



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.

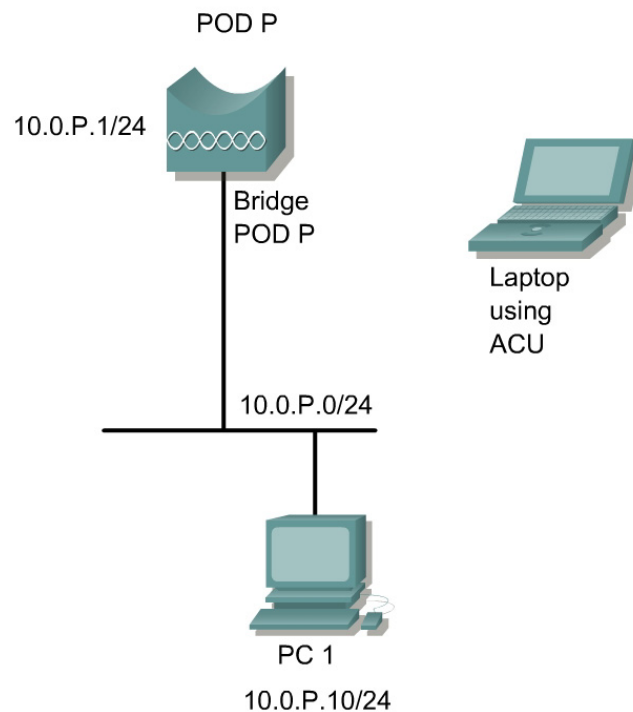
Objective

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

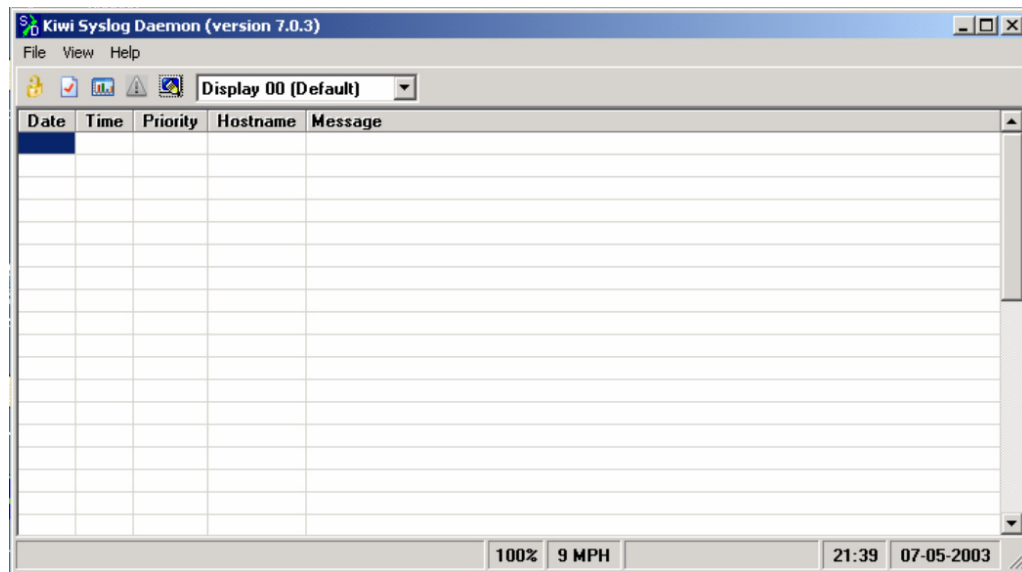
Step 1 Download and install the software

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



- 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

BPod1 Setup
Cisco 350 Series Bridge 12.03T

CISCO SYSTEMS
Uptime: 04:54:27

Home Map Network Associations Setup Logs Help

Express Setup

Associations

Display Defaults	Spanning Tree	Port Assignments	Advanced
Address Filters	Protocol Filters	VLAN	Service Sets

Event Log

Display Defaults	Event Handling	Notifications
----------------------------------	--------------------------------	-------------------------------

Services

Console/Telnet	Boot Server	Routing	Name Server
Time Server	FTP	Web Server	SNMP
Cisco Services	Security	Accounting	Proxy Mobile IP

Network Ports [Diagnostics](#)

Ethernet	Identification	Hardware	Filters	Advanced
Root Radio	Identification	Hardware	Filters	Advanced

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

BPod1 Event Notifications Setup
Cisco 350 Series Bridge 12.03T

CISCO SYSTEMS
Uptime: 04:56:16

Map Help

Should Notify-Disposition Events generate SNMP Traps? ☒ yes ☐ no

SNMP Trap Destination:

SNMP Trap Community:

Should Notify-Disposition Events generate Syslog Messages? ☒ yes ☐ no

Should Syslog Messages use the Cisco EMBLEM Format? ☐ yes ☒ no

Syslog Destination Address:

Network Default Syslog Destination:

Syslog Facility Number:

IEEE SNMP Traps should generate the following notifications:

Client Authentication Failure	<input type="text" value="Both IEEE Trap and Event Log"/>
Client Deauthentication	<input type="text" value="Both IEEE Trap and Event Log"/>
Client Disassociation	<input type="text" value="Both IEEE Trap and Event Log"/>

Apply OK Cancel Restore Defaults

- 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.

