Alan Palayil

ECE 407

ECE 407

Introduction to Computer Networks Laboratory

Practice 8 – Access Control Lists

Objectives

The goal of this experiment is to:

1. Familiarize students with named and numbered standard Access Control Lists (ACLs).
2. Familiarize students with named and numbered extended ACLs.

Background[1]

As a form of network security, administrators use Access Control Lists (ACLs) on routers to stop or permit traffic based on criteria from the packet header. An ACL is a sequential list of permit or deny statements that apply to addresses (source IP address, destination IP address) or upper-layer protocols (TCP/UDP source port, TCP/UDP destination port). Such information is extracted from the packet header, and tested against the rules of the ACL before a decision (whether to permit or deny traffic) is made.

A general rule for applying ACLs on a router can be recalled by remembering "the three Ps". You can configure one ACL per protocol, per direction, per interface:

- One ACL per protocol: to control traffic flow on an interface, an ACL must be defined for each protocol (e.g. IP, IPX, AppleTalk) enabled on the interface.
- One ACL per direction: ACLs control traffic in one direction at a time on an interface. Two separate ACLs must be created to control inbound and outbound traffic. Inbound ACLs are applied on incoming packets, and are processed before packets are routed to the outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet is discarded. If the packet is permitted by the tests, it is then processed for routing. Outbound ACLs are applied on incoming packets after they are routed to the outbound interface.
- One ACL per interface: ACLs control traffic for an interface, for example, Fast Ethernet 0/0.

[1] Source: http://ictechnotes.blogspot.com/2011/07/acls.html

ACL statements operate in a sequential order. They evaluate packets against the ACL, from the top, one statement at a time. If a packet header and an ACL statement match, the rest of the statements in the list are skipped, and the packet is permitted or denied as determined by the matched statement. If a packet header does not match an ACL statement, the packet is tested against the next statement in the list. This matching process continues until the end of the list is reached.

A final implied statement, also known as the “implicit deny any statement" or the "deny all traffic" statement, covers all packets which did not match any previous statement, and results in denial of the packet. Because of this statement, an ACL should have at least one permit statement in it; otherwise, the ACL blocks all traffic.

There are two types of Cisco ACLs, standard and extended;

1. **Standard ACLs: s**tandard ACLs allow you to permit or deny traffic from source IP addresses. The destination of the packet and the ports involved do not matter.

   Example: *access-list 10 permit 192.168.30.0 0.0.0.255*

   The example allows all traffic from network 192.168.30.0/24 network. Because of the implied "deny any" at the end, all other traffic is blocked with this ACL. Standard ACLs are created in global configuration mode.

2. **Extended ACLs:** extended ACLs filter IP packets based on several attributes, for example, protocol type, source and destination IP address, destination IP address, source TCP or UDP ports, destination TCP or UDP ports, and optional protocol type information for finer granularity of control.

   Example: *access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80*

   ACL 103 permits traffic originating from any address on the 192.168.30.0/24 network to any destination host port 80 (HTTP). Extended ACLs are created in global configuration mode.

Numbering and Naming of ACLs

Using numbered ACLs is an effective method for determining the ACL type on smaller networks with more homogeneously defined traffic. However, a number does not inform you of the purpose of the ACL. For this reason, you can use a name to identify a Cisco ACL. The rule to designate numbered ACLs and named ACLs is:

1. **Numbered ACL:** assign a number based on which protocol you want to filter,
   - (1 to 99) and (1300 to 1999): Standard IP ACL
   - (100 to 199) and (2000 to 2699): Extended IP ACL

