**Discovery 20: Configure Syslog**

**Introduction**

The objective of this discovery lab is to provide you with some experience with the syntax of basic syslog configuration to facilitate the management of Cisco IOS devices. This lab is prepared with the router and server that is represented in the topology diagram and the connectivity table. The devices have their basic configurations in place, including hostnames and IP addresses.

Your configuration task is as follows:

* Configure the Router to Log to Server

**Task 1: Configure the Router to Log to Server**

**Activity**

**Step 1:** On R1, define SRV1 (10.1.1.10) as the R1 syslog server.

On R1, enter the following commands:

R1# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)# logging 10.1.1.10



**Step 2:** Set the minimal severity threshold to log to the server to "informational."

On R1, enter the following commands:

R1(config)# logging trap informational

R1(config)# end

R1#



Notice that two syslog messages are displayed to the console indicating that configuration has occurred on the console and logging has started to the server at 10.1.1.10. The first message is of severity 5 (Notification), and the second message is of severity 6 (Informational).

Setting the threshold to "informational" means that messages of severity 0 through 6 will be forwarded to the syslog server. Both of these messages are forwarded.

**Step 3:** Enter the show logging command to display the syslog status and the local logging buffer.

On R1, enter the following command:

R1# show logging





The output indicates that R1 is now sending syslog messages to 10.1.1.10, with the minimum severity threshold set to "informational." The output also indicates that two messages have been sent to the syslog server. Syslog uses UDP for transport and is inherently not reliable. If these two messages are lost somewhere in the transport path, there is no mechanism to recognize the lost message or to request a retransmission.

There is a local logging buffer. It is in its default state, with a severity threshold of "debugging" (Severity 7) and sized at 4096 bytes. In the sample transcript, 32 messages have been logged in the local buffer. The end of the show logging command output displays the contents of the buffer. At this point in the discovery, the buffer is mostly filled with the messages that were produced when R1 booted. At the end of the buffer, however, are the two syslog messages that were produced as a result of the syslog configuration activity.

**Step 4:** Initiate some activity that will generate more syslog messages. On R1, enter global configuration mode, enable the Ethernet0/3 interface, then disable the interface, and leave the configuration mode.

On R1, enter the following commands:

R1# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)# interface g0/3

R1(config-if)# no shutdown

R1(config-if)# shutdown

R1(config-if)# end

R1#



**Note**

This sample activity caused the generation of five syslog messages.

**Step 5:** Display the logging status and the local logging buffer.

On R1, enter the following command:

R1# show logging





Additional messages were logged to 10.1.1.10.

**Note**

The five syslog messages that were produced in response to your previous activity are at the end of the local logging buffer.