BPod1 SNMP Setup

Cisco 350 Series Bridge 12.03T

Map Help Uptime: 05:16:47

Simple Network Management Protocol (SNMP): ☐ Enabled ☒ Disabled

System Description: Cisco 350 Series Bridge 12.03T

System Name: BPod1

System Location:

System Contact: Aironet Wireless Communications, I

SNMP Trap Destination: 10.0.1.10

SNMP Trap Community: public

[Browse Management Information Base \(MIB\)](#)

Apply OK Cancel Restore Defaults

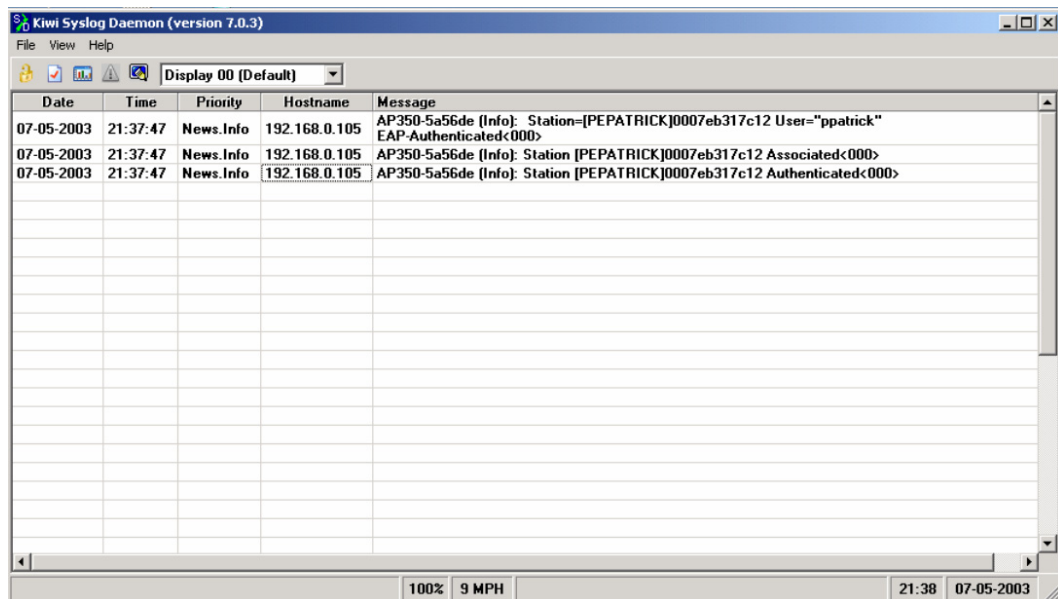
- d. From the Setup Page, click on the **Services** SNMP link.
- e. Click on the **Enabled** radio button to enable SNMP.
- f. Configure a System location and contact.
- g. Click the **Apply** button to begin logging events to the SNMP Trap Watcher.

Step 4 View event logs

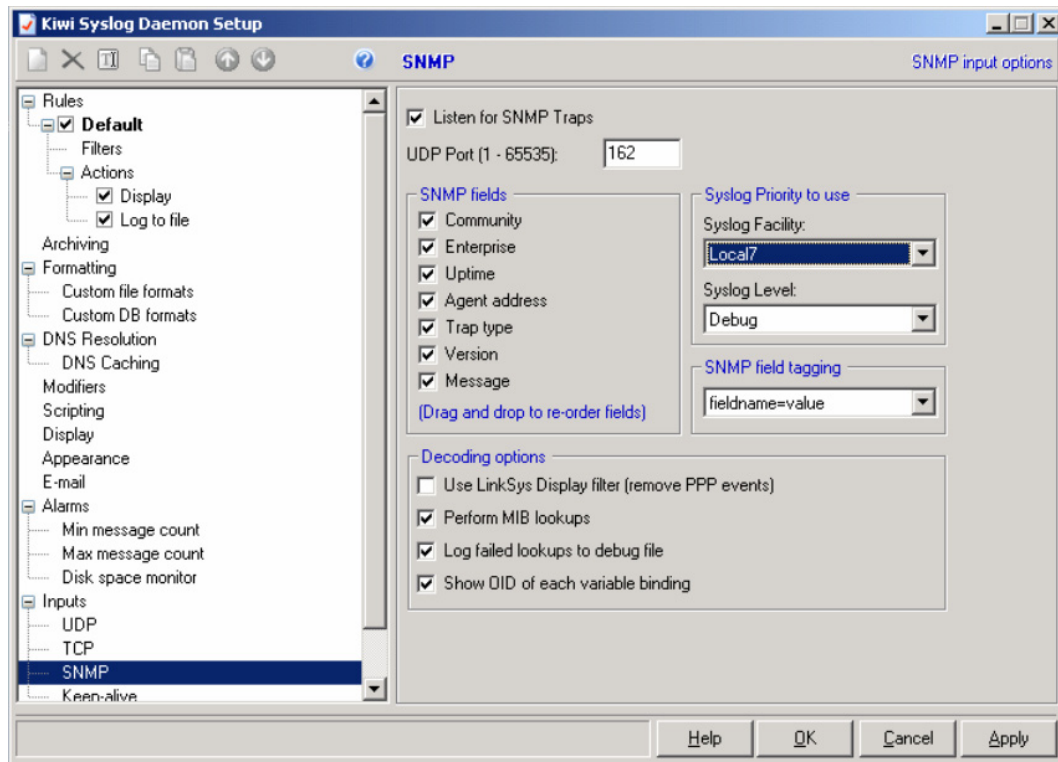
Configuring logging is only half of the logging scenario. A security administrator must monitor the logs on a daily basis.


