Lab 11.5.6.2 Configure SNMP on AP

Estimated Time: 20 minutes

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

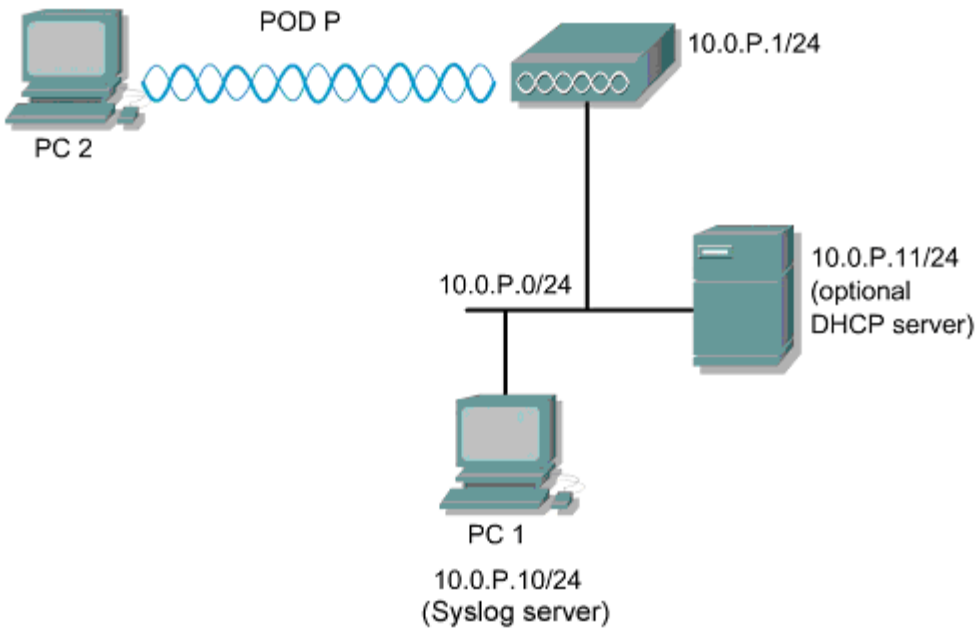
Objective

In this lab, the student will install and configure the Kiwi Syslog Daemon to listen for SNMP logs. The student will configure the contact and location of the SNMP agent and test the configuration.

Scenario

SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the TCP/IP protocol suite. SNMP uses User Datagram Protocol (UDP) port 161 for most requests and responses. SNMP traps use UDP port 162.

Topology



Preparation

Team	AP Name	SSID	Address
1	Pod1	AP1	10.0.1.1/24
2	Pod2	AP2	10.0.2.1/24

Tools and resources

The following tools and resources are required:

- One AP 1200
- A wired PC (PC1) acting as the SNMP server.
- A wireless PC or laptop with ACU

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise:

Command	Description
no snmp-server	Disable SNMP.
show snmp	Monitors SNMP status.
snmp-server community	Defines the community access string.
snmp-server contact	Sets the system contact string.
snmp-server enable traps snmp	Enables the sending of traps, and specifies the type of notification to be sent.
snmp-server host	Configures the recipient of an SNMP trap operation.
snmp-server location	Sets the system location string.