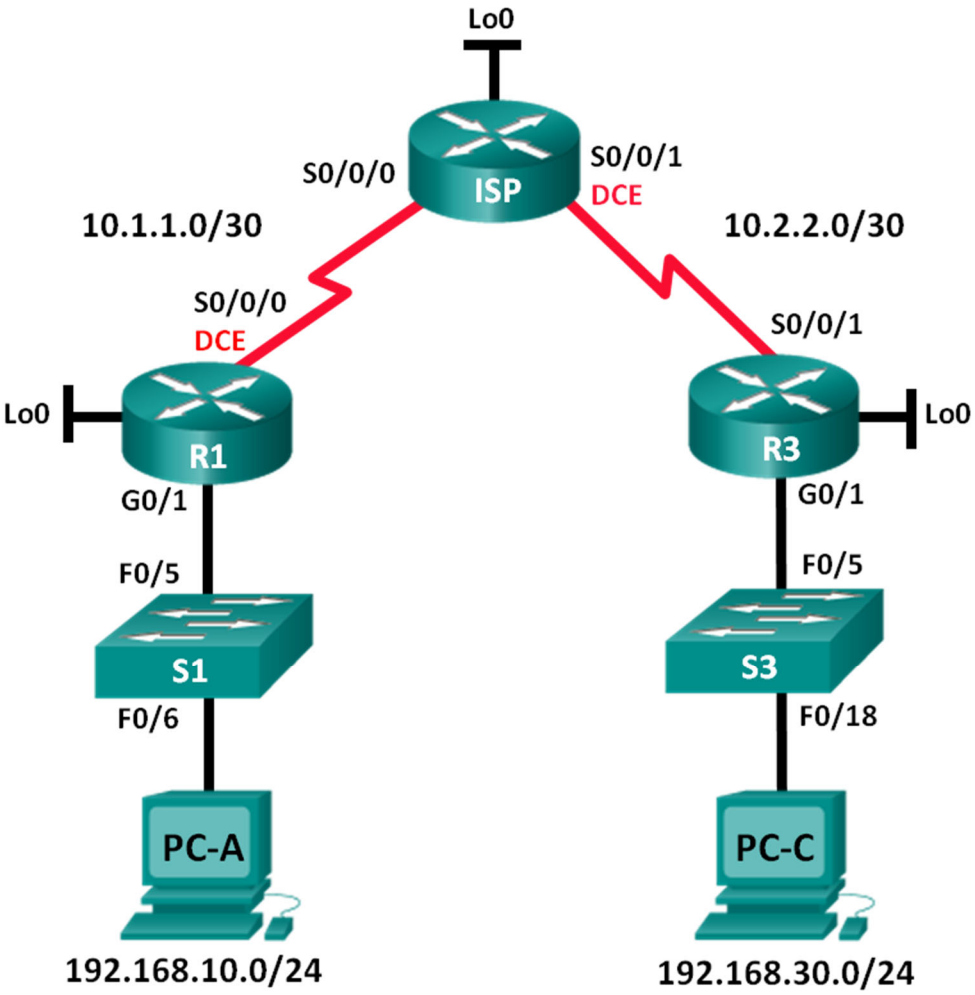
2. **Named ACL:** assign a name by providing the name of the ACL. Names can contain alphanumeric characters. Names cannot contain spaces or punctuation and must begin with a letter. With named ACLs, you can add or delete entries within the ACL.

The proper placement of an ACL to filter undesirable traffic makes the network operate more efficiently. For example, traffic that will be denied at a remote destination should not use network resources along the route to that destination. Every ACL should therefore be placed where it has the greatest impact on efficiency. The basic rules are:

- Locate extended ACLs as close as possible to the source of the traffic denied. This way, undesirable traffic is filtered without crossing the network infrastructure.
- Because standard ACLs do not specify destination addresses, place them as close to the destination as possible.

Exercise 1: Configuring and Verifying Standard IPv4 ACLs (7.2.2.6)

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A

	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Scenario

Network security is an important issue when designing and managing IP networks. The ability to configure proper rules to filter packets, based on established security policies, is a valuable skill. In this exercise, you will set up filtering rules for two offices represented by R1 and R3. Management has established some access policies between the LANs located at R1 and R3, which you must implement. The ISP router sitting between R1 and R3 will not have any ACLs placed on it. You would not be allowed any administrative access to an ISP router because you can only control and manage your own equipment.

A. Set Up the Topology and Initialize Devices using Cisco Packet Tracer

B. Configure Devices and Verify Connectivity

Configure basic settings on the routers, switches, and PCs. Refer to the Topology and Addressing Table for device names and address information.

Step 1: Configure IP addresses on PC-A and PC-C.

Step 2: Configure basic settings for the routers.

a. Console into the router and enter global configuration mode.

b. Copy the following basic configuration and paste it to the running-configuration on the router.

no ip domain-lookup

hostname R1

service password-encryption

enable secret class

banner motd #

Unauthorized access is strictly prohibited. #

Line con 0

password cisco

login

logging synchronous

line vty 0 4

password cisco

login

c. Configure the device name as shown in the topology.
d. Create loopback interfaces on each router as shown in the Addressing Table.
e. Configure interface IP addresses as shown in the Topology and Addressing Table.
f. Assign a clock rate of **128000** to the DCE serial interfaces.
g. Enable Telnet access.
h. Copy the running configuration to the startup configuration.

