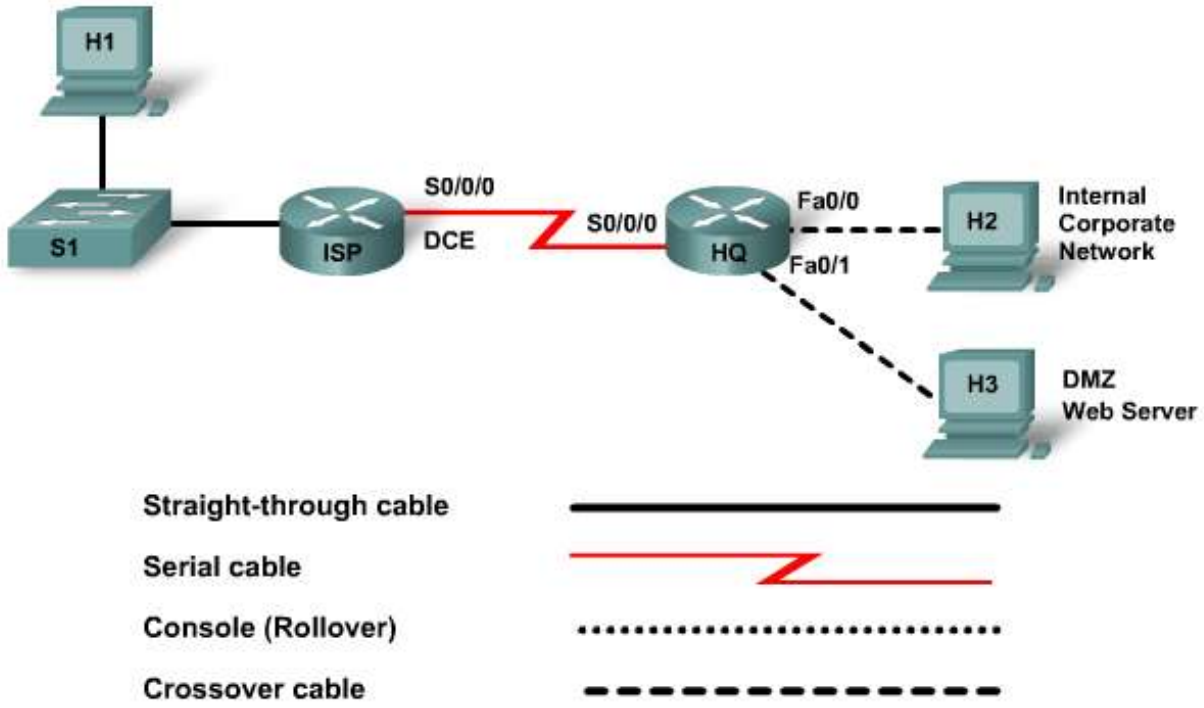
Lab 9.5.2 Troubleshooting ACL Configuration and Placement



Device	Host Name	Interface	IP Address	Subnet Mask	Default Gateway	Enable Secret Password	Enable, vty, and Console Password
Router 1	ISP	**Fa0/0**	172.19.2.1	255.255.255.0	N/A	class	cisco
		S0/0/0	172.16.1.1	255.255.255.252	N/A		
Router 2	HQ	**Fa0/0**	172.18.2.1	255.255.255.0	N/A	class	cisco
		Fa0/1	172.17.0.1	255.255.0.0	N/A		
		S0/0/0	172.16.1.2	255.255.255.252	N/A		
Host 1	H1	**NIC**	172.19.2.2	255.255.255.0	172.19.2.1		
Host 2	H2	**NIC**	172.18.2.2	255.255.255.0	172.18.2.1		
Web server (Discovery Server)	H3	**NIC**	172.17.1.1	255.255.0.0	172.17.0.1		

Objectives

- Load the routers with preconfigurations.
- Discover where communication is failing.
- Gather information about the misconfigured ACLs.
- Analyze information to determine why communication is not possible.
- Propose solutions to network errors.
- Implement solutions to network errors.