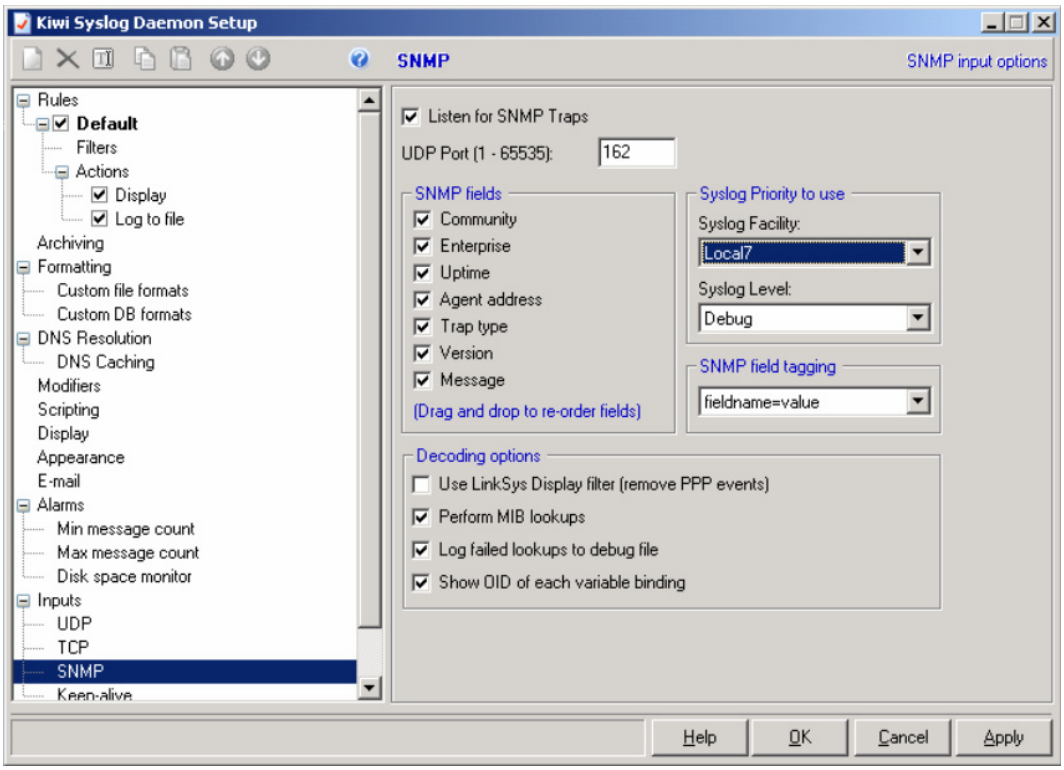
Step 1 Download and install the software

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

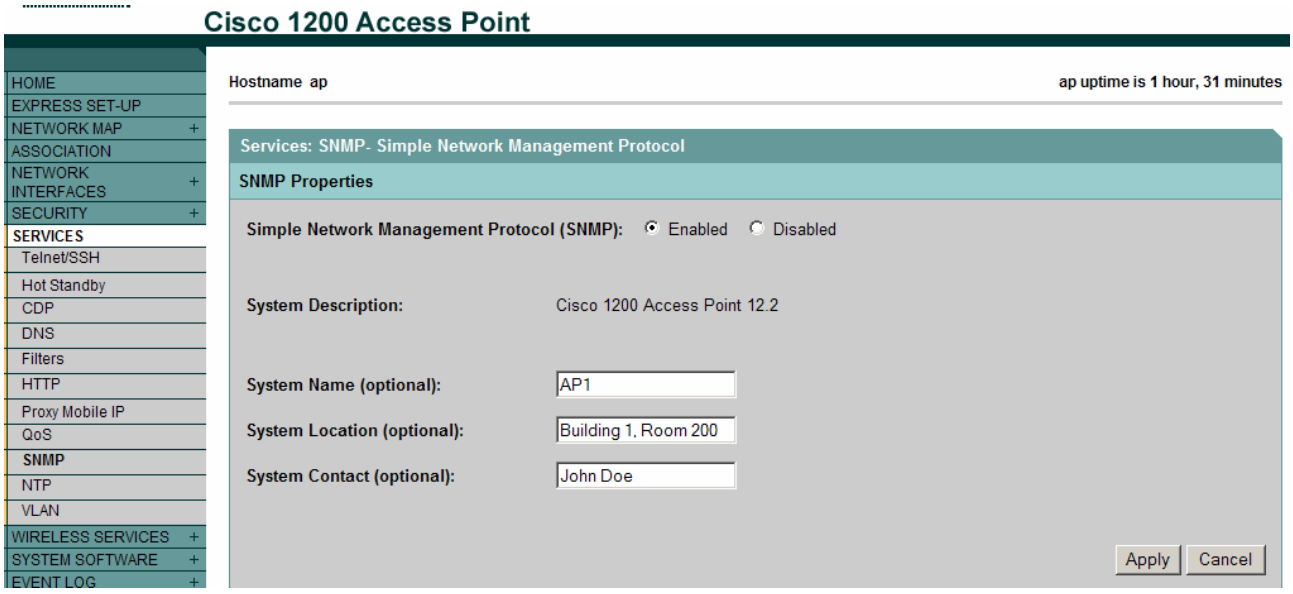
b. Configure SNMP on Kiwi Syslog Daemon by checking the **Listen for SNMP Traps** box.

c. Click the **OK** button to save the changes.

d. What UDP port does SNMP Trap Watcher listen on?

