Lab 11.5.6.1 Configure Syslog on AP

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.

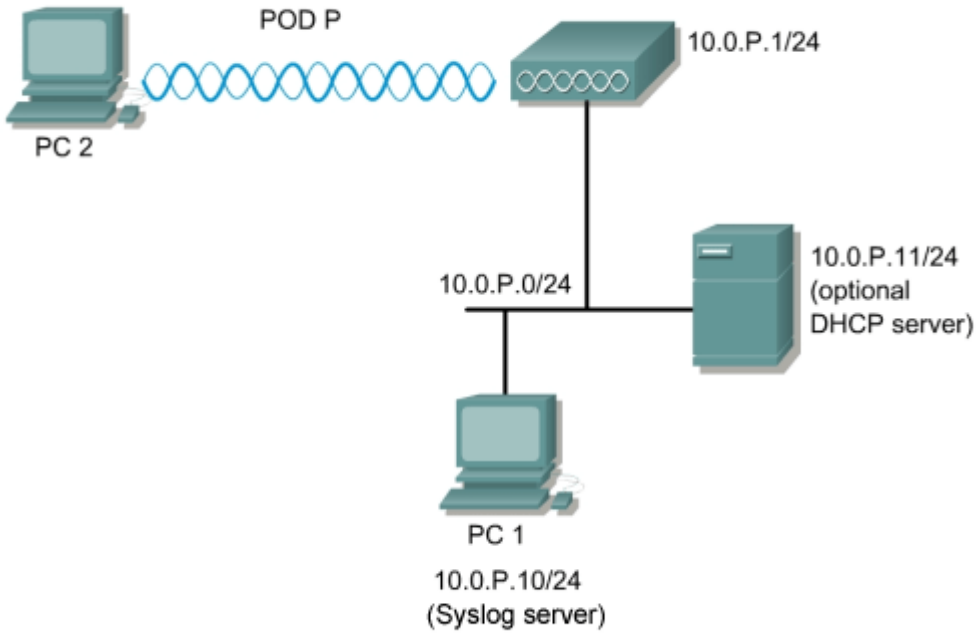
Scenario

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

A Syslog Server is a basic application that allows Aironet AP and bridge event information to be viewed from a Windows system. It includes all the following features:

- Receiving syslog messages through either TCP or UDP
- Full reliability because messages can be sent through TCP
- Ability to receive syslog messages from devices

Topology



Preparation

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

There are numerous syslog servers available on the Internet. This lab assumes that Kiwi Syslog Daemon is used. This is a freeware utility that can be downloaded at http://www.kiwisyslog.com. Download the syslog server and install the executable file.

Tools and resources

The following tools and resources will be helpful with this lab:

- A properly setup wired LAN
- A properly setup and installed AP
- A PC acting as the syslog server with a static IP address
- A PC with a properly installed wireless client adapter and utility

Additional materials

Further information about the objectives covered in this lab can be found at the following website: http://www.kiwisyslog.com

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.

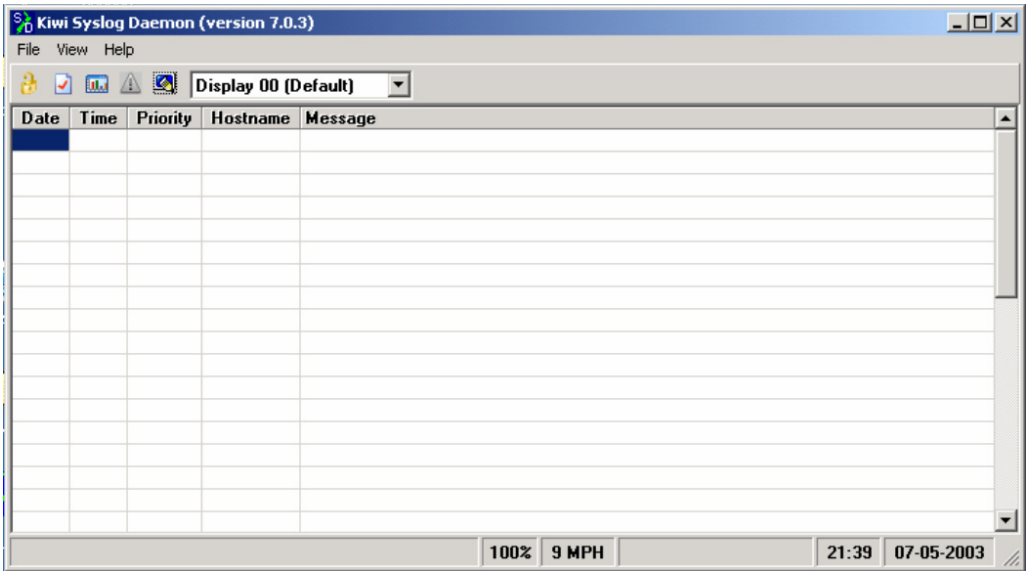
Command	Description
configure terminal	Enter global configuration mode
logging on	Enables Message Logging
logging host	Log Messages to a syslog server host
show logging	Verify the log settings and entries entries.
show running-config	Verify the active configuration in DRAM.
copy running-config startup-config	Save the active configuration into Flash
service timestamps log uptime	Enable log timestamps.
service sequence-numbers	Enable sequence numbers.