Background / Preparation

A small manufacturing company wants to create an awareness of their products over the Internet. Their immediate requirement is to promote their products to potential customers by providing product overviews, reports, and testimonials. Because they need a secure infrastructure to support their internal and external network requirements, you have implemented a two-tier security architecture consisting of an internal corporate network zone and a Demilitarized Zone (DMZ). The corporate network zone would house private servers and internal clients. The DMZ would house only one external server that would provide World Wide Web services. Since the company can only administer their own HQ router and not that of the ISP, all ACLs must be applied to the HQ router.

- **Access list 101 is implemented to limit the traffic out of the corporate network zone**, which houses private servers and internal clients. No other network should be able to access it. Protecting the corporate network begins by specifying which traffic can exit out of the network. This may sound strange, but it becomes clearer when it is known that most hackers are internal employees.
- **Access list 102 is implemented to limit the traffic into the corporate network.** Traffic entering the corporate network will be coming from either the Internet (ISP) or the DMZ. Only traffic that originated from the corporate network can be allowed back into that network. To make network management and troubleshooting easier, it is also decided to permit ICMP into the network. This will allow internal hosts to receive ICMP messages. At this time, no other traffic is desired into the corporate network.
- **Access list 111 is implemented to control outbound DMZ network traffic.** The DMZ network will house only one external server that will provide World Wide Web services. Other services such as e-mail, FTP, and DNS will be implemented at a later time. The traffic that can exit the network is specified here.
- **Access list 112 is implemented to control inbound DMZ network traffic.** Traffic entering the DMZ network will be coming from the Internet (ISP) or the corporate network requesting World Wide Web services, which must be allowed in. Allow only corporate users ICMP access into the DMZ network. No other traffic is permitted into the DMZ network.
- **Access list 121 is implemented to deter spoofing.** Networks are becoming increasingly prone to attacks from outside users. Hackers maliciously try to break into networks and render networks incapable of responding to legitimate request (Denial of Service (DoS) attacks). The access list should make it difficult for outside users to spoof internal addresses by specifying three common source IP addresses that hackers attempt to forge. These include valid internal private addresses, such as 172.18.2.0, loopback addresses such as 127.0.0.0, and multicast addresses (i.e., 224.x.x.x-239.x.x.x).

Cable a network similar to the one shown in the topology diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to the 1841 router. Other routers may be used; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switch or other comparable switch; alternately, crossover cables may be used between the hosts and routers and the switch omitted.
- One router with one Serial interface and 2 Ethernet interfaces
- One router with one Serial interface and one Ethernet interface
- Two Windows-based PCs, with a terminal emulation program, and set up as hosts
- One Windows-based PC running the Discovery Live CD representing the web server
- RJ-45-to-DB-9 connector console cable to configure the routers
- Two straight-through Ethernet cables
- One 2-part (DTE/DCE) serial cable
- Two crossover cables
- Cisco Discovery Live CD (obtain from instructor)

NOTE: Make sure that the routers have been erased and have no startup configurations. For instructions on erasing and reloading a switch and a router please refer to the Lab Manual. The Lab Manual can be found and downloaded on the Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM for basic router configuration, refer to the instructions provided in the Lab Manual which can be found and downloaded on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Fa0/0 interface of Router 1 to the Fa0/1 interface of the switch using a straight-through cable.

b. Connect one host to the Fa0/2 switch port of the switch using a straight-through cable.

c. Connect serial cables from Router 1 to Router 2 according to the topology diagram.

d. Connect hosts to the Fa0/0 and Fa0/1 interfaces of Router 2 using crossover cables according to the above topology.

Step 2: Load the preconfiguration on ISP

a. See your instructor for obtaining the preconfigurations for this lab.

b. Connect Host 1 to the console port of Router 1 to perform loading the preconfigurations using a terminal emulation program.

c. Transfer the configuration from Host 1 to Router 1:

1) In the terminal emulation program on H1, choose **Transfer > Send Text File**.

2) Locate the preconfiguration file and choose **Open** to start the transfer of the preconfiguration to Router 1.

NOTE: The preconfiguration can also be copied and pasted into the router using the HyperTerminal program. Choose **Edit** and then **Paste to Host**. Before using the **Paste** function, be sure that you are in configuration mode.

3) When the transfer is complete, save the configuration.

Step 3: Load the preconfiguration on HQ

Copy the preconfiguration on HQ using the process detailed in Step 2.