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.

Date	Time	Priority	Hostname	Message
07-05-2003	21:43:20	News.Info	192.168.0.105	AP350-5a56de (Info): Station=[PEPATRICK]0007eb317c12 User="ppatrick" EAP-Authenticated<000>
07-05-2003	21:43:20	Local7.Debug	192.168.0.105	community=public enterprise=1.3.6.1.4.1.522 enterprise_mib_name=enterprises uptime=42986213 agent_ip=192.168.0.105 generic_num=6 specific_num=4 version=Ver1 var01_oid=1.3.6.1.4.1.522.3.14.23.1.2.9186880 var01_value="4 days, 23:24:14" var01_mib_name=awcEventTime var02_oid=1.3.6.1.4.1.522.3.14.23.1.3.9186880 var02_value=14 var02_mib_name=awcEventSeverity var02_mib_value=protocolInfo var03_oid=1.3.6.1.4.1.522.3.14.23.1.4.9186880 var03_value=" (Info): Station=[PEPATRICK]0007eb317c12 User="ppatrick" EAP-Authenticated" var03_mib_name=awcEventDescription var04_oid=1.3.6.1.4.1.522.3.14.23.1.5.9186880 var04_value=EAP_AuthOK
07-05-2003	21:43:20	News.Info	192.168.0.105	AP350-5a56de (Info): Station [PEPATRICK]0007eb317c12 Associated<000>
07-05-2003	21:43:20	Local7.Debug	192.168.0.105	community=public enterprise=1.3.6.1.4.1.522 enterprise_mib_name=enterprises uptime=42986205 agent_ip=192.168.0.105 generic_num=6 specific_num=4 version=Ver1 var01_oid=1.3.6.1.4.1.522.3.14.23.1.2.9191576 var01_value="4 days, 23:24:14" var01_mib_name=awcEventTime var02_oid=1.3.6.1.4.1.522.3.14.23.1.3.9191576 var02_value=14 var02_mib_name=awcEventSeverity var02_mib_value=protocolInfo var03_oid=1.3.6.1.4.1.522.3.14.23.1.4.9191576 var03_value=" (Info): Station [PEPATRICK]0007eb317c12 Associated" var03_mib_name=awcEventDescription var04_oid=1.3.6.1.4.1.522.3.14.23.1.5.9191576 var04_value=AssociationOK
07-05-2003	21:43:20	News.Info	192.168.0.105	AP350-5a56de (Info): Station [PEPATRICK]0007eb317c12 Authenticated<000>
07-05-2003	21:43:20	Local7.Debug	192.168.0.105	community=public enterprise=1.3.6.1.4.1.522 enterprise_mib_name=enterprises uptime=42986203 agent_ip=192.168.0.105 generic_num=6 specific_num=4 version=Ver1 var01_oid=1.3.6.1.4.1.522.3.14.23.1.2.9191608 var01_value="4 days, 23:24:14" var01_mib_name=awcEventTime var02_oid=1.3.6.1.4.1.522.3.14.23.1.3.9191608 var02_value=14 var02_mib_name=awcEventSeverity var02_mib_value=protocolInfo var03_oid=1.3.6.1.4.1.522.3.14.23.1.4.9191608 var03_value=" (Info): Station [PEPATRICK]0007eb317c12 Authenticated" var03_mib_name=awcEventDescription var04_oid=1.3.6.1.4.1.522.3.14.23.1.5.9191608 var04_value=AuthenticationOK

- 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.