_____

Step 3 Use the web browser to setup SNMP



a. Ensure the AP is configured according to the Topology and Preparation table. Ping from PC1, located at 10.0.P.10 to the AP to ensure connectivity.

b. Browse to the **SERVICES>SNMP** Page of the AP.

c. Click the Enabled radio button to Enable SNMP on the AP.

d. Set a System Name (this is optional, but useful)

e. Set a System Location (this is optional, but useful)

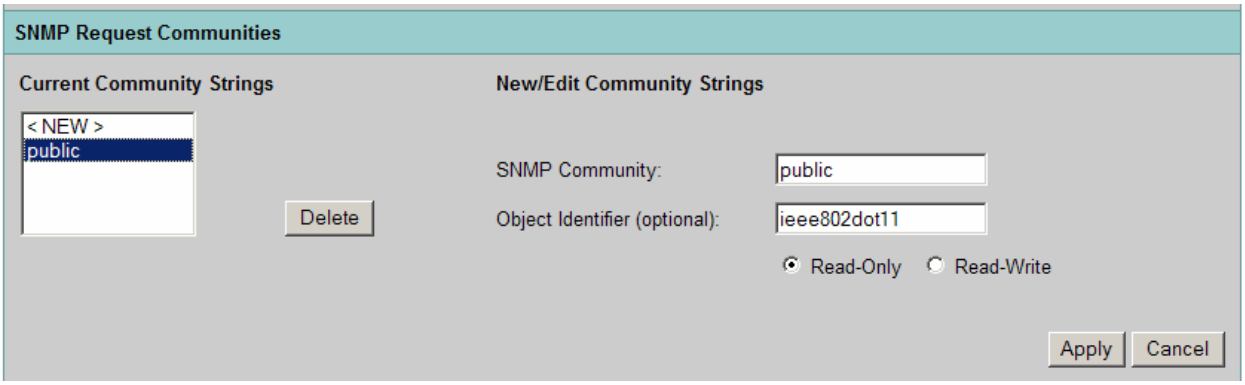
f. Set a System Contact (this is optional, but useful)

g. Complete the following information for your AP in the table below:

System Name	
System Location	
System Contact	

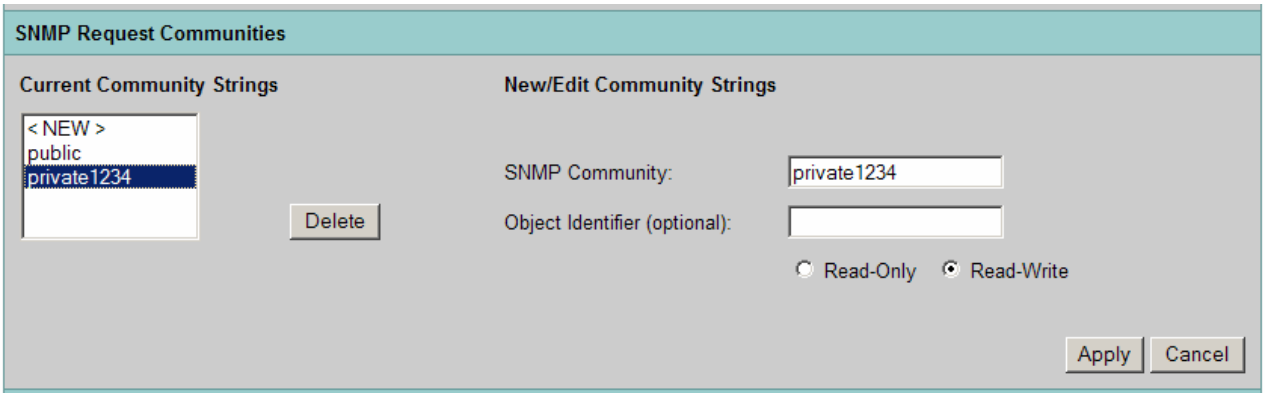
h. Click on the **Apply** buttion.

