Lab 11.5.6.3 Configure Syslog and SNMP on the Bridge

Estimated Time: 25 minutes

Number of Team Members: Students will work in teams of two.

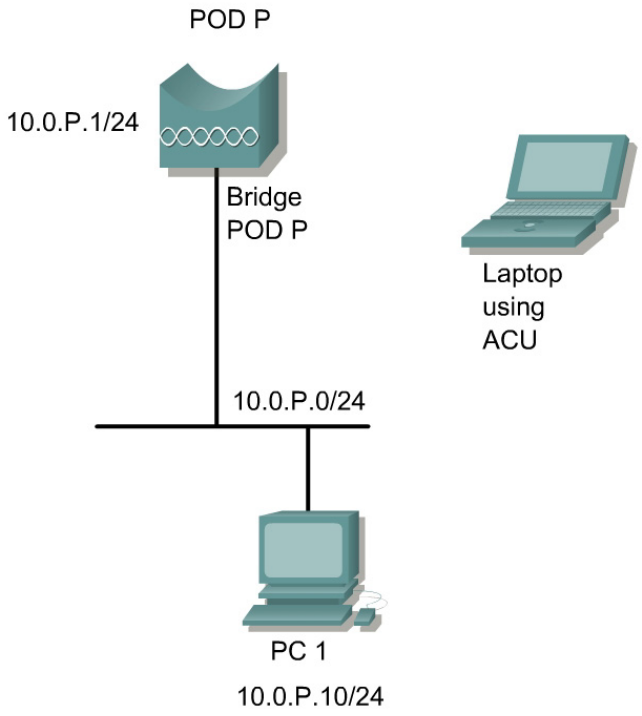
Objective

In this lab, students will configure and use syslog logging to monitor network events. Also, the student will configure the contact and location of the SNMP agent and test the configuration.

Scenario

A network security administrator should always log significant events on the bridge to the syslog or SNMP server. A server should be located on a secure internal network to ensure log integrity. The server can be a dedicated server or another server running syslog services or SNMP

Topology



Preparation

The student will read and understand material presented in FWL Chapter 11 prior to this lab.

Tools and resources

The following tools and resources are required:

- One BR350
- A wired PC (PC1) acting as the syslog and syslog server with a static IP address
- A PC or laptop with a properly installed wireless client adapter and utility

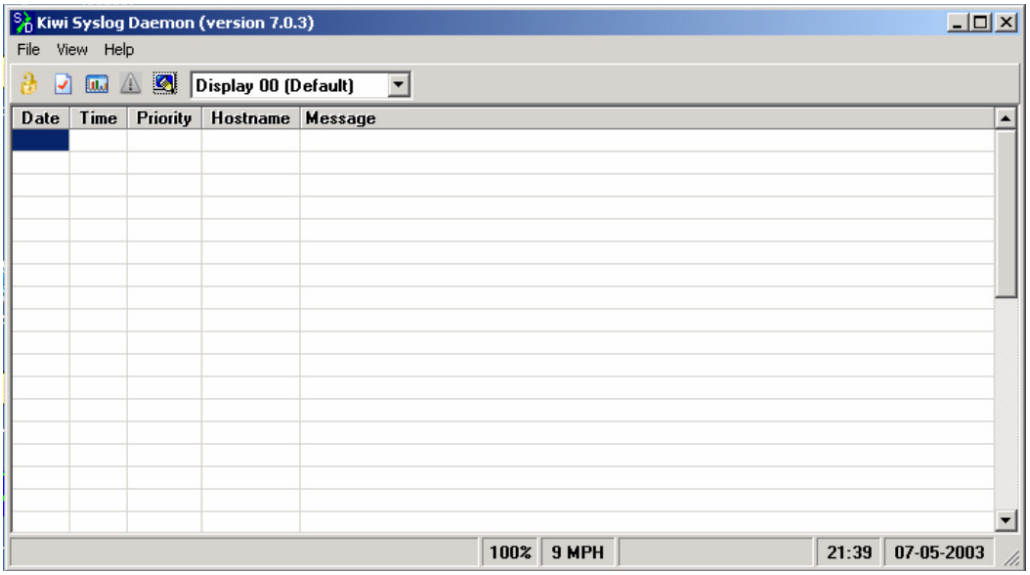
Step 1 Download and install the software