Step 3: (Optional) Configure basic settings on the switches.

a. Console into the switch and enter global configuration mode.
i. Copy the following basic configuration and paste it to the running-configuration on the switch.

no ip domain-lookup

service password-encryption

enable secret class

banner motd #

Unauthorized access is strictly prohibited. #

Line con 0

password cisco

login

logging synchronous

line vty 0 15

password cisco

login

exit

j. Configure the device name as shown in the topology.

k. Configure the management interface IP address as shown in the Topology and Addressing Table.

l. Configure a default gateway.

m. Enable Telnet access.

n. Copy the running configuration to the startup configuration.

Step 4: Configure Rip routing on R1, ISP, and R3.

a. Configure RIP version 2 and advertise all networks on R1, ISP, and R3. The RIP configuration for R1 and ISP is included for reference.

R1(config)# **router rip**

R1(config-router)# **version 2**

R1(config-router)# **network 192.168.10.0**

R1(config-router)# **network 192.168.20.0**

R1(config-router)# **network 10.1.1.0**

ISP(config)# **router rip**

ISP(config-router)# **version 2**

ISP(config-router)# **network 209.165.200.224**

ISP(config-router)# **network 10.1.1.0**

ISP(config-router)# **network 10.2.2.0**

o. After configuring Rip on R1, ISP, and R3, verify that all routers have complete routing tables, listing all networks. Troubleshoot if this is not the case.

Step 5: Verify connectivity between devices.

Note: It is very important to test whether connectivity is working **before** you configure and apply access lists! You want to ensure that your network is properly functioning before you start to filter traffic.

a. From PC-A, ping PC-C and the loopback interface on R3. Were your pings successful?
Yes

p. From R1, ping PC-C and the loopback interface on R3. Were your pings successful?
Yes

q. From PC-C, ping PC-A and the loopback interface on R1. Were your pings successful?
Yes

r. From R3, ping PC-A and the loopback interface on R1. Were your pings successful?
Yes

C. Configure and Verify Standard Numbered and Named ACLs

Step 1: Configure a numbered standard ACL.

Standard ACLs filter traffic based on the source IP address only. A typical best practice for standard ACLs is to configure and apply it as close to the destination as possible. For the first access list, create a standard numbered ACL that allows traffic from all hosts on the 192.168.10.0/24 network and all hosts on the 192.168.20.0/24 network to access all hosts on the 192.168.30.0/24 network. The security policy also states that a **deny any** access control entry (ACE), also referred to as an ACL statement, should be present at the end of all ACLs.

What wildcard mask would you use to allow all hosts on the 192.168.10.0/24 network to access the 192.168.30.0/24 network?

0.0.0.255

Following Cisco's recommended best practices, on which router would you place this ACL?
R3

On which interface would you place this ACL? In what direction would you apply it?

G0/1. ACL should be applied going out as going in would effectively block LANs on R1 from getting to 192.168.40.0/24

a. Configure the ACL on R3. Use 1 for the access list number.

R3(config)# **access-list 1 remark Allow R1 LANs Access**
R3(config)# **access-list 1 permit 192.168.10.0 0.0.0.255**
R3(config)# **access-list 1 permit 192.168.20.0 0.0.0.255**
R3(config)# **access-list 1 deny any**

s. Apply the ACL to the appropriate interface in the proper direction.

R3(config)# **interface g0/1**
R3(config-if)# **ip access-group 1 out**

t. Verify a numbered ACL.

The use of various **show** commands can aid you in verifying both the syntax and placement of your ACLs in your router.

To see access list 1 in its entirety with all ACEs, which command would you use?

R3# show access-lists 1

What command would you use to see where the access list was applied and in what direction?

R3# show ip interface g0/1

1) On R3, issue the show access-lists 1 command.

   R3# **show access-list 1**
   Standard IP access list 1
   10 permit 192.168.10.0, wildcard bits 0.0.0.255
   20 permit 192.168.20.0, wildcard bits 0.0.0.255
   30 deny any

2) On R3, issue the show ip interface g0/1 command.

