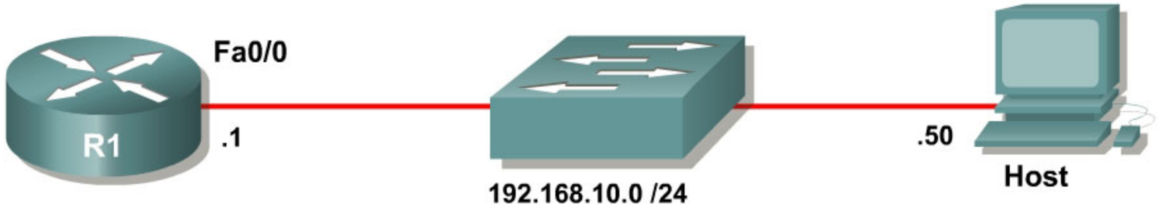
Lab 5.5 Configuring Logging

Learning Objectives

- Configure a router to log to a Syslog server
- Use Kiwi Syslog Daemon as a Syslog server
- Configure local buffering on a router

Topology Diagram



Scenario

In this lab, you will configure a router to log system messages and notifications to a Syslog server. You will also view the logs on the Syslog server.

Step 1: Configure the interface

Configure the router interface shown in the topology diagram.

```
R1(config)# interface fastethernet0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
```

Apply the IP address shown in the topology diagram to the host. If you do not know how to set up an IP address on a host, consult Lab 3.1: Configuring SDM on a Router.

Verify that you have connectivity between R1 and the host with the **ping** command.

```
R1# ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Step 2: Install the Kiwi Syslog Daemon

This lab uses the Kiwi Syslog Daemon, which is a free Syslog server for use with Microsoft Windows. If it is not currently installed on the host, download the installer from http://www.kiwisyslog.com. If it is installed, skip to step 3.

As of the time of this writing, there are two versions of this software: a free version and a licensed version. This lab uses only the features found in the free version. When prompted to install the program as a service or application, you can choose whether you want the Syslog daemon started automatically as a system service or triggered by user action, like a normal Windows application. This lab was written using the service installation.

Step 3: Run the Kiwi Syslog Service Manager

Open the Kiwi Syslog Daemon Manager, which can be accessed either by the icon on the host's desktop labeled **Kiwi Syslog Daemon** or by clicking on the **Start** button and choosing **Programs > Kiwi Enterprises > Kiwi Syslog Daemon > Kiwi Syslog Daemon**.

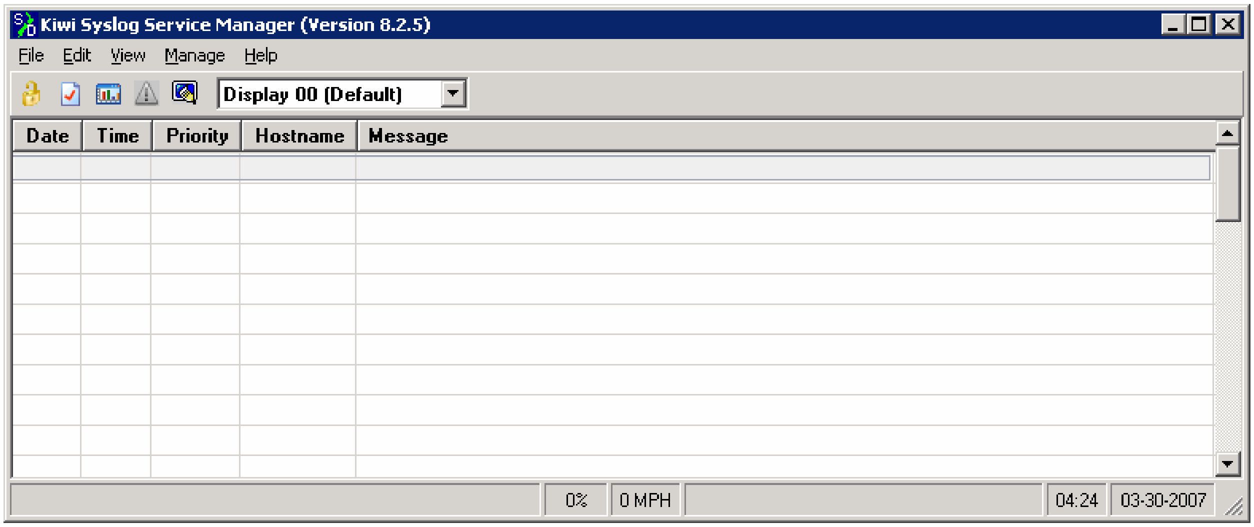


Figure 3-1: Kiwi Syslog Daemon Manager Main Window

If this is your first time running the program after installing it, choose **Manage > Install the Syslogd service**. You need to start the service if you just installed it, or if you are not sure the service is running. Start the service with **Manage > Start the Syslogd service**. You can check if the service is running by selecting **Manage > Ping the Syslogd service**.

Step 4: Configure the Router for Logging

Configuring a router to use a Syslog server is a relatively simple process and only requires a few commands in global configuration mode.

First, configure the IP address of a Syslog server with the **logging host** *hostname* command. In this lab, use an IP address instead of a hostname.

