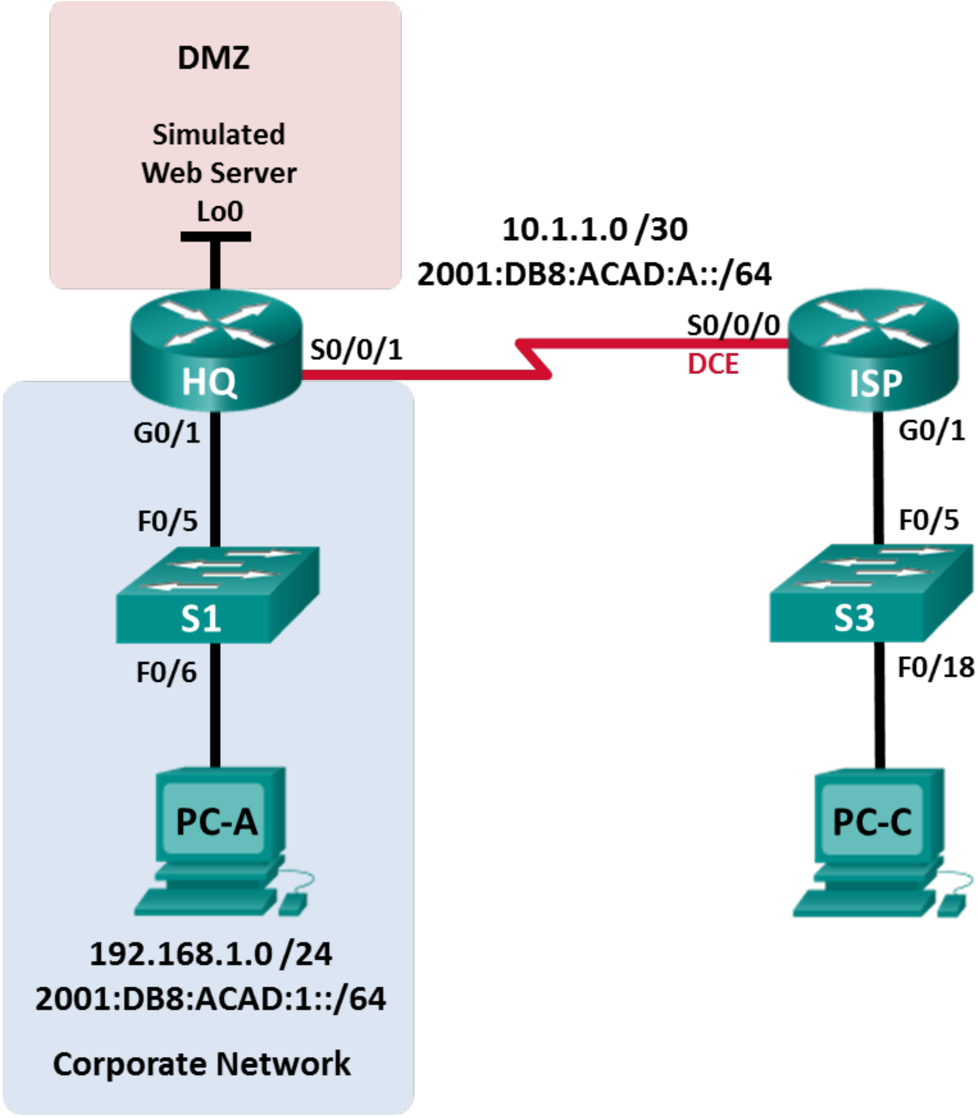
Lab - Troubleshooting ACL Configuration and Placement

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
		IPv6 Address / Prefix		
		Link Local Address		
HQ	G0/1	192.168.1.1	255.255.255.0	N/A
		2001:DB8:ACAD:1::1/64		
		FE80::1		
	S0/0/1	10.1.1.2	255.255.255.252	N/A
		2001:DB8:ACAD:A::2/64		
		FE80::2		
	Lo0	192.168.4.1	255.255.255.0	N/A
		2001:DB8:ACAD:4::1/64		
		FE80::1		
ISP	G0/1	192.168.3.1	255.255.255.0	N/A
		2001:DB8:ACAD:3::1/64		
		FE80::1		
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
		2001:DB8:ACAD:A::1/64		
		FE80::1		
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
		2001:DB8:ACAD:1::3/64		FE80::1
		FE80::3		
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1
		2001:DB8:ACAD:3::3/64		FE80::1
		FE80::3		