   R3# **show ip interface g0/1**
   GigabitEthernet0/1 is up, line protocol is up
   Internet address is 192.168.30.1/24
   Broadcast address is 255.255.255.255
   Address determined by non-volatile memory
   MTU is 1500 bytes
   Helper address is not set
   Directed broadcast forwarding is disabled
   Multicast reserved groups joined: 224.0.0.10
   Outgoing access list is 1
   Inbound access list is not set
   Output omitted

3) Test the ACL to see if it allows traffic from the 192.168.10.0/24 network access to the 192.168.30.0/24 network. From the PC-A command prompt, ping the PC-C IP address. Were the pings successful? Yes

4) Test the ACL to see if it allows traffic from the 192.168.20.0/24 network access to the 192.168.30.0/24 network. You must do an extended ping and use the loopback 0 address on R1 as your source. Ping PC-C's IP address. Were the pings successful? Yes

   R1# ping
   Protocol [ip]:

Target IP address: 192.168.30.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: **y**
Source address or interface: **192.168.20.1**
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms

u. From the R1 prompt, ping PC-C's IP address again.

R1# **ping 192.168.30.3**

Was the ping successful? Why or why not?

No the pings fail as when trying to ping the router it uses the closest interface to the destination as the source address. Because the source was 10.1.1.1 the access list on R3 doesn't allow that network.

Step 2: Configure a named standard ACL.

Create a named standard ACL that conforms to the following policy: allow traffic from all hosts on the 192.168.40.0/24 network access to all hosts on the 192.168.10.0/24 network. Also, only allow host PC-C access to the 192.168.10.0/24 network. The name of this access list should be called BRANCH-OFFICE-POLICY.

Following Cisco's recommended best practices, on which router would you place this ACL?
R1

On which interface would you place this ACL? In what direction would you apply it?

G0/1. The ACL should be going out as once again it would block all the LANs on R3 from getting to 192.168.20.0/24.

a. Create the standard named ACL BRANCH-OFFICE-POLICY on R1.

R1(config)# **ip access-list standard BRANCH-OFFICE-POLICY**

R1(config-std-nacl)# **permit host 192.168.30.3**

R1(config-std-nacl)# **permit 192.168.40.0 0.0.0.255**

R1(config-std-nacl)# **end**

R1#

*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console

Looking at the first permit ACE in the access list, what is another way to write this?

R1(config-std-nacl)# permit 192.168.30.3 0.0.0.0

v. Apply the ACL to the appropriate interface in the proper direction.

R1# **config t**

R1(config)# **interface g0/1**

R1(config-if)# **ip access-group BRANCH-OFFICE-POLICY out**

w. Verify a named ACL.

1) On R1, issue the show access-lists command.

R1# **show access-lists**

Standard IP access list BRANCH-OFFICE-POLICY

10 permit 192.168.30.3

20 permit 192.168.40.0, wildcard bits 0.0.0.255

Is there any difference between this ACL on R1 with the ACL on R3? If so, what is it?

There is no line 30 although with **deny any** on R1 it may be assumed. We use the deny any command as it shows up in the ACL when issuing a show access-lists command which could be useful when troubleshooting ACLs. It could result in traffic being denied that should have been allowed.

2) On R1, issue the show ip interface g0/1 command.

R1# **show ip interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

Internet address is 192.168.10.1/24

Broadcast address is 255.255.255.255

Address determined by non-volatile memory

MTU is 1500 bytes

Helper address is not set

Directed broadcast forwarding is disabled

Multicast reserved groups joined: 224.0.0.10

Outgoing access list is BRANCH-OFFICE-POLICY

Inbound access list is not set

<Output omitted>

3) Test the ACL. From the command prompt on PC-C, ping PC-A's IP address. Were the pings successful? Yes

4) Test the ACL to ensure that only the PC-C host is allowed access to the 192.168.10.0/24 network. You must do an extended ping and use the G0/1 address on R3 as your source. Ping PC-A's IP address. Were the pings successful? No

5) Test the ACL to see if it allows traffic from the 192.168.40.0/24 network access to the 192.168.10.0/24 network. You must perform an extended ping and use the loopback 0 address on R3 as your source. Ping PC-A's IP address. Were the pings successful? Yes

D. Modify a Standard ACL

It is common in business for security policies to change. For this reason, ACLs may need to be modified. Here, you will change one of the previous ACLs you configured to match a new management policy being put in place.

Management has decided that users from the 209.165.200.224/27 network should be allowed full access to the 192.168.10.0/24 network. Management also wants ACLs on all of their routers to follow consistent rules. A **deny any** ACE should be placed at the end of all ACLs. You must modify the BRANCH-OFFICE-POLICY ACL.