```
R1(config)# logging host 192.168.10.50
```

Set the Syslog severity level with the global configuration command **logging trap** *level*. You can specify the severity level by either using a keyword or an integer from 0 to 7.

```
R1(config)# logging trap ?
  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
  <cr>
```

The severity levels in order are as follows:

- Emergencies – 0
- Alerts – 1
- Critical – 2
- Errors – 3
- Warnings – 4
- Notifications – 5
- Informational – 6 (default)
- Debugging –7

Each severity level includes the severity levels with lower numbers. This may seem a little counter-intuitive, so predict what will happen in this example.

Predict which severity levels of messages would be logged if you issued the following command:

```
Router(config)# logging trap critical
```

The default level is 6, informational logging. To demonstrate the command, set the logging trap level to informational. Note that the command does not show up in the running configuration, because it is the default.

```
R1(config)# logging trap informational
```

Generate some logging messages for your log server by configuring your device to log users entering and exiting privileged mode with the **logging userinfo** command. When you have completed entering commands, enter the **end** command to exit configuration mode. This user action generates a Syslog message that the router was just configured. There may also be another Syslog message stating that logging to the host just started.

```
R1(config)# logging userinfo
R1(config)# end
R1#

*Mar 30 08:39:23.458: %SYS-5-CONFIG_I: Configured from console by console
*Mar 30 08:39:24.458: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
192.168.10.50 started - CLI initiated
```

You may also want to verify logging settings with the **show logging** command.

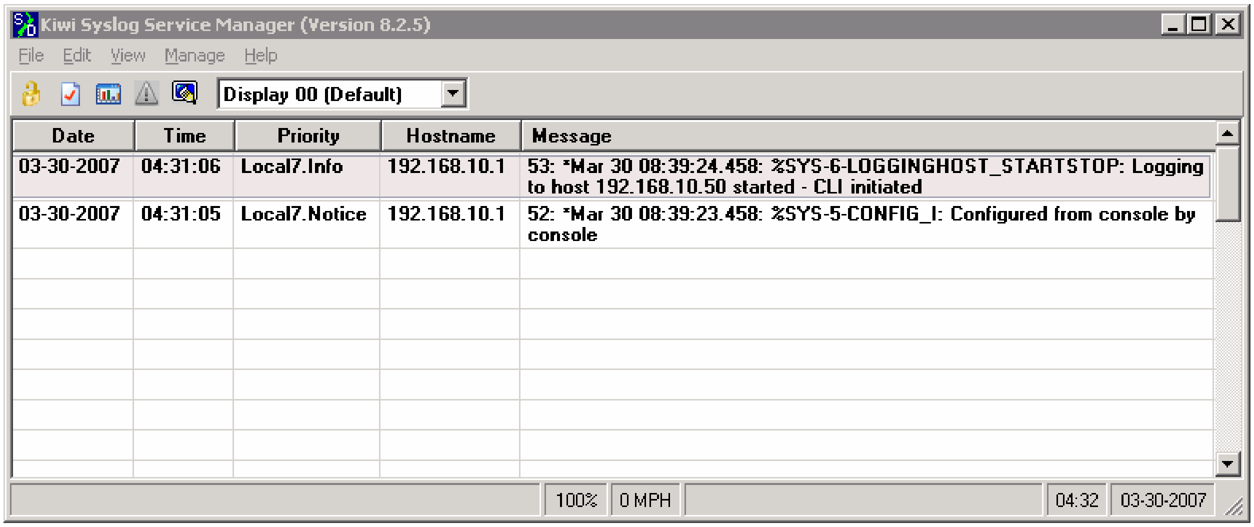
```
R1# show logging
Syslog logging: enabled (11 messages dropped, 1 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 46 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: disabled, xml disabled,
                    filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled

No active filter modules.

    Trap logging: level informational, 50 message lines logged
        Logging to 192.168.10.50(global) (udp port 514, audit disabled, link
up), 2 message lines logged, xml disabled,
               filtering disabled
```

Step 5: Verify Logging

On the host, look at the Kiwi Syslog Daemon Manager. The log messages that were just created will be displayed.


Kiwi Syslog Service Manager (Version 8.2.5)
File Edit View Manage Help
Display 00 (Default)
100%
0 MPH
04:32
03-30-2007

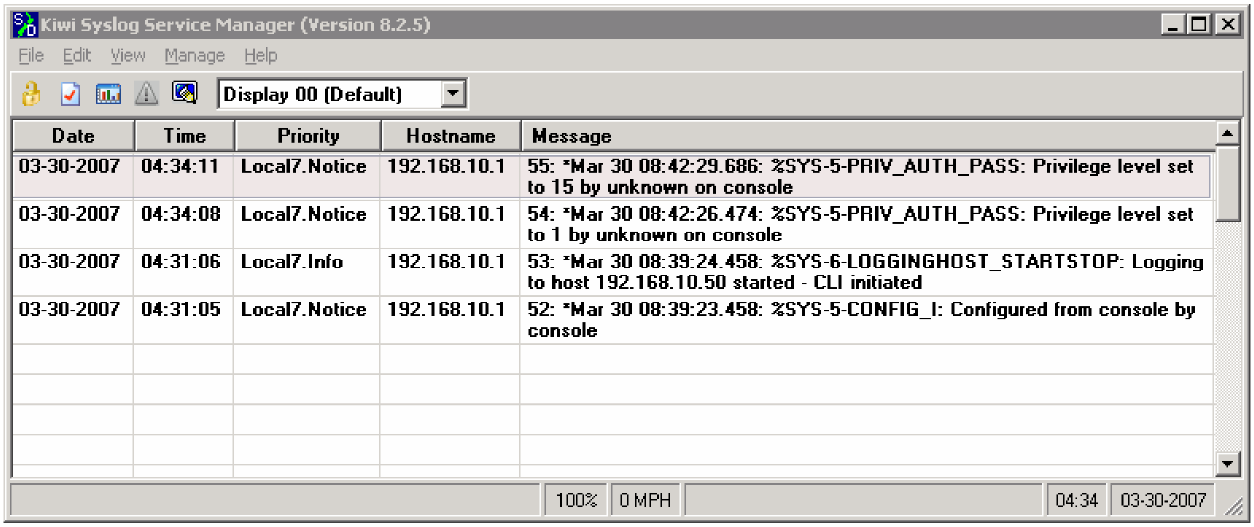
Date	Time	Priority	Hostname	Message
03-30-2007	04:31:06	Local7.Info	192.168.10.1	53: *Mar 30 08:39:24.458: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.50 started - CLI initiated
03-30-2007	04:31:05	Local7.Notice	192.168.10.1	52: *Mar 30 08:39:23.458: %SYS-5-CONFIG_I: Configured from console by console

Figure 5-1: Informational Log Messages from R1

On the router, exit privileged EXEC mode, and then reenter it using the **enable** command.

Log messages will appear on the router as well as in the Kiwi Syslog Daemon Manager. The reason log messages are generated is because of the **logging userinfo** command you issued earlier.

