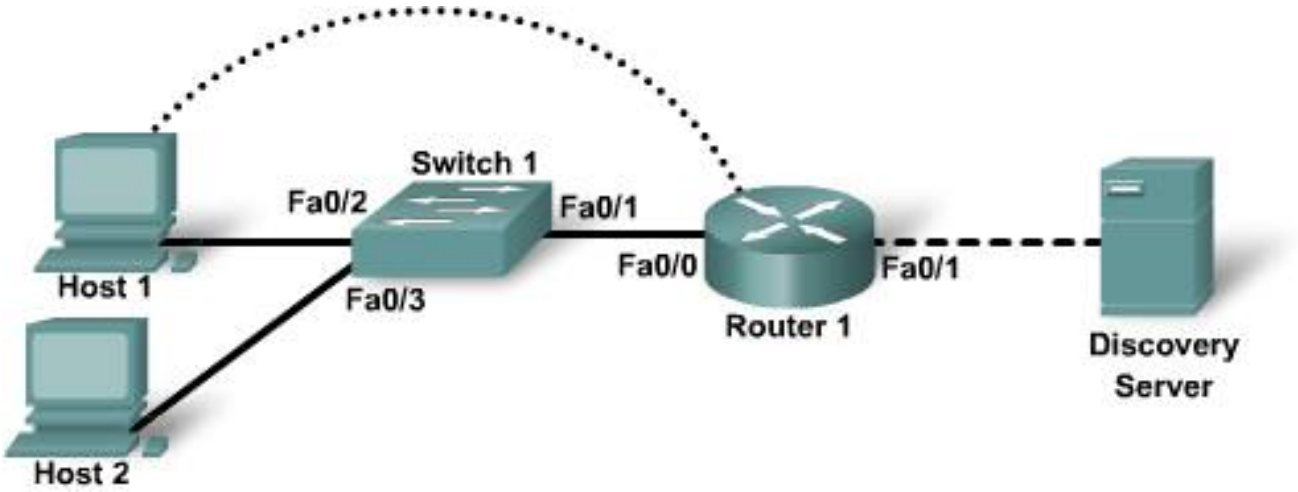
Lab 1.3.4 Creating an ACL



Device	Host Name	Address	Subnet Mask
Discovery Server	Server	172.17.1.1	255.255.0.0
R1	FC-CPE-1	Fa0/1 172.17.0.1 Fa0/0 10.0.0.1	255.255.0.0 255.255.255.0
S1	FC-ASW-1	—	—
Host1	PC1	10.0.0.10	255.255.255.0
Host2	PC2	10.0.0.201	255.255.255.0

Objective

- Create Access Control Lists (ACLs) to filter traffic for security and traffic management.

640-802 CCNA Exam Objectives

This lab contains skills that relate to the following CCNA exam objectives:

- Configure and apply ACLs based on network filtering requirements (including CLI/SDM).
- Configure and apply ACLs to limit telnet and SSH access to the router using (including SDM/CLI).
- Verify and monitor ACLs in a network environment.

Expected Results and Success Criteria

Before starting this lab, read through the tasks that you are expected to perform. What do you expect the result of performing these tasks will be?

_____

_____

_____

How is an understanding of ACLs useful in network administration?

_____

_____

_____

How will a network administrator know if the ACL is working properly?

_____

_____

_____

Background / Preparation

In this lab you will consider the need for data traffic control and filtering in a network, and design the policies to achieve this.

The traffic security design will then be applied to an example network using ACLs.

ACLs are typically applied at the Distribution Layer. This lab will use a router connected to a server that will provide sample network applications to demonstrate ACL placement and operation.

Step 1: Analyze the traffic filtering requirements

a. Determine the access and filtering requirements.

For this lab:

1) PC1 is a network administrator's workstation. This host must be permitted FTP and HTTP access to the network server, and telnet access to the router FC-CPE-1.

2) PC2 is a general workstation that is to have HTTP access only. FTP services and Telnet access to the router is not permitted.

b. Having determined specific requirements, decide if all other traffic is to be allowed or denied.

List the benefits and potential problems to the following filtering scenarios:

Benefits of allowing all other traffic:

_____

Potential problems with allowing all other traffic:

_____

Benefits of denying all other traffic:

_____

Potential problems with denying all other traffic:

_____

Step 2: Design and create the ACL

a. Review, and then apply, ACL recommended practice.