Step 4 Public community string



Create a public community string with Read Only. In a production environment, it is important to configure a unique string for increase security. SNMP read only provides monitoring through an SNMP management application.

Step 5 Private community string



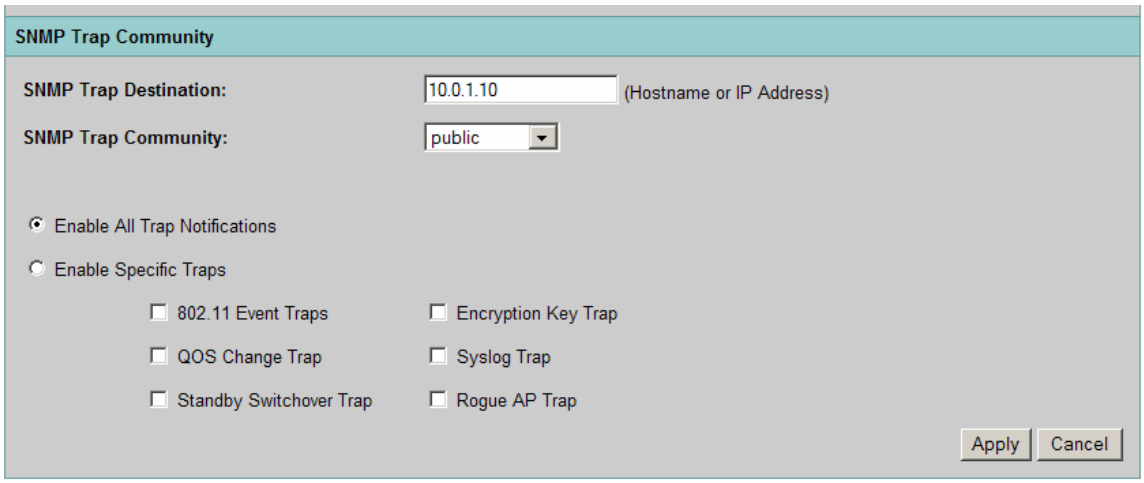
SNMP read-write access monitoring and management using SNMP management applications.

a. Click on the <NEW> in the Current Community String

b. Create a private1234 community string with Read_Write

c. Click the **Apply** button to create the string.

Step 6 SNMP trap destinations



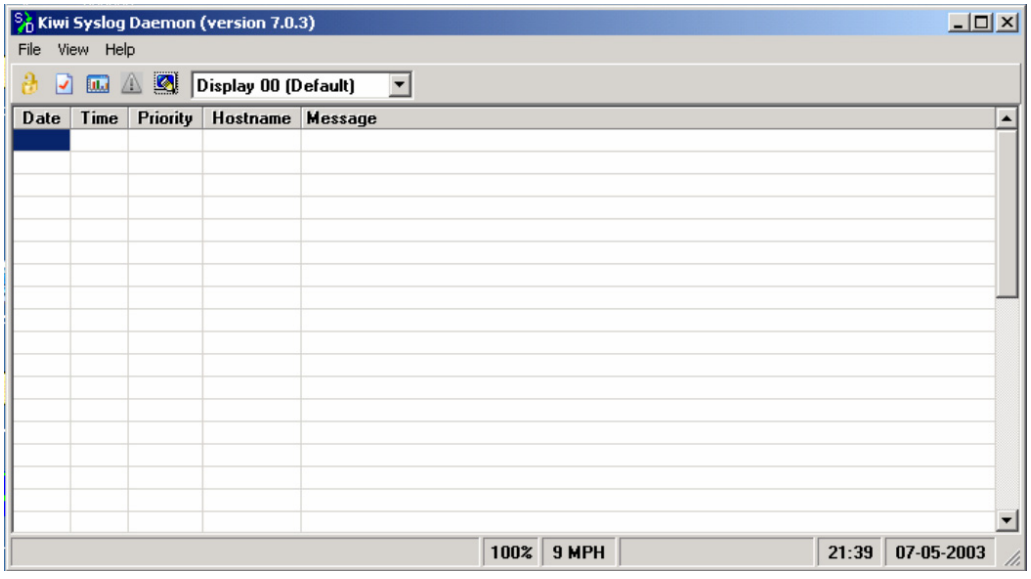
a. Set a SNMP Trap Destination by entering the IP address of PC1 located at 10.0.P.10.

b. Set the SNMP Trap Community to public.

c. Enable All Trap Notifications.

d. Click the **Apply** button.