```
R1# disable
*Mar 30 08:42:26.474: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 1 by
unknown on console
R1> enable
*Mar 30 08:42:29.686: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 15 by
unknown on console
R1#
```


Kiwi Syslog Service Manager (Version 8.2.5)
File Edit View Manage Help
Display 00 (Default)
100%
0 MPH
04:34
03-30-2007

Date	Time	Priority	Hostname	Message
03-30-2007	04:34:11	Local7.Notice	192.168.10.1	55: *Mar 30 08:42:29.686: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 15 by unknown on console
03-30-2007	04:34:08	Local7.Notice	192.168.10.1	54: *Mar 30 08:42:26.474: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 1 by unknown on console
03-30-2007	04:31:06	Local7.Info	192.168.10.1	53: *Mar 30 08:39:24.458: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.50 started - CLI initiated
03-30-2007	04:31:05	Local7.Notice	192.168.10.1	52: *Mar 30 08:39:23.458: %SYS-5-CONFIG_I: Configured from console by console

Figure 5-2: User Information Log Messages from R1

Why it is better to have centralized logging servers rather than only have the routers log locally?

Step 6: Configure Buffered Logging

In cases where you have a small network and do not have a centralized logging server, you may consider buffering logs to a local memory buffer. The commands coincide with those used for the Syslog server.

Issue the **logging buffered** [*bytes*] [*severity-level*] command on R1 to begin buffering to the local buffer. Use the informational level and set the buffer size to 32 KB. Exit global configuration mode, which generates a log message.

```
R1(config)# logging buffered 32768 informational
R1(config)# exit
R1#

*Mar 30 14:44:56.968: %SYS-5-CONFIG_I: Configured from console by console
```

Issue the **show logging** command to get general information about the buffer and view the buffer log.

```
R1# show logging
Syslog logging: enabled (11 messages dropped, 1 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 54 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level informational, 1 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled

No active filter modules.

    Trap logging: level informational, 58 message lines logged
        Logging to 192.168.10.50(global) (udp port 514, audit disabled, link
up), 6 message lines logged, xml disabled,
               filtering disabled

Log Buffer (32768 bytes):

*Mar 30 14:44:56.968: %SYS-5-CONFIG_I: Configured from console by console
```

Exit privileged EXEC mode and then reenter it. This generates some user information messages that are saved to the memory buffer.

```
R1# disable
```

```
*Mar 30 14:45:22.272: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 1 by
unknown on console

R1> enable
R1#
*Mar 30 14:45:23.200: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 15 by
unknown on console
```

Display the contents of the internal buffer again with the **show logging** command.

```
R1# show logging
Syslog logging: enabled (11 messages dropped, 1 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 56 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level informational, 3 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled

No active filter modules.

    Trap logging: level informational, 60 message lines logged
        Logging to 192.168.10.50(global) (udp port 514, audit disabled, link
up), 8 message lines logged, xml disabled,
               filtering disabled

Log Buffer (32768 bytes):

*Mar 30 14:44:56.968: %SYS-5-CONFIG_I: Configured from console by console
*Mar 30 14:45:22.272: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 1 by
unknown on console
*Mar 30 14:45:23.200: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 15 by
unknown on console
```

Final Configuration

```
R1# show run
!
hostname R1
!
logging userinfo
logging buffered 32768 informational
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
logging 192.168.10.50
!
end
```