You will add two additional lines to this ACL. There are two ways you could do this:

OPTION 1: Issue a **no ip access-list standard BRANCH-OFFICE-POLICY** command in global configuration mode. This would effectively take the whole ACL out of the router. Depending upon the router IOS, one of the following scenarios would occur: all filtering of packets would be cancelled and all packets would be allowed through the router; or, because you did not take off the **ip access-group** command on the G0/1 interface, filtering is still in place. Regardless, when the ACL is gone, you could retype the whole ACL, or cut and paste it in from a text editor.

OPTION 2: You can modify ACLs in place by adding or deleting specific lines within the ACL itself. This can come in handy, especially with ACLs that have many lines of code. The retyping of the whole ACL or cutting and pasting can easily lead to errors. Modifying specific lines within the ACL is easily accomplished.

Note: For this exercise, use Option 2.

Step 1: Modify a named standard ACL.

a. From R1 privileged EXEC mode, issue a **show access-lists** command.

R1# **show access-lists**

Standard IP access list BRANCH-OFFICE-POLICY

10 permit 192.168.30.3 (8 matches)

20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)

x. Add two additional lines at the end of the ACL. From global config mode, modify the ACL, BRANCH-OFFICE-POLICY.

R1#(config)# **ip access-list standard BRANCH-OFFICE-POLICY**

R1(config-std-nacl)# **30 permit 209.165.200.224 0.0.0.31**

R1(config-std-nacl)# **40 deny any**

R1(config-std-nacl)# **end**

y. Verify the ACL.

1) On R1, issue the **show access-lists** command.

R1# **show access-lists**

Standard IP access list BRANCH-OFFICE-POLICY

10 permit 192.168.30.3 (8 matches)

20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)

30 permit 209.165.200.224, wildcard bits 0.0.0.31

40 deny any

Do you have to apply the BRANCH-OFFICE-POLICY to the G0/1 interface on R1?

No as the ip access-group BRANCH-OFFICE-POLICY is still on G0/1.

2) From the ISP command prompt, issue an extended ping. Test the ACL to see if it allows traffic from the 209.165.200.224/27 network access to the 192.168.10.0/24 network. You must do an extended ping and use the loopback 0 address on ISP as your source. Ping PC-A's IP address. Were the pings successful? Yes

Reflection

1. As you can see, standard ACLs are very powerful and work quite well. Why would you ever have the need for using extended ACLs?

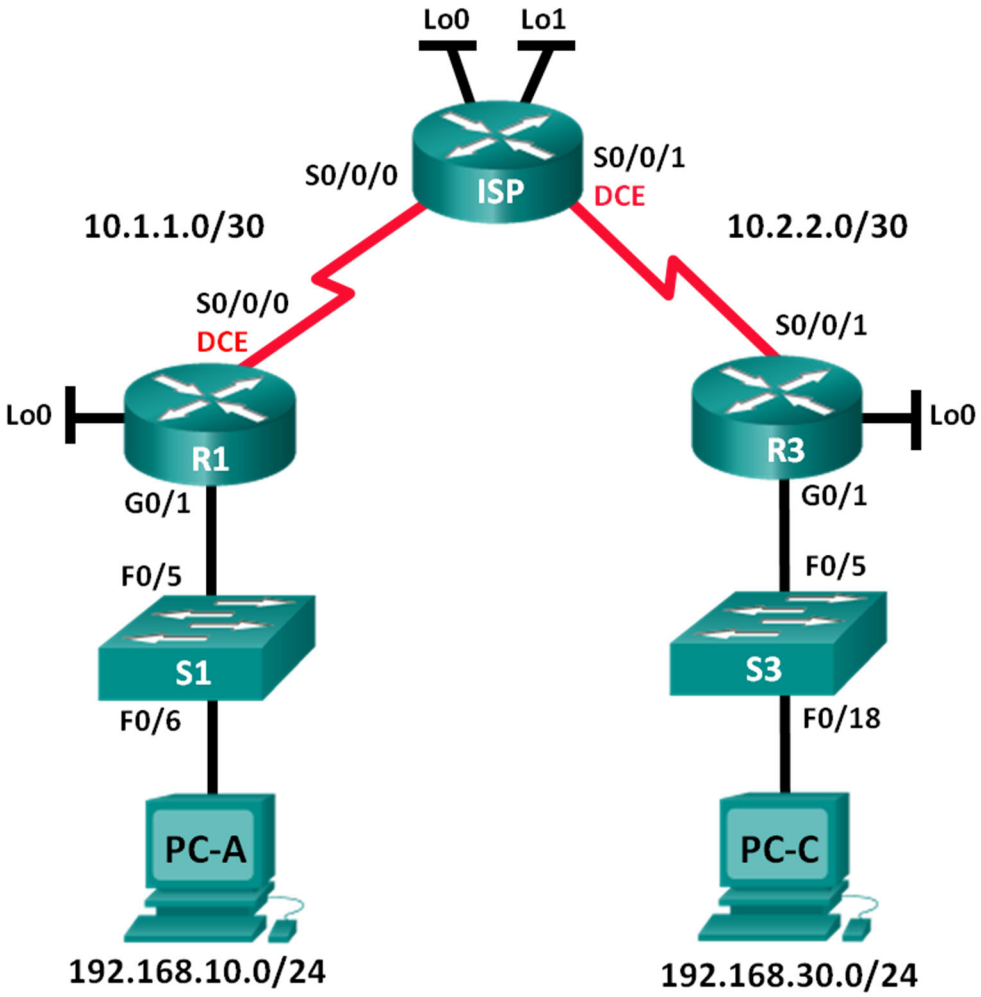
   Standard ACLs are good as they can filter based on the source address although are bad as they are one unit. When using them they allow or deny all protocols and service. Extended ACLs are better for complex networks where you may need to give or take away access to specific ports.