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot Internal Access

Part 3: Troubleshoot Remote Access

Background / Scenario

An access control list (ACL) is a series of IOS commands that provide basic traffic filtering on a Cisco router. ACLs are used to select the types of traffic to be processed.

A single ACL statement is called an access control entry (ACE). The ACEs in the ACL are evaluated from top to bottom with an implicit deny all ACE at the end of the list. ACLs can also control the types of traffic into or out of a network by the source and destination hosts or network. To process the desired traffic correctly, the placement of the ACLs is critical.

In this lab, a small company has just added a web server to the network to allow customers to access confidential information. The company IPv4 and IPv6 network is divided into two zones: Corporate network zone and Demilitarized Zone (DMZ). The corporate network zone houses private servers and internal clients. The DMZ houses the externally accessible web server (simulated by Lo0 on HQ).

To secure access to the corporate and DMZ networks, several ACLs were configured on the HQ router. However, there are problems with the configured ACLs. In this lab, you will examine what the ACLs are doing and take corrective actions to implement them properly.

When troubleshooting ACLs, it is important that its purpose and desired outcome is well understood. For this reason, the following describes the ACLs configured on HQ:

- **ACL 101** is implemented to limit the traffic leaving the corporate network zone. This zone is often referred to as the private or internal network because it houses the private servers and internal clients. In this topology, this zone is assigned network address 192.168.1.0/24. Therefore, only traffic from that network should be permitted to leave the internal network.
- **ACL 102** is used to limit the traffic into the corporate network. Only responses to requests that originated from within the corporate network are allowed back into that network. This includes TCP-based requests from internal hosts such as Web and FTP. ICMP is allowed into the network for troubleshooting purposes so that incoming ICMP messages generated in response to pings can be received by internal hosts. No other network should be able to access the corporate zone.
- **ACL 121** controls outside traffic to the DMZ and corporate network. Only HTTP traffic is allowed to the DMZ web server (simulated by Lo0 on HQ). Other network related traffic, such as EIGRP, is allowed from outside networks. Furthermore, valid internal private addresses, such as 192.168.1.0, loopback address such as 127.0.0.1 and multicast addresses are denied entrance to the corporate network to prevent malicious network attacks from outside users.
- **IPv6 ACL** named NO-ICMP denies ICMP traffic to the DMZ and corporate network originated from the outside. ICMP response is allowed into the network that is responding to the requests from the internet hosts. Other network related traffic, such as EIGRP, is allowed from outside networks. Furthermore, the outside network is allowed to access the DMZ web server (simulated by Lo0 on HQ).

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.4(3) (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.4(3) universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)

- 2 PCs (Windows with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the routers and switches with basic settings such as passwords and IP addresses. Preset configurations are also provided for you for the initial router configurations. You will also configure the IP settings for the PCs in the topology.

Step 1: Cable the network as shown in the topology.

Step 2: Configure PC hosts according to the Addressing Table

Step 3: Initialize and reload the routers and switches as necessary.

Step 4: (Optional) Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure host names as shown in the Topology.

c. Configure IP addresses and default gateways as shown in the Addressing Table.

d. Assign **cisco** as the console and vty passwords.

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

f. Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 5: Configure basic settings for each router.

a. Disable DNS lookup.

b. Configure host names as shown in the topology.

c. Assign **class** as the privileged EXEC password.

d. Assign **cisco** as the console and vty passwords.

e. Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 6: Configure HTTP access and user credentials on HQ router.

Local user credentials are configured to access the simulated web server (192.168.4.1).

```
HQ(config)# ip http server
HQ(config)# username admin privilege 15 secret adminpass
HQ(config)# ip http authentication local
```

Step 7: Load router configurations.