Step 4: Configure hosts H1 and H2

a. Configure the Ethernet interfaces of H1 and H2 with the IP addresses and default gateways from the addressing table.

b. Test the PC configuration by pinging the default gateway from each PC. H1 should be able to reach its default gateway, but H2 cannot.

Step 5: Configure the web server host H3

a. Load the Discovery LIVE CD on Host H3. The server's Ethernet interface is preconfigured with the IP address and default gateway shown in the addressing table. If using another web server, configure the IP address and subnet mask to match that in the table.

b. Test the PC configuration by pinging the default gateway from the H3 PC.

Step 6: Troubleshoot the HQ router and access list 101

a. Begin troubleshooting with the HQ router.

Access list 101 is implemented to protect the internal corporate network zone, which houses private servers and internal clients. No other network should be able to access it. Protecting the corporate network begins by specifying which traffic can exit out of the network.

b. Examine the HQ router to find possible configuration errors. Begin by viewing the summary of access list 101. Enter the command **`show access-list 101.`**

What does the information show?

_____

_____

_____

c. Verify reachability by pinging all systems and routers from each system. If a successful ping is not reached by all hosts, there is a problem with the access list.

Can H2 ping its default gateway (172.1.2.1)? _____

Can H2 ping the web server (172.17.1.1)? _____

Can H2 ping H1 (172.19.2.2)? _____

Are there any problems with access list 101? _____

If yes, what?

_____

_____

d. If any errors were found, make the necessary configuration changes to HQ. Remember that access lists have to be deleted and re-entered if there is any discrepancy in the commands.

_____

_____

_____

_____

e. Issue the command **`show ip interface fa0/0`**.

Is the access list applied in the correct direction on the Fa0/0 interface? _____

f. Now that the correct network is permitted inbound on Fa 0/0, H2 should be able to ping its default-gateway. Perform the pings from Step 6c again. If H2 cannot ping other locations, troubleshooting additional ACLs is required.

Step 7: Troubleshoot the HQ router and access list 102

a. Continue troubleshooting with the HQ router.

Access list 102 is implemented to limit the traffic into the corporate network (outbound on Fa 0/0). Traffic entering the corporate network will be coming from either the Internet (ISP) or the DMZ. Only traffic that originated from the corporate network (established traffic) can be allowed back into that network. To make network management and troubleshooting easier, it is also decided to permit ICMP echo replies into the network. This will allow internal hosts to receive replies from external hosts but not allow external hosts to ping internal hosts. At this time no other traffic is desired into the corporate network.

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

What does the information show?

_____

_____

_____

_____

c. Verify reachability by pinging all systems and routers from each system. If the access list is working correctly, traffic that originates from H2, should be permitted. Also, ICMP echo replies should also be permitted.

Can H2 ping the web server (172.17.1.1)? _____

Can H2 ping H1 (172.19.2.2)? _____

Can H1 ping the web server (172.17.1.1)? _____

Can H1 ping H2 (172.18.2.2)? _____

Can H3 ping H2 (172.18.2.2)? _____

Are there any problems with access list 102? _____

If yes, what?

_____

_____

d. If any errors were found, make the necessary configuration changes to HQ. Remember to delete the entire access list before making the corrections. The commands must be in logical, sequential order.

_____

_____

_____

_____

_____

_____

_____

_____

e. Open a web browser, such as Windows Explorer, Netscape Navigator, or Firefox and enter the address of the web server in the address location. Verify that H2 has web access to the web server.

f. Issue the command **`show ip interface fa0/0`**.

Is the access list applied in the correct direction on the interface? _____

g. At this point, the ACLs applied to the FastEthernet 0/0 interface on HQ, should be allowing all necessary traffic to and from the corporate network. Since this is not the case, we must expand our troubleshooting.

Step 8: Troubleshoot the HQ router and access list 111

a. Continue troubleshooting with the HQ router.

Access list 111 is implemented to protect the DMZ network. The DMZ network will house only one external server that will provide World Wide Web services. Other services such as email, FTP, and DNS will be implemented at a later time. The HQ router will allow World Wide Web services destined for the web server into the DMZ network. Only corporate users will be allowed ICMP access into the DMZ network. No other traffic is permitted into the DMZ network.

b. Examine the HQ router to find possible configuration errors. Begin by viewing the summary of access list 111. Enter the command **`show access-list 111.`**

What does the information show?