2. Typically, more typing is required when using a named ACL as opposed to a numbered ACL. Why would you choose named ACLs over numbered?

   ACLs give the ability to modify specific lines within itself without having to redo the whole thing.

Exercise 2: Configuring and Verifying Extended ACLs (4.2.2.13)

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	209.165.201.1	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Scenario

Extended access control lists (ACLs) are extremely powerful. They offer a much greater degree of control than standard ACLs as to the types of traffic that can be filtered, as well as where the traffic originated and where it is going. In this exercise, you will set up filtering rules for two offices represented by R1 and R3. Management has established some access policies between the LANs located at R1 and R3, which you must implement. The ISP router between R1 and R3 does not have any ACLs placed on it. You would not be allowed any administrative access to an ISP router as you can only control and manage your own equipment.

A. Set Up the Topology and Initialize Devices using Cisco Packet Tracer

B. Configure Devices and Verify Connectivity

Configure basic settings on the routers, switches, and PCs. Refer to the Topology and Addressing Table for device names and address information.

Step 1: Configure IP addresses on PC-A and PC-C.

Step 2: Configure basic settings on R1.

a. Disable DNS lookup.

b. Configure the device name as shown in the topology.

c. Create a loopback interface on R1.

d. Configure interface IP addresses as shown in the Topology and Addressing Table.

e. Configure a privileged EXEC mode password of **class**.

f. Assign a clock rate of **128000** to the S0/0/0 interface.

g. Assign **cisco** as the console and vty password and enable Telnet access. Configure **logging synchronous** for both the console and vty lines.

h. Enable web access on R1 to simulate a web server with local authentication for user **admin**.

R1(config)# **ip http server**

R1(config)# **ip http authentication local**

R1(config)# **username admin privilege 15 secret class**

Step 3: Configure basic settings on ISP.

a. Configure the device name as shown in the topology.

b. Create the loopback interfaces on ISP.

c. Configure interface IP addresses as shown in the Topology and Addressing Table.

d. Disable DNS lookup.

e. Assign **class** as the privileged EXEC mode password.

f. Assign a clock rate of **128000** to the S0/0/1 interface.

g. Assign **cisco** as the console and vty password and enable Telnet access. Configure **logging synchronous** for both console and vty lines.

h. Enable web access on the ISP. Use the same parameters as in Step 2h.

Step 4: Configure basic settings on R3.

a. Configure the device name as shown in the topology.

b. Create a loopback interface on R3.

c. Configure interface IP addresses as shown in the Topology and Addressing Table.

d. Disable DNS lookup.

e. Assign **class** as the privileged EXEC mode password.

f. Assign **cisco** as the console password and configure **logging synchronous** on the console line.

g. Enable SSH on R3.

R3(config)# **ip domain-name cisco.com**

R3(config)# **crypto key generate rsa modulus 1024**

R3(config)# **line vty 0 4**

R3(config-line)# **login local**

R3(config-line)# **transport input ssh**

h. Enable web access on R3. Use the same parameters as in Step 2h.