The configurations for the routers ISP and HQ are provided for you. There are errors within these configurations, and it is your task to correct them.

Router ISP

```
hostname ISP
ipv6 unicast-routing
```

```
ipv6 router eigrp 1
 eigrp router-id 10.1.1.1
 no shutdown
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:3::1/64
 ipv6 eigrp 1
 no shutdown
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 128000
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:A::1/64
 ipv6 eigrp 1
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.3.0
 no auto-summary
end
```

Router HQ

```
hostname HQ
ipv6 unicast-routing
ipv6 router eigrp 1
 eigrp router-id 10.1.1.2
 no shutdown
interface Loopback0
 ip address 192.168.4.1 255.255.255.0
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:4::1/64
 ipv6 eigrp 1
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:1::1/64
 ip access-group 101 out
ip access-group 102 in
ipv6 eigrp 1
 no shutdown
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
 ip access-group 121 in
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:ACAD:A::2/64
 ipv6 eigrp 1
ipv6 traffic-filter NO-ICMP out
 no shutdown
router eigrp 1
```

```
 network 10.1.1.0 0.0.0.3
 network 192.168.1.0
 network 192.168.4.0
 no auto-summary
ip http server
access-list 101 permit ip 192.168.11.0 0.0.0.255 any
access-list 101 deny ip any any
access-list 102 permit tcp any any established
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any unreachable
access-list 102 deny ip any any
access-list 121 permit tcp any host 192.168.4.1 eq 89
access-list 121 deny icmp any host 192.168.4.11
access-list 121 deny ip 192.168.1.0 0.0.0.255 any
access-list 121 deny ip 127.0.0.0 0.255.255.255 any
access-list 121 deny ip 224.0.0.0 31.255.255.255 any
access-list 121 permit ip any any
access-list 121 deny ip any any
ipv6 access-list NO-ICMP
 deny icmp any any echo-request
 permit ipv6 any any
end
```

Part 2: Troubleshoot Internal Access

In Part 2, the ACLs on router HQ are examined to determine if they are configured correctly.

Step 1: Troubleshoot ACL 101

ACL 101 is implemented to limit the traffic leaving the corporate network zone. This zone houses only internal clients and private servers. Only 192.168.1.0/24 network can exit this corporate network zone.

a. Can PC-A ping its default gateway? No

b. After verifying that PC-A was configured correctly, examine the HQ router to find possible configuration errors by viewing the summary of ACL 101. Enter the command **show access-lists 101**.

```
HQ# show access-lists 101
Extended IP access list 101
    10 permit ip 192.168.11.0 0.0.0.255 any
    20 deny ip any any
```

c. Are there any problems with ACL 101?

Yes

d. Correct ACL 101. Record the commands used to correct the errors.

show access-list
ip access-list extended 101
no 10
10 permit ip 192.168.1.0 0.0.0.255 any

e. Can PC-A ping its default gateway? No, we have not
changed the direction

f. PC-A still cannot ping its default gateway, therefore verify that ACL 101 is applied in the correct direction on the G0/1 interface. Enter the **show ip interface g0/1** command.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  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 101
  Inbound  access list is 102
```

Is the direction for interface G0/1 configured correctly for ACL 101?

No, we have not changed the direction access list. There was 102

g. Correct the direction of ACL 101 on the G0/1 interface. Record the commands used to correct the errors.

no ip access-group 101 out
ip access-group 101 in

h. Verify the traffic from network 192.168.1.0 /24 can exit the corporate network. PC-A should now be able to ping its default gateway interface.

Step 2: Troubleshoot ACL 102

ACL 102 is implemented to limit traffic going into the corporate network. Traffic originating from the outside network is not allowed onto the corporate network. Remote traffic is allowed into the corporate network if the established traffic originated from the internal network. ICMP reply messages are allowed for troubleshooting purposes.

a. Can PC-A ping PC-C? No

b. Examine the HQ router to find possible configuration errors by viewing the summary of ACL 102. Enter the command **show access-lists 102**.