- Always plan thoroughly before implementation.
- The sequence of the statements is important. Put the more specific statements at the beginning and the more general statements at the end.
- Statements are added to the end of the ACL as they are written.
- Create and edit ACLs with a text editor and save the file.
- Use Named ACLs wherever possible.
- Use comments (**`remark`** option) within the ACL to document the purpose of the statements.
- To take effect, ACLs must be applied to an interface.
- An interface can have one ACL per Network Layer protocol, per direction.
- Although there is an implicit **`deny any`** statement at the end of every ACL, it is good practice to configure this explicitly. This ensures that you remember that the effect is in place and allows logging of matches to this statement to be used.
- ACLs with many statements take longer to process, which may affect router performance.
- Placement of ACLs:
    - Standard: closest to destination (if have administrative authority on that router)
    - Extended: closest to source (if have administrative authority on that router)

b. Consider the two approaches to writing ACLs:

- Permit specific traffic first and then deny general traffic.
- Deny specific traffic first and then permit general traffic.

When would it be best to permit specific traffic first and then deny general traffic?

_____

_____

When would it be best to deny specific traffic first and then permit general traffic?

_____

_____

c. Select one approach and write the ACL statements that will meet the requirements of this lab.

_____

_____

_____

_____

_____

_____

After an ACL is written and applied to an interface, it is useful to know if the ACL statements are having the desired effect. The number of packets that meet the conditions of each ACL statement can be logged by adding the option **log** at the end of each statement.

Why is it important to know to how many times packets that match an ACL statement are denied?

_____

_____

Step 3: Cable and configure the given network

NOTE: If the PCs used in this lab are also connected to your Academy LAN or to the Internet, ensure that you record the cable connections and TCP/IP settings so these can be restored at the conclusion of the lab.

a. Referring to the topology diagram, connect the console (or rollover) cable to the console port on the router and the other cable end to the host computer with a DB-9 or DB-25 adapter to the COM 1 port. Ensure that power has been applied to both the host computer and router.

b. Connect and configure the devices in accordance with the given topology and configuration. Your instructor may substitute Discovery Server with an equivalent server for this lab.

c. Establish a HyperTerminal, or other terminal emulation program, from PC1 to Router R1.

d. From the global configuration mode issue the following commands:

```
Router(config)#hostname FC-CPE-1

FC-CPE-1(config)#interface FastEthernet0/0
FC-CPE-1(config-if)#ip address 10.0.0.1 255.255.255.0
FC-CPE-1(config-if)#no shutdown
FC-CPE-1(config-if)#exit

FC-CPE-1(config)#interface FastEthernet0/1
FC-CPE-1(config-if)#ip address 172.17.0.1 255.255.0.0
FC-CPE-1(config-if)#no shutdown
FC-CPE-1(config-if)#exit

FC-CPE-1(config)#line vty 0 4
FC-CPE-1(config-line)#password telnet
FC-CPE-1(config-line)#login
FC-CPE-1(config-line)#end
```

e. Ping between PC1 and Discovery Server to confirm network connectivity. Troubleshoot and establish connectivity if the pings fail.

Step 4: Test the network services without ACLs

Perform the following tests on PC1:

a. Open a web browser on PC1 and enter the URL **http://172.17.1.1** at the address bar.

What web page was displayed?

_____

b. Open a web browser on PC1 and enter the URL **ftp://172.17.1.1** at the address bar.

What web page was displayed?

_____

c. On the Discovery FTP Home Directory, open the **Discovery 1** folder. Click and drag a Chapter file to the local Desktop.

Did the file copy successfully? _____

d. From the PC1 command line prompt, issue the command **telnet 10.0.0.1**, or use a Telnet client (HyperTerminal or TeraTerm, for example) to establish a Telnet session to the router.

What response did the router display?

_____

e. Exit the Telnet session.

Perform the following tests on PC2:

a. Open a web browser on PC2 and enter the URL **http://172.17.1.1** at the address bar.

What web page was displayed?

_____

b. Open a web browser on PC2 and enter the URL **ftp://172.17.1.1** at the address bar.

What web page was displayed?