Step 5: (Optional) Configure basic settings on S1 and S3.

a. Configure the hostnames as shown in the topology.

b. Configure the management interface IP addresses as shown in the Topology and Addressing Table.

c. Disable DNS lookup.

d. Configure a privileged EXEC mode password of **class**.

e. Configure a default gateway address.

Step 6: Configure OSPF routing on R1, ISP, and R3.

a. Assign 1 as the OSPF process ID and advertise all networks on R1, ISP, and R3. The OSPF configuration for R1 is included for reference.

R1(config)# **router ospf 1**

R1(config-router)# **network 192.168.10.0 0.0.0.255 area 0**

R1(config-router)# **network 192.168.20.0 0.0.0.255 area 0**

R1(config-router)# **network 10.1.1.0 0.0.0.3 area 0**

b. After configuring OSPF on R1, ISP, and R3, verify that all routers have complete routing tables listing all networks. Troubleshoot if this is not the case.

Step 7: Verify connectivity between devices.

Note: It is very important to verify connectivity **before** you configure and apply ACLs! Ensure that your network is properly functioning before you start to filter out traffic.

a. From PC-A, ping PC-C and the loopback and serial interfaces on R3.

   Were your pings successful? Yes

b. From R1, ping PC-C and the loopback and serial interface on R3.

   Were your pings successful? Yes

c. From PC-C, ping PC-A and the loopback and serial interface on R1.

   Were your pings successful? Yes

d. From R3, ping PC-A and the loopback and serial interface on R1.

   Were your pings successful? Yes

e. From PC-A, ping the loopback interfaces on the ISP router.

   Were your pings successful? Yes

f. From PC-C, ping the loopback interfaces on the ISP router.

   Were your pings successful? Yes

g. Open a web browser on PC-A and go to http://209.165.200.225 on ISP. You will be prompted for a username and password. Use admin for the username and class for the password. If you are prompted to accept a signature, accept it. The router will load the Cisco Configuration Professional (CCP) Express in a separate window. You may be prompted for a username and password. Use admin for the username and class for the password.

h. Open a web browser on PC-C and go to http://10.1.1.1 on R1. You will be prompted for a username and password. Use admin for username and class for the password. If you are prompted to accept a signature, accept it. The router will load CCP Express in a separate window. You may be prompted for a username and password. Use admin for the username and class for the password.

C. Configure and Verify Extended Numbered and Named ACLs

Extended ACLs can filter traffic in many different ways. Extended ACLs can filter on source IP addresses, source ports, destination IP addresses, destination ports, as well as various protocols and services.

Security policies are as follows:

1. Allow web traffic originating from the 192.168.10.0/24 network to go to any network.
2. Allow an SSH connection to the R3 serial interface from PC-A.
3. Allow users on 192.168.10.0/24 network access to 192.168.20.0/24 network.
4. Allow web traffic originating from the 192.168.30.0/24 network to access R1 via the web interface and the 209.165.200.224/27 network on ISP. The 192.168.30.0/24 network should NOT be allowed to access any other network via the web.

In looking at the security policies listed above, you will need at least two ACLs to fulfill the security policies. A best practice is to place extended ACLs as close to the source as possible. We will follow this practice for these policies.

Step 1: Configure a numbered extended ACL on R1 for security policy numbers 1 and 2.

You will use a numbered extended ACL on R1. What are the ranges for extended ACLs?

100-199 and 2000-2699

a. Configure the ACL on R1. Use 100 for the ACL number.

R1(config)# **access-list 100 remark Allow Web & SSH Access**

R1(config)# **access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22**

R1(config)# **access-list 100 permit tcp any any eq 80**

What does the 80 signify in the command output listed above?

It is the destination port.

To what interface should ACL 100 be applied?

S0/0 if you were to pick G0/1 it is able to block the user on network 192.168.10.0/24 from getting to other LANs attached to R1.

In what direction should ACL 100 be applied?

It should be going out.

b. Apply ACL 100 to the S0/0/0 interface.

R1(config)# **interface s0/0/0**

R1(config-if)# **ip access-group 100 out**

c. Verify ACL 100.

1) Open up a web browser on PC-A, and access http://209.165.200.225 (the ISP router). It should be successful; troubleshoot, if not.

2) Establish an SSH connection from PC-A to R3 using 10.2.2.1 for the IP address. Log in with **admin** and **class** for your credentials. It should be successful; troubleshoot, if not.