```
HQ# show access-lists 102
Extended IP access list 102
    10 permit tcp any any established
    20 permit icmp any any echo-reply
    30 permit icmp any any unreachable
    40 deny ip any any (57 matches)
```

c. Are there any problems with ACL 102? No

d. Verify that the ACL 102 is applied in the correct direction on G0/1 interface. Enter the **show ip interface g0/1** command.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  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 101
  Inbound  access list is 101
```

e. Are there any problems with the application of ACL 102 to interface G0/1?

There was correct direction (102 was in)

f. Correct any errors found regarding ACL 102. Record the commands used to correct the errors.

There was correct direction (102 was in)

g. Can PC-A ping PC-C now? Yes

Part 3: Troubleshoot Remote Access

In Part 3, ACL 121 is configured to prevent spoofing attacks from the outside networks and allow only remote HTTP access to the web server (192.168.4.1) in the DMZ.

a. Verify ACL 121 has been configured correctly. Enter the **show ip access-list 121** command.

```
HQ# show ip access-lists 121
Extended IP access list 121
    10 permit tcp any host 192.168.4.1 eq 89
    20 deny icmp any host 192.168.4.11
    30 deny ip 192.168.1.0 0.0.0.255 any
    40 deny ip 127.0.0.0 0.255.255.255 any
    50 deny ip 224.0.0.0 31.255.255.255 any
    60 permit ip any any (354 matches)
    70 deny ip any any
```

Are there any problems with this ACL?

10 permit tcp any host 192.168.4.1 eq 89
We should change it from eq 89 to 80 because HTTP uses 80

b. Make and record the necessary configuration changes to ACL 121.

no permit tcp any host 192.168.4.1 eq 89
10 permit tcp any host 192.168.4.1 eq 80
no 20
20 deny icmp any host 192.168.4.1

c. Verify that the ACL 121 is applied in the correct direction on the HQ S0/0/1 interface. Enter the **show ip interface s0/0/1** command.

```
HQ# show ip interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet address is 10.1.1.2/30
  Broadcast address is 255.255.255.255
```

```
<output omitted>
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is 121
```

Are there any problems with the application of this ACL?

There are no problems with direction

d. Verify that PC-C can only access the simulated web server on HQ by using the web browser. Provide the username **admin** and password **adminpass** to access the web server (192.168.4.1).

Part 4: Troubleshoot IPv6 ACL

In Part 4, an IPv6 ACL named NO-ICMP denies ICMP traffic to the DMZ and corporate network originating from the outside. ICMP response to the internal hosts, EIGRP packets, and network related traffic are allowed from outside networks. Furthermore, the outside network is allowed to access the DMZ web server (simulated by Lo0 on HQ).

a. Verify ACL **NO-ICMP** has been configured correctly. Enter the **show ipv6 access-list NO-ICMP** command.

```
HQ# show ipv6 access-list NO-ICMP
IPv6 access list NO-ICMP
    deny icmp any any echo-request sequence 10
permit ipv6 any any sequence 20
```

Are there any problems with this ACL?

It's ok

b. Verify that the ACL NO-ICMP is applied in the correct direction on the HQ S0/0/1 interface. Enter the **show ipv6 interface s0/0/1** command.

```
HQ# show ipv6 interface s0/0/1
Serial0/0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::2
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::A
    FF02::1:FF00:1
    FF02::1:FF00:2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  Output features: Access List
  Outgoing access list NO-ICMP
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
```

Are there any problems with the application of this ACL?

Incorrect direction of Outgoing access list NO-ICMP. It's out but should be in

c. Make and record the necessary configuration changes to ACL NO-ICMP.

no ipv6 traffic-filter NO-ICMP out
ipv6 traffic-filter NO-ICMP in

Reflection

1. How should the ACL statement be ordered? From general to specific or vice versa?

   Specific options should be first then more general

2. If you delete an ACL by using the **no access-list** command and the ACL is still applied to the interface, what happens?

   It would apply deny any any and it MIGHT cause that administrator could lose controll of devices

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.