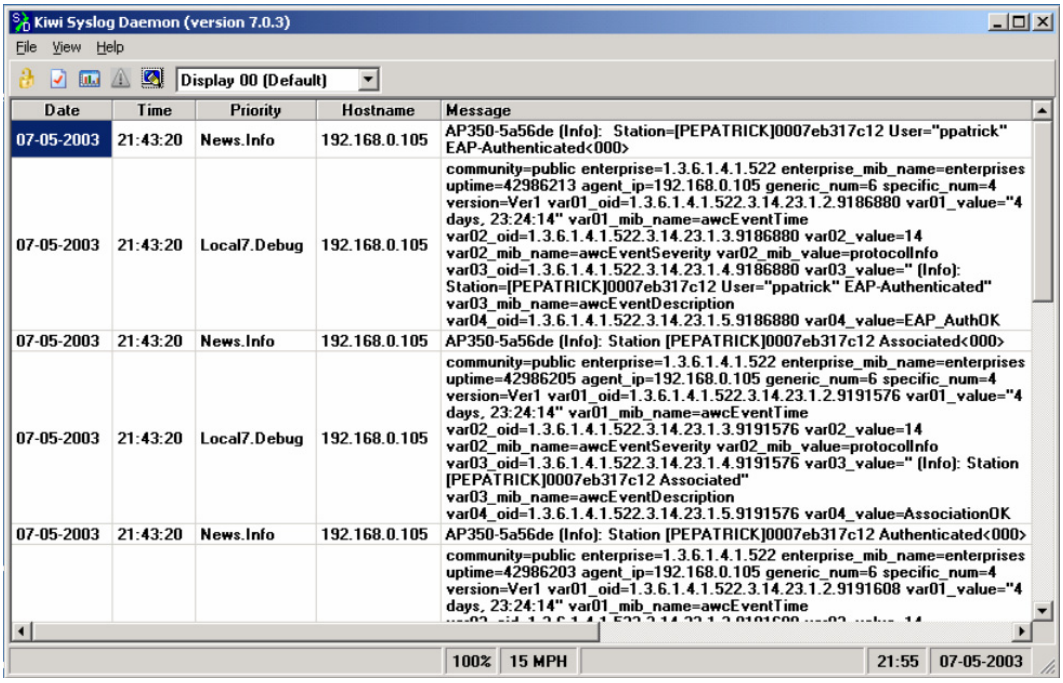
Step 7 Test the configuration



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.

b. Have a wireless user connect to the bridge.

c. Have the wireless user disconnect from the bridge.



d. View the main logging screen on Kiwi.

Step 8 Set the system contact, and location of the SNMP agent through IOS CLI

Before beginning this step, reset the AP back to factory configuration. Configure the AP according to the Topology and Preparation table.

a. Now configure the system contact and location:

```
PodP(config)#snmp-server contact [name] [phone]
PodP(config)#snmp-server location [location]
```

b. What command would be used to verify this information on an AP?

_____

Step 9 Enable SNMP traps

a. Enable all the SNMP trap types at once,

```
PodP(config)#snmp-server enable traps snmp
```

b. Specify to the SNMP destination host the trap notifications will be sent to.

```
PodP(config)#snmp-server host 10.0.P.10 private udp-port 162
```

c. If the default for an SNMP response is on port 162, what port is the request sent on?

_____

Step 10 Test the configuration

a. Exit out of the AP and log back in using the wrong password. After the failed attempts log back into the AP. There will now be entries of traps sent from the AP to the SNMP server. Check the SNMP application on PC1.

Besides **`startup-config`** and **`running-config`**, where would information on the contact, location, and SNMP logging information for SNMP on the router be?

_____

Step 11 Disable the SNMP traps on the AP by using the following commands

```
PodP(config)#no snmp-server enable traps
PodP(config)#no snmp-server system-shutdown
PodP(config)#no snmp-server trap-auth
```

Note	By disabling SNMP trap notifications, which are not needed, the amount of free bandwidth can be increased and unnecessary SNMP processing tasks can be eliminated.