3) From privileged EXEC mode prompt on R1, issue the **show access-lists** command.

R1# **show access-lists**

Extended IP access list 100

10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (22 matches)

20 permit tcp any any eq www (111 matches)

4) From the PC-A command prompt, issue a ping to 10.2.2.1. Explain your results.

The pings failed with a message of "Reply from 192.168.10.1: Destination net unreachable" because of deny any at the end of every ACL. ACL 100 will only permit SSH and web traffic.

Step 2: Configure a named extended ACL on R3 for security policy number 3.

a. Configure the policy on R3. Name the ACL WEB-POLICY.

R3(config)# **ip access-list extended WEB-POLICY**

R3(config-ext-nacl)# **permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80**

R3(config-ext-nacl)# **permit tcp 192.168.30.0 0.0.0.255 209.165.200.224 0.0.0.31 eq 80**

b. Apply ACL WEB-POLICY to the S0/0/1 interface.

R3(config-ext-nacl)# **interface S0/0/1**

R3(config-if)# **ip access-group WEB-POLICY out**

c. Verify the ACL WEB-POLICY.

1) From R3 privileged EXEC mode command prompt, issue the **show ip interface s0/0/1** command.

What, if any, is the name of the ACL? WEB-POLICY

In what direction is the ACL applied? Out

2) Open up a web browser on PC-C and access http://209.165.200.225 (the ISP router). It should be successful; troubleshoot, if not.

3) From PC-C, open a web session to http://10.1.1.1 (R1). It should be successful; troubleshoot, if not.

4) From PC-C, open a web session to http://209.165.201.1 (ISP router). It should fail; troubleshoot, if not.

5) From a PC-C command prompt, ping PC-A. What was your result and why?

They failed as only web traffic is allowed to exit from 192.168.30.0/24

D. Modify and Verify Extended ACLs

Because of the ACLs applied on R1 and R3, no pings or any other kind of traffic is allowed between the LAN networks on R1 and R3. Management has decided that all traffic between the 192.168.10.0/24 and 192.168.30.0/24 networks should be allowed. You must modify both ACLs on R1 and R3.

Step 1: Modify ACL 100 on R1.

a. From R1 privileged EXEC mode, issue the **show access-lists** command.

How many lines are there in this access list? 2 at line 10 and 20.

b. Enter global configuration mode and modify the ACL on R1.

R1(config)# **ip access-list extended 100**

R1(config-ext-nacl)# **30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255**

R1(config-ext-nacl)# **end**

c. Issue the **show access-lists** command.

Where did the new line that you just added appear in ACL 100?

At the last line, 30

Step 2: Modify ACL WEB-POLICY on R3.

a. From R3 privileged EXEC mode, issue the **show access-lists** command.

How many lines are there in this access list? 2 at lines 10 and 20

b. Enter global configuration mode and modify the ACL on R3.

R3(config)# **ip access-list extended WEB-POLICY**

R3(config-ext-nacl)# **30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255**

R3(config-ext-nacl)# **end**

c. Issue the **show access-lists** command to verify that the new line was added at the end of the ACL.

Step 3: Verify modified ACLs.

a. From PC-A, ping the IP address of PC-C. Were the pings successful? Yes

b. From PC-C, ping the IP address of PC-A. Were the pings successful? Yes

Why did the ACLs work immediately for the pings after you changed them?

ACLs of both R1 and R3 are still corresponding to the proper interfaces as seen in the ip access-group command.

Reflection

1. Why is careful planning and testing of ACLs required?

As they may improperly block wanted traffic from entering/leaving.

2. Which type of ACL is better: standard or extended?

There are pros and cons to each. For example, standard ACL may be easier to write and configure if all traffic is wanted to be blocked or denied. Although it only can check source addresses and cannot block specifics. This is where the extended ACL may come in handy. It can filter specific traffic better although is much more complicated to set up.

3. **Why are OSPF hello packets and routing updates not blocked by the implicit** deny any **access control entry (ACE) or ACL statement of the ACLs applied to R1 and R3?**

   OSPFs do not update from LAN but from the serial interfaces of R1 and R3. ACLs are able to filter the traffic going through the router and not traffic from the router itself. If an ACL is placed on an ISP router, it can possibly have blocked OSPF updates in between R1 and R3 along with other router communication. This could be a reason that PC-A and PC-C loss connection.