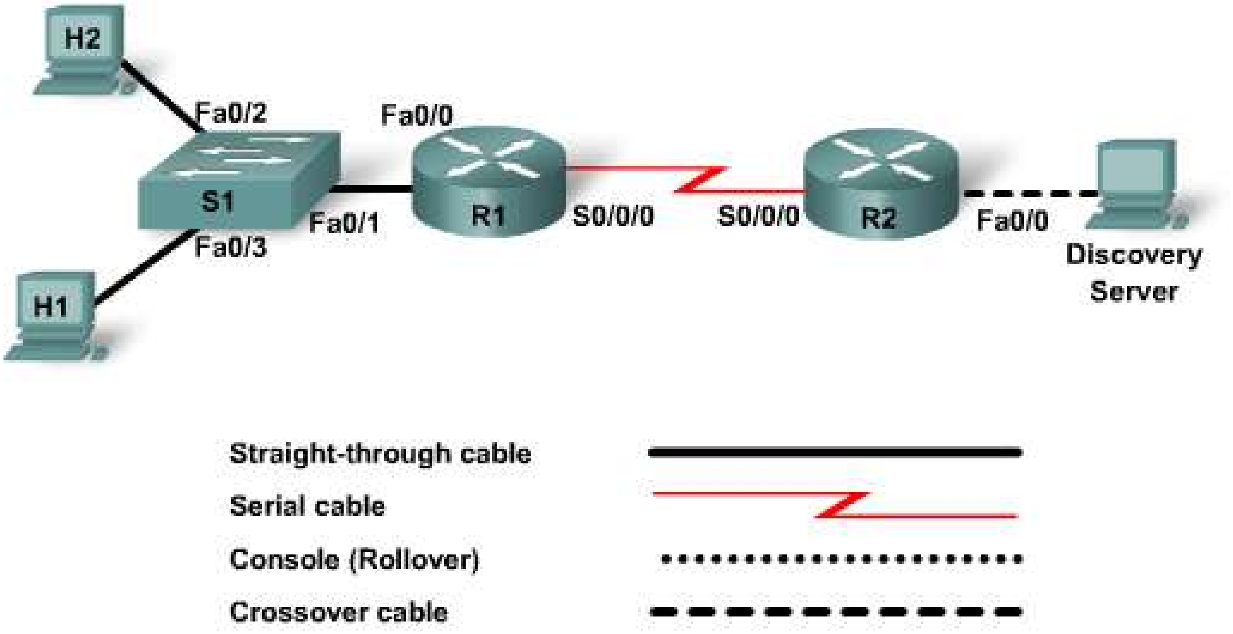
Lab 8.5.2 Configuring ACLs and Recording Activity to a Syslog Server



Device	Host Name	Fast Ethernet 0/0 IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Interface Type	Network Statements	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.1.1/24	192.168.15.1/30	DCE	192.168.1.0 192.168.15.0	class	Cisco
Router 2	R2	172.17.0.1/16	192.168.15.2/30	DTE	192.168.15.0 172.17.0.0	class	Cisco
Switch 1	S1					class	Cisco
Host 1	H1	192.168.1.5/24 DG: 192.168.1.1					
Host 2	H2	192.168.1.6/24 DG: 192.168.1.1					
Discovery Server	Server	172.17.1.1 DG: 172.17.0.1					

Objectives

- Configure and verify ACLs to control traffic.
- Verify ACLs using a syslog server.

Background / Preparation

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

The command syntax given in the lab may vary. For example, the interfaces may differ due to the router model. 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:

- Two Cisco 2960 switch or other comparable switch
- Two Cisco 1841 or comparable routers, each with a serial connection and an Ethernet interface
- Two Windows-based PCs, each with a terminal emulation program and set up as a host
- One Discovery Live CD for the server
- One PC to use as the Discovery Server
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switch
- Three straight-through Ethernet cables
- One crossover Ethernet cable
- One DTE/DCE serial cable
- Kiwi Syslog Daemon (downloadable from www.kiwisyslog.com or check with your instructor)

NOTE: Make sure that the routers and switch have been erased and have no startup configurations. Instructions for erasing both the switch and router are provided at the end of this lab.

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 at the end of this lab or contact your instructor if necessary.

NOTE: This lab makes use of the Discovery Server Live CD. For detailed instructions on the installation and configuration of the Discovery Server Live CD, please refer to the lab manual that is located on Academy Connection in the Tools Section.

Step 1: Connect the equipment

a. Connect the Serial 0/0/0 interface of Router 1 to the Serial 0/0/0 interface of Router 2 using a serial cable.

b. Connect the Fa0/0 interface of Router 1 to the Fa0/1 port on Switch 1 using a straight-through cable.

c. Connect Host 1 to the Fa0/3 port on Switch 1 using a straight-through cable.

d. Connect Host 2 to the Fa0/2 port on Switch 1 with a straight-through cable.

e. Connect the Discovery Server with a crossover cable to the Fa0/0 interface of Router 2.