Go to the following web sites and download Kiwi Syslog Daemon Standard version software

http://www.kiwisyslog.com/software_downloads.htm

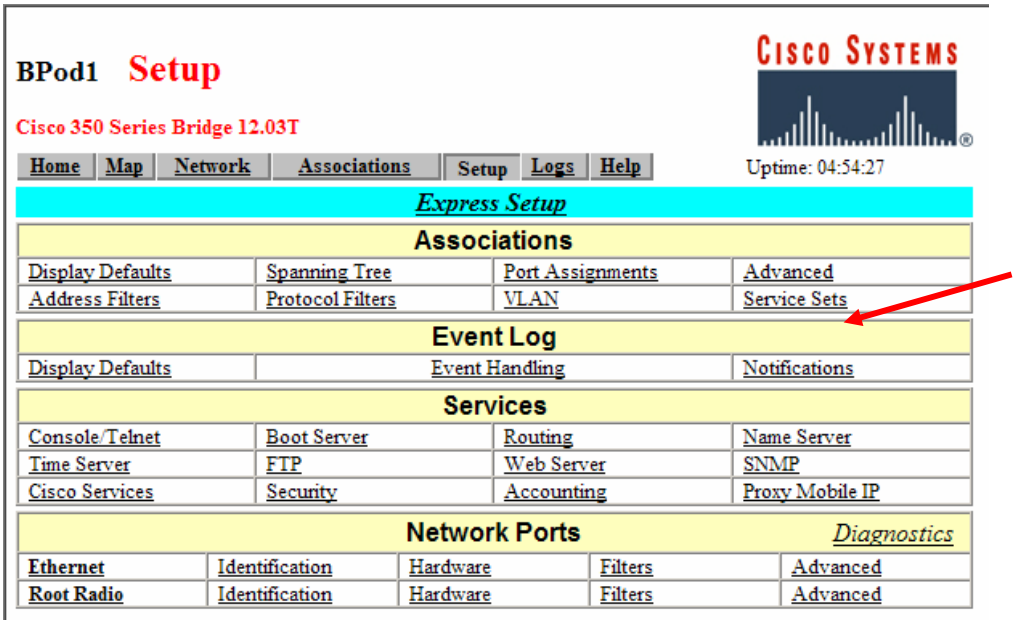
Install the program on PC1.