_____

_____

_____

_____

c. Verify reachability by pinging all systems and routers from each system. H1 should not be able to ping H2 if the access list is correct.

Can H2 ping the web server? _____

Can H1 ping the web server? _____

Can H3 ping H2 (172.18.2.2)? _____

Are there any problems with access list 111? _____

If yes, what?

_____

_____

_____

_____

d. If any errors were found, make the necessary configuration changes to HQ.

_____

_____

_____

_____

e. Issue the command **`show ip interface fastethernet0/1`**.

Is the access list applied in the correct direction on the interface? _____

f. Use **ping** to test connectivity. The ping tests should reveal that H3 can ping its default gateway, as well as the default gateway of H2. H3 can also ping H1. H3 still cannot ping H2, but that is expected behavior based on ACL 102. If the pings do not produce the expected results, continue to troubleshoot the next access control list.

Step 9: Troubleshoot the HQ router and access list 112

a. Continue troubleshooting with the HQ router.

Access list 112 is implemented to protect the DMZ network. Traffic entering the DMZ network will be coming from the Internet (ISP) or the corporate network requesting World Wide Web services, which must be allowed in. Allow only corporate users ICMP access into the DMZ network. No other traffic is permitted into the DMZ network.

b. Examine the HQ router to find possible configuration errors. Begin by viewing the summary of access list 112. Enter the command **`show access-list 112.`**

What does the information show?

_____

_____

_____

_____

c. Verify reachability by pinging all systems and routers from each system. If the access list is correct, H1 should not be able to ping the web server or H2.

Can H2 ping the web server? _____

Can H1 ping the web server? _____

Can H1 open a web page on H3? _____

Can H2 open a web page on H3? _____

Are there any problems with access list 112? _____

If yes, what?

_____

_____

d. If any errors were found, make the necessary configuration changes to HQ.

_____

_____

_____

_____

e. Open a web browser, such as Windows Explorer. Netscape Navigator, or Firefox and enter the address of the web server in the address location. Verify that H1 and H2 have web access to the web server.

Can H1 view the web page on the web server? _____

Can H2 view the web page on the web server? _____

Can H1 ping all locations? _____

Can H2 ping all locations? _____

f. Issue the command **show ip interface fastethernet0/1**.

Is the access list applied in the correct direction on the interface? _____

g. If web browser services are not successful as they should be, troubleshoot as necessary.

Step 10: Troubleshoot the HQ router and access list 121

a. Continue troubleshooting with the HQ router.

Access list 121 is implemented to deter spoofing. Networks are becoming increasingly prone to attacks from outside users. Hackers maliciously try to break into networks and render networks incapable of responding to legitimate request (Denial of Service (DoS) attacks). The access list should make it difficult for outside users to spoof internal addresses by specifying three common source IP addresses that hackers attempt to forge; valid internal private addresses, such as 172.19.2.0, loopback addresses such as 127.0.0.0, and multicast addresses (i.e., 224.x.x.x-239.x.x.x).

b. Examine the HQ router to find possible configuration errors. Begin by viewing the summary of access list 121. Enter the command **show access-list 121.**

What does the information show?

_____

_____

_____

_____

c. Verify reachability by pinging all systems and routers from each system. If the access list is correct, only H2 should successfully ping the web server.

Can H2 ping the web server? _____

Can H2 ping H1? _____

Can H1 ping the web server? _____

Can H1 ping H2? _____

Are there any problems with access list 121? _____

If yes, what?

_____

_____

_____

_____

d. Issue the command **show ip interface serial0/0/0**.

Is the access list applied in the correct direction on the interface? _____

e. If any errors were found, make the necessary configuration changes to HQ.

_____

_____

_____

f. Open a web browser such as Windows Explorer or Netscape Navigator or Firefox and enter the address of the web server in the address location. Verify that H1 and H2 still have web access to the web server.

Can H1 view the web page on the web server? _____

Can H2 view the web page on the web server? _____

Step 11: Reflection

There were a number of configuration errors in the preconfigurations that were provided for this lab. Use this space below to write a brief description of the errors that you found.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____