip access-group 30 out
```

Step 3 : Configure and apply a numbered standard ACL ***on all 3 routers***.

a. Create an ACL that will only allow PCs from the admin network (10.10.10.0/25 **Blue**) to telnet into each of the 3 company routers (LA, SF and HQ).

b. By default, an access list denies all traffic that does not match any rules. To permit all other traffic, configure the following statements:

```
HQ(config)#access-list 50 remark Telnet Access for Admins Only
HQ(config)#access-list 50 permit 10.10.10.0 0.0.0.127
```

Note: You can use the **remark** command in any of the IP numbered standard. IP numbered extended or named ACLs

The **remark** command allows you to include a comment. (Limited to a 100 characters)

You can use the **remark** command before or after a **permit** or **deny** statement.

When restricting access through Telnet, use the **access-class** command rather than the **access-group** command, which is used when applying an ACL to a physical interface.

Use following commands to apply the ACL to all 5 vty virtual interfaces in an inbound direction.

```
HQ(config)#line vty 0 4
HQ(config)#access-class 50 in
```

Configure and apply the standard ACL *on all 3 routers*.

Caution: *Do not apply* an ACL intending to restrict telnet traffic on a physical interface. If you apply an ACL to a physical interface, *all packets are compared to the ACL* before it can continue on to its destination. This scenario can lead to a large reduction in performance.

Step 4: Verify your ACL implementation is working correctly,

a. Verify ACL **30** is working correctly by doing the following: Open a command prompt on SF-3 Office Manager PC and verify that you can communicate with the DMZ 10.10.10.128/25 **Green** network by issuing a ping command to the file server.

```
C:\>ping 10.10.10.165

Pinging 10.10.10.165 with 32 bytes of data:
Request timed out.

Reply from 10.10.10.165: bytes=32 time=1ms TTL=126
Reply from 10.10.10.165: bytes=32 time=2ms TTL=126
Reply from 10.10.10.165: bytes=32 time=2ms TTL=126
Ping statistics for 10.10.10.165:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Your ping should be successful. If not, troubleshoot your network until fixed.

b. Open a command prompt on SF-1 or SF-2 PCs and verify that you **cannot** communicate with the DMZ **Green** by issuing a ping command to the file server.

```
C:\>ping 10.10.10.165
Pinging 10.10.10.165 with 32 bytes of data:
Request
timed out.
Request
timed out.
Request
timed out.
Request
timed out.
Ping    statistics
for
10.10.10.165:
Packets: Sent = 4,
Received = 0, Lost
= 4 (100% loss),
```

Note: The pings from the SF-1 and SF-2 PC were unsuccessful because these system's ip addresses were not specified in the ACL. They were blocked due to the implicit deny statement that is at the end of every ACL.

Step 5: Verify ACL **50** is working properly by doing the following: From a PC in the admin network open a command prompt (Desktop Tab) and use the **Telnet** command and any ip address of any active interface on the router you are wanting to Telnet. In the example we used PC ADM-1 to telnet to the LA router.

```
C:\>telnet 172.16.10.6

Trying 172.16.10.6 ...Open
User Access Verification
Username:
admin
Password:
LA>

[Connection to
172.16.10.6
closed by foreign
host]
C:\>
```

Next telnet to a router from any PC not in the admin network. In the example below, we used PC LA-3 to try and telnet to the LA router. Notice the Telnet connected is refused by the LA router.

```
C:\>telnet 172.16.10.6
Trying 172.16.10.6 ...
% Connection refused by remote host
C:\>
```

Part 4: Configure, Apply and Verify Extended ACL

Step 1: Configure and apply a numbered extended ACL on the San Francisco router.

In the 1st extended ACL we want to deny access of the San Francisco **(Pink)** office pc's (Not including the Manager) from communicating with the LA **(Yellow)** Office systems. *Permit all other traffic*. Because the San Francisco office is expecting to hire 10 more employees, it has been decided to block the following range of addresses in the San Francisco network. Deny range 192.168.10.5 - 192.168.10.20 from accessing network 192.168.20.0/24

Note: To find the correct wildcard mask to isolate ip addresses 192.168.10.5 through 192.168.10.20. You need to subtract the lowest ip address from the highest ip address in the range.

```
192. 168. 10. 20
192. 168. 10.  5
  0.   0.  0. 15
```

This will be the wildcard mask we will use in our ACE (Access Control List Entry)

SF(config)# **access-list 101 deny ip 192.168.10.5 0.0.0.15 192.168.20.0 0.0.0.255** SF(config)# **access-list 101 permit ip any any**

Step 2: Configure and apply a numbered extended ACL on the San Francisco

SF(config)# **int G0/0**
SF(config-if)# **ip access-group 101 in**

Reflection Questions

1. Troubleshoot this ACL statement -

On the LA router, if placed inbound on the LAN interface will the following ACL deny the LA network from accessing the San Francisco network. If not, what would need to be changed? LA(config)# **access-list 130 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255** **Yes it will deny the LA network from reaching the san Francisco network**

Submit Your Work:

Submit all text files, screenshots, or answers to questions to your instructor.
Embed any content into this document for each grading. Thanks!

Packet Tracer:
Submit Packet Tracer file as well as your text file with your findings and notes.

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1:Verify and Remove a Standard ACL. (5 pts)	Verify and Remove a Standard ACL 11 from the LA router. (5 pts)
	Criteria #2: Configure, apply and verify standard ACLs on HQ router (30 pts)	Configure, apply and verify 2 standard ACLs on HQ router (30 pts) ACL 30 - Access to DMZ (15 pts) ACL 50 - Telnet access to routers
	Criteria #3: Configure, apply and verify standard ACLs on LA router (30 pts)	Configure, apply and verify 2 standard ACLs on HQ router (30 pts) ACL 50 - Telnet access to routers

	Criteria #4: Configure, apply and verify standard ACLs on SF router (30 pts)	Configure, apply and verify 2 standard ACLs on HQ router (30 pts) ACL 101 - Deny access from SF Office to LA Office systems. ACL 50 - Telnet access to routers
	Criteria #5: Submit instructions document with lab questions completed. (5 pts)	Criteria #5: Submit instructions document with lab questions completed. (5 pts)