Step 2 Setup and execute the Kiwi Syslog Daemon

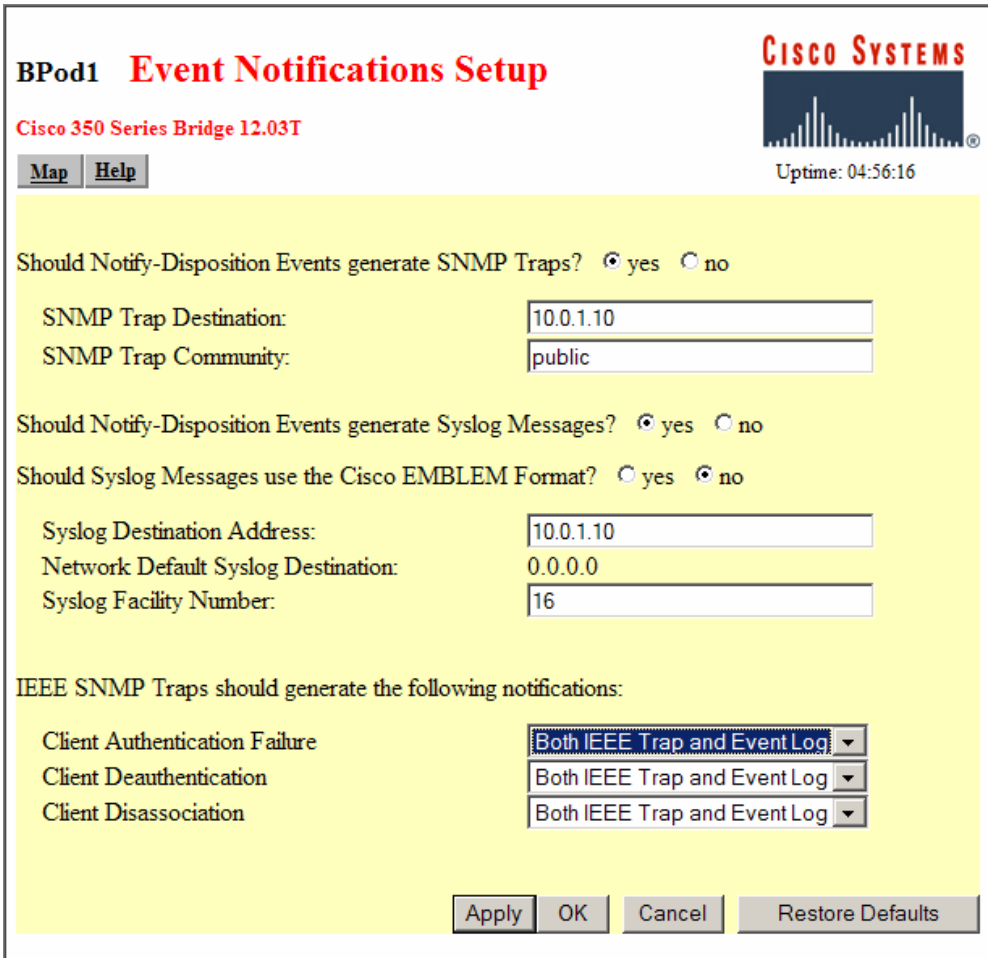


a. Click on the **Kiwi Syslog Daemon** Icon on the desktop to bring up the syslog application. The Kiwi Syslog Daemon can be customized or the defaults can be used.

Step 3 Enable logging on the bridge

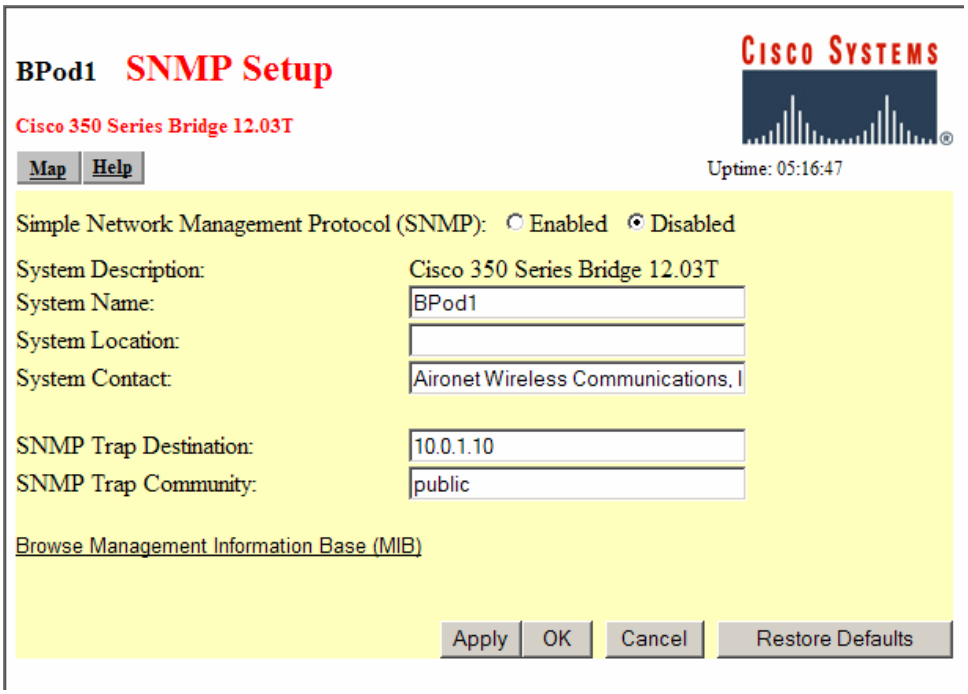


a. From the Setup Page, click on the **Event Log** Notifications link.



b. Type in the Syslog and SNMP Destination Host IP address. This should be 10.0.P.10

c. Click the **Apply** button to begin logging events to the Kiwi Syslog.



d. From the Setup Page, click on the **Services** SNMP link.

e. Click on the **Enabled** radio button to enable SNMP.

f. Configure a System location and contact.

g. Click the **Apply** button to begin logging events to the SNMP Trap Watcher.