Step 2: Perform basic configuration on Router 1

Step 3: Perform basic configuration on Router 2

Step 4: Perform basic configuration on Switch 1

Step 5: Configure the hosts with the proper IP address, subnet mask, and default gateway

a. Configure each host with the proper IP address, subnet mask, and default gateway.

1) Host 1 should be assigned 192.168.1.5 /24 and the default gateway of 192.168.1.1.

2) Host 2 should be assigned 192.168.1.6 /24 and the default gateway of 192.168.1.1.

3) The server should be assigned 172.17.1.1 and a default gateway of 172.17.0.1.

b. Each host should be able to ping the other hosts. If the ping is not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Configure and apply ACLs

ACLs will be configured to control what services Hosts 1 and 2 can access from the server. An ACL will be created that allows Host 1 web (HTTP) and FTP access to the server but denies Host 2. Host 2 will be allowed to telnet to the server, but this service is denied to Host 1. These ACLs will be configured and verified with **show** commands and logging. Logging will be enabled on the access control list statements.

a. Create an ACL based on the requirements previously outlined. This ACL is applied to R1.

```
R1(config)#access-list 110 remark Allow Host 1 web access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq www log
R1(config)#access-list 110 remark Allow Host 1 FTP access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq ftp log
R1(config)#access-list 110 remark Allow Host 2 Telnet access to server
R1(config)#access-list 110 permit tcp host 192.168.1.6 host 172.17.1.1
eq telnet log
R1(config)#access-list 110 remark Deny all other traffic
R1(config)#access-list 110 deny ip any any
```

b. Apply the ACL to the FastEthernet 0/0 interface on R1 in the inbound direction.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip access-group 110 in
```

c. From Host 1, open a web browser and attempt to connect to the web and FTP services on the server. In the web browser address textbox, enter **http://172.17.1.1**.

Is the web connection from Host 1 successful? __________

d. In the web browser address textbox, enter **ftp://172.17.1.1**.

Is the FTP connection from Host 1 successful? __________

e. Attempt to connect to the web and FTP services on the server from Host 2.

Are you able to connect from Host 2? __________

f. Attempt to telnet to the server from Host 1 and Host 2.

Is the Telnet connection from Host 1 successful? __________

Is the Telnet connection from Host 2 successful? __________

When these connections are attempted, console messages appear on R1 indicating the `access-list` lines matched by the various types of packets transmitted.

Step 7: Configure the syslog service on Host 2

Using the logging option in an `access-list` line provides helpful information but also has its disadvantages:

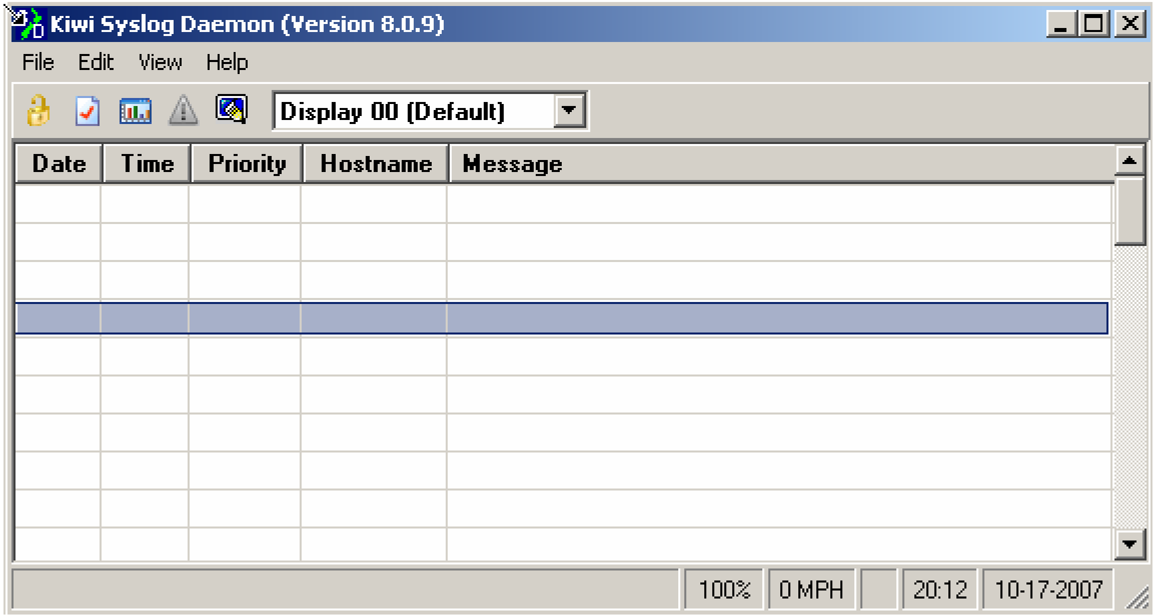
- It can require a lot of router resources.
- It also requires that a router console connection be active at all times or else messages are missed.

A solution that helps with both of these disadvantages is to log the messages to a syslog server. Logging messages to a syslog server reduces the load on the router and provides a destination for the messages. In addition, management tools are available to analyze syslog output to help detect patterns or problems.

Install the Kiwi Syslog Daemon on Host 2. If you need assistance with this, contact your instructor.

NOTE: A number of commercial and open source syslog servers are available. In this lab, the Kiwi syslog server is used. This software may be downloaded from www.kiwisyslog.com.

When the syslog server is running on the server, it should produce a display similar to this one:



The syslog service needs to be configured on the router. To do this properly involves setting the time and date on the router, enabling the timestamp service on the router, and configuring the router to send console messages to the syslog server.

Step 8: Configure the router to properly use the syslog service

Displaying the correct time and date on the syslog messages is vital when using syslog to monitor a network. If the correct time and date of a message is not known, it is sometimes impossible to determine what network event caused the message.

a. Set the correct time and date on the router. Replace the hours, minutes, seconds, month, day, and year variables with the proper values.