Step 1 Download and install the Kiwi Syslog software

a. Go to the http://www.kiwisyslog.com/software_downloads.htm site and download the free edition of the kiwi syslog software.

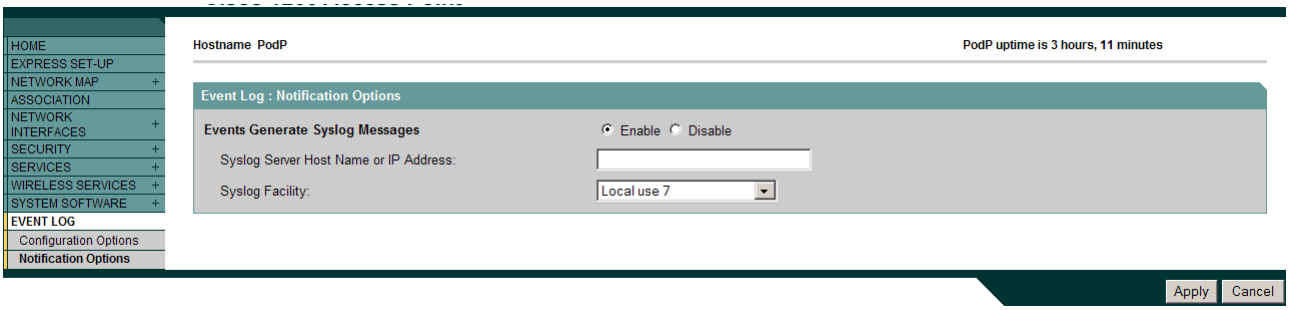
b. Install the executable file.

Step 2 Setup the Kiwi Syslog Daemon



a. Click on the **Kiwi Syslog Daemon** Icon on the desktop to bring up the syslog screen.

Step 3 Enable logging on the AP



a. Open up the AP browser menu and go to the **EVENT LOG>Notification Options** Page.

b. Enable the **Event Generate Syslog Messages** utility on the AP

c. Type in the Syslog Server Host IP address. This should be 10.0.P.10

d. Set the Syslog Facility logging level. The default, Local7, can be used.

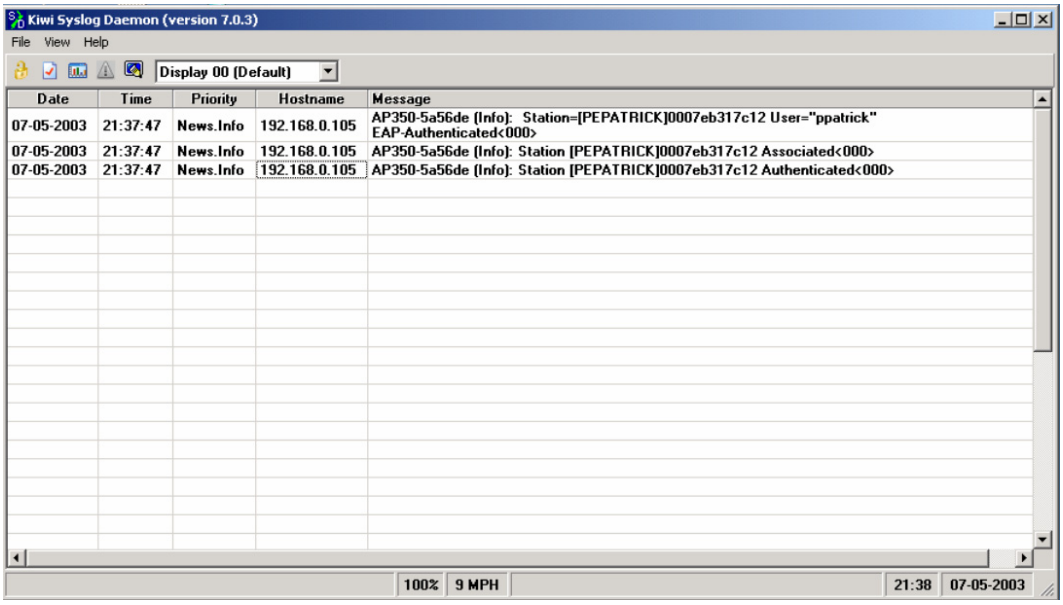
e. What other selections are available?