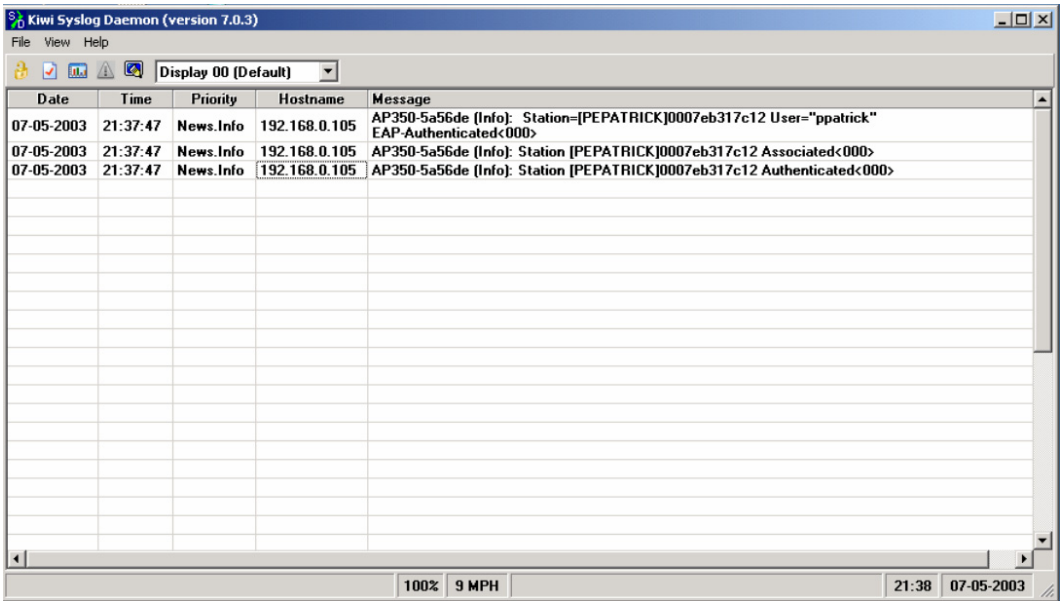
Step 4 View event logs

Configuring logging is only half of the logging scenario. A security administrator must monitor the logs on a daily basis.

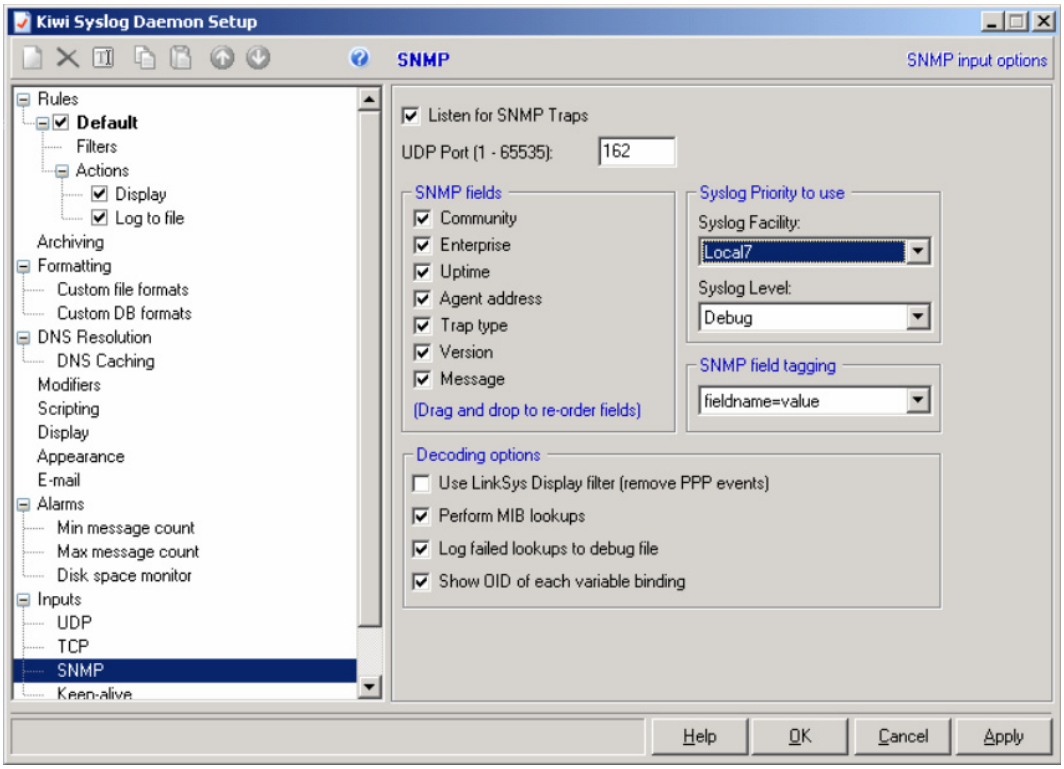
Generate events to the syslog by logging into the bridge that is being monitored.