```
R1#clock set 15:22:00 may 17 2007
```

b. Configure the correct time zone on the router. Replace the zone name and offset with the correct values for your area.

```
R1(config)#clock timezone cdt -5
```

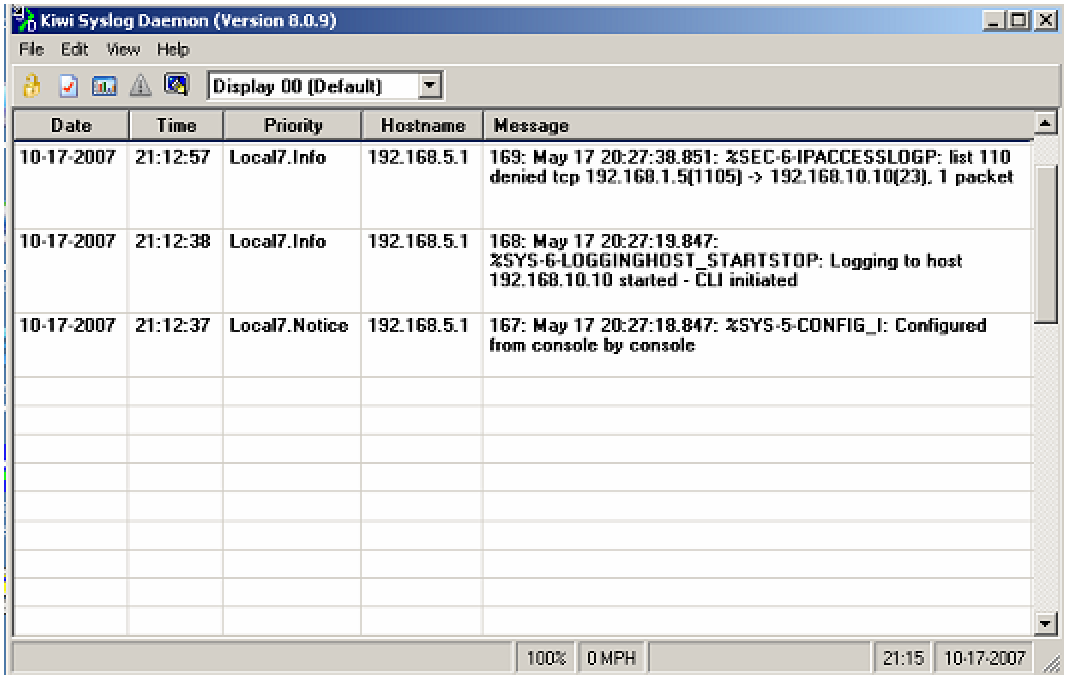
c. Enable the timestamp service on the router.

```
R1(config)#service timestamps
```

d. Configure the syslog service on the router to send syslog messages to the syslog server.

```
R1(config)#logging 192.168.1.6
```

e. Attempt to telnet from Host 1 to the server and then view the syslog display on the server. It should look similar to this example:



Date	Time	Priority	Hostname	Message
10-17-2007	21:12:57	Local7.Info	192.168.5.1	169: May 17 20:27:38.851: %SEC-6-IPACCESSLOGP: list 110 denied tcp 192.168.1.5(1105) -> 192.168.10.10(23), 1 packet
10-17-2007	21:12:38	Local7.Info	192.168.5.1	168: May 17 20:27:19.847: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.10 started - CLI initiated
10-17-2007	21:12:37	Local7.Notice	192.168.5.1	167: May 17 20:27:18.847: %SYS-5-CONFIG_I: Configured from console by console

f. Because logging is turned on at all levels, all console messages appear on the syslog output, including the configuration messages. To control the message display, set the logging level required to generate a message.

NOTE: The time and date appear in both the system message and as a function of the Kiwi syslog server.

g. With the current configuration, syslog messages are displayed on the syslog server and the console. With the syslog server displaying them, console logging can be turned off on router R1.

```
R1(config)#no logging console
```

h. Attempt various Telnet, web, and FTP connections from both hosts to the server and observe the results on the syslog server. In addition to viewing messages from the connection attempts, observe other messages from Hosts 1 and 2, such as NetBIOS broadcasts (UDP port 138).

Step 9: Reflection

a. State the advantages of using a syslog server instead of console logging.

____

____

What factor determines the maximum number of messages stored on the syslog server?

____