_____

c. On the Discovery FTP Home Directory, open the **Discovery 1** folder. Click and drag a Chapter file to the local Desktop.

Did the file copy successfully? _____

d. From the PC2 command line prompt, issue the command **telnet 10.0.0.1**, or use a Telnet client (HyperTerminal or TeraTerm, for example) to establish a Telnet session to the router.

What response did the router display?

_____

e. Exit the Telnet session.

Why was each of the above connections successful?

_____

_____

If any of the above connections was not successful, troubleshoot the network and configurations and establish each type of connection from each host.

Step 5: Configure the network services ACL

From the global configuration mode issue the following commands:

a. Allow PC1 to access the web server and telnet to the router.

```
FC-CPE-1(config)#ip access-list extended Server-Access
FC-CPE-1(config-ext-nacl)#remark Allow PC1 access to server
FC-CPE-1(config-ext-nacl)#permit tcp host 10.0.0.10 host 172.17.1.1 eq
ftp www log
```


b. Allow PC2 to access the web server.

```
FC-CPE-1(config-ext-nacl)#remark Allow PC2 to access web server
FC-CPE-1(config-ext-nacl)#permit tcp host 10.0.0.201 host 172.17.1.1 eq
www log
```

c. Allow PC1 telnet access to router

```
FC-CPE-1(config-ext-nacl)#remark Allow PC1 to telnet router
FC-CPE-1(config-ext-nacl)#permit tcp host 10.0.0.10 host 10.0.0.1 eq telnet log
```

d. Deny all other traffic.

```
FC-CPE-1(config-ext-nacl)#remark Deny all other traffic
FC-CPE-1(config-ext-nacl)#deny ip any any log
FC-CPE-1(config-ext-nacl)#exit
```

Step 6: Apply the ACLs

a. Apply the Extended ACL to the router interface closest to the source.

```
FC-CPE-1(config)#interface FastEthernet0/0
FC-CPE-1(config-if)#ip access-group Server-Access in
FC-CPE-1(config-if)#end
```

b. From the Privileged EXEC mode, issue the **show running-configuration** command and confirm that the ACLs have been configured and applied as required.

Reconfigure if errors are noted.

Step 7: Test the network services with ACLs

Perform the following tests on PC1:

a. Open a web browser on PC1 and enter the URL **http://172.17.1.1** at the address bar.

What web page was displayed?

_____

b. Open a web browser on PC1 and enter the URL **ftp://172.17.1.1** at the address bar.

What web page was displayed?

_____

c. On the Discovery FTP Home Directory, open the **Discovery 1** folder. Click and drag a Chapter file to the local Desktop.

Did the file copy successfully? _____

Why is this the outcome?

_____

d. From the PC1 command line prompt, issue the command **telnet 10.0.0.1**, or use a Telnet client (HyperTerminal or TeraTerm, for example) to establish a Telnet session to the router.

What response did the router display?

_____

Why is this the outcome?

_____

e. Exit the Telnet session.

Perform the following tests on PC2:

a. Open a web browser on PC2 and enter the URL **http://172.17.1.1** at the address bar.

What web page was displayed?

_____

Why is this the outcome?

_____

b. Open a web browser on PC2 and enter the URL **ftp://172.17.1.1** at the address bar.

What web page was displayed?

_____

Why is this the outcome?

_____

c. From the PC2 command line prompt, issue the command **`telnet 10.0.0.1`**, or use a Telnet client (HyperTerminal or TeraTerm, for example) to establish a Telnet session to the router.

What response did the router display?

_____

Why is this the outcome?

_____

If any of these transactions did not result in the expected outcome, troubleshoot the network and configurations and retest the ACLs from each host.

Step 8: Observe the number of statement matches

a. From the Privileged EXEC mode, issue the command:

```
FC-CPE-1#show access-list Server-Access
```

List the number of matches logged against each ACL statement.

_____

_____

Step 9: Clean up

Erase the configurations and reload the routers and switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Challenge

Rewrite the Server-Access ACL used in this lab so that:

1) Administrator workstations are considered to be in the address range of 10.0.0.10 /24 to 10.0.0.15 /24 instead of a single host; and,

2) The general workstations have the address range of 10.0.0.16 /24 to 10.0.0.254 /24 instead of being a single host.

_____

_____

_____

_____

_____

_____

_____