a. Have a wireless user connect to the bridge.

b. Have the wireless user disconnect from the bridge.



c. View the messages in the Kiwi syslog window. The Hostname should match the IP address of the bridge.



d. Click on the **Setup** icon located in the upper left corner of the syslog program window.

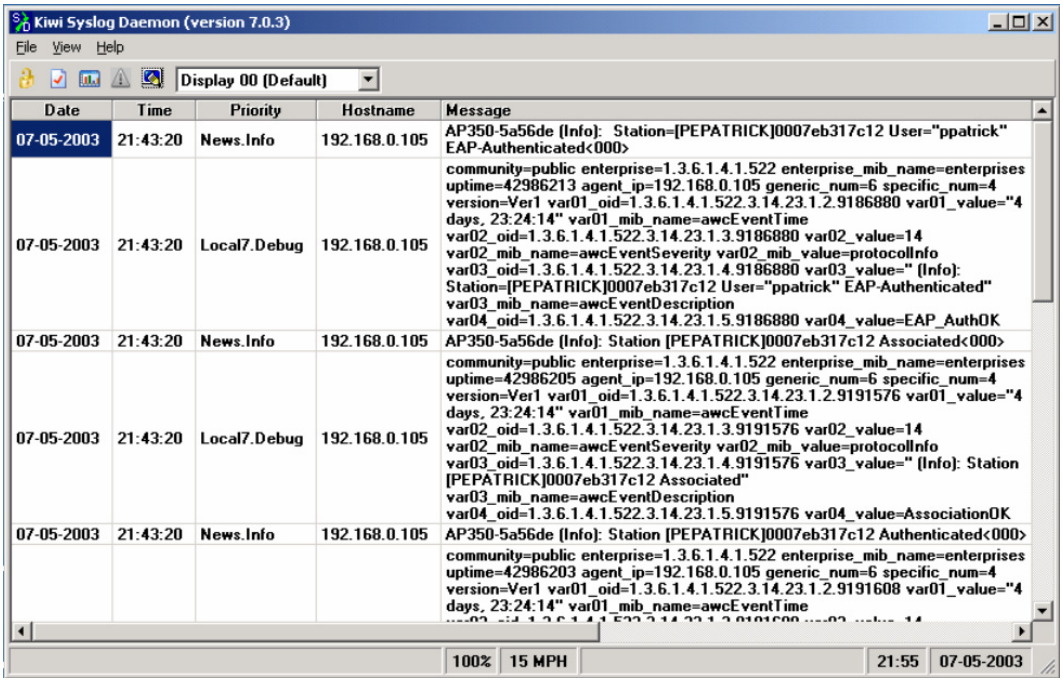
e. Configure SNMP on Kiwi Syslog Daemon by checking the **Listen for SNMP Traps** box.

f. Click the OK button to save the changes.

g. Have a wireless user connect to the bridge.

h. Have the wireless user disconnect from the bridge.

i. View the main logging screen on Kiwi.



j. Notice the SNMP messages contain much more information than the syslog messages. The Hostname should match the IP address of the bridge.

k. When using the Cisco WLAN Solutions engine or other enterprise level SNMP applications, SNMP can be used for monitoring and management.