_____

_____

f. Click the apply button to begin logging events to the Kiwi Syslog.

Step 4 View the Kiwi Syslog event log



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

b. Have the wireless users log onto the AP.

c. Have the wireless users log off the AP.

d. These changes will trigger a logged event on the syslog. What is the message that was displayed on the syslog?

_____

_____

Step 5 Enabling logging on the AP

a. Erase the configuration and reload the AP.

b. Configure the AP according to the Topology.

c. Enabled on an AP using the Cisco IOS with the following commands:

```
PodP(config)#logging on
```

d. To send the logging messages to a syslog server which is located on PC1, use the following command:

```
PodP(config)#logging host 10.0.P.10 (where P is the Pod number)
```

e. View the available messaging levels for syslog :

```
PodP(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>
```

f. Configure the syslog message level to debugging.

```
PodP(config)#logging trap debugging  (or 7)
```

g. Enable the service timestamps on the AP using the following command:

```
PodP(config)#service timestamps log uptime
```

h. Enable the service sequence numbers on the AP logging using the following command:

```
PodP(config)#service sequence-numbers
```

Step 6 Verify the configuration

a. Verify the configuration on the AP.

```
PodP#show running-config
Building configuration...

Current configuration : 2552 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log uptime
service password-encryption
service sequence-numbers
!
hostname PodP
!
logging trap debugging
logging 10.0.1.10
!
[output omitted]
```


b. Use the show logging command to view the entries.

```
PodP#show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns)
    Console logging: level debugging, 312 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 314 messages logged
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 316 message lines logged
Log Buffer (4096 bytes):
*Mar  4 04:44:28.924: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticatin
 Station 0007.8592.e4ea Reason: Previous authentication no longer valid
*Mar  4 04:47:55.076: %DOT11-6-ASSOC: Interface Dot11Radio0, Station csawyer 00
9.b74c.b479 Associated KEY_MGMT[NONE]
*Mar  4 04:51:36.967: %DOT11-4-MAXRETRIES: Packet to client 0009.b74c.b479 reac
ed max retries, remove the client
*Mar  4 04:51:36.968: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticatin
 Station 0009.b74c.b479 Reason: Previous authentication no longer valid
*Mar  4 05:36:44.416: %DOT11-6-ASSOC: Interface Dot11Radio0, Station KDEVIAEN-W
K02 00d0.59c8.ca3f Reassociated KEY_MGMT[NONE]
 --More--
[output omitted]
```

c. To clear the log, use the following command:

```
PodP#clear logging
Clear logging buffer [confirm]
PodP#
```

d. Issue the show log command again to view the clear log:

```
PodP#show log
    Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes,
     0 overruns)
        Console logging: level debugging, 312 messages logged
        Monitor logging: level debugging, 0 messages logged
        Buffer logging: level debugging, 314 messages logged
        Logging Exception size (4096 bytes)
        Count and timestamp logging messages: disabled
        Trap logging: level informational, 316 message lines logged

    Log Buffer (4096 bytes):
    PodP#
```


Step 7 View the Kiwi Syslog event log

a. Generate events to the syslog by establishing a wireless connection to the AP. Next, use Telnet or SSH to log into the AP.

b. The login will trigger logged events on the syslog server located on PC1.

c. What is the message that was displayed on the syslog?

_____

_____

