Configuring Syslog Server On Cisco Routers

Syslog

Syslog is a standard for forwarding log messages in an Internet Protocol (IP) computer network. ***It allows separation of the software that generates log messages from the system that stores the messages.***

Syslog is a ***client/server protocol****: a logging application transmits a maximum 1024-byte text message to the syslog receiver. The receiver is commonly called syslogd, syslog daemon or syslog server.* ***Syslog messages may be sent via the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP). The data is sent in cleartext****; although not part of the syslog protocol itself, an SSL wrapper may be used to provide for a layer of encryption through SSL/TLS.* ***Syslog uses the port number 514****.*

Syslog is typically used for computer system management and security auditing*. While it has a number of shortcomings, syslog is supported by a wide variety of devices and receivers across multiple platforms. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository.*

Syslog is now standardized within the Syslog working group of the IETF.

Text is from Wikipedia, emphasis is mine.

Logging On Cisco Routers

System logging messages (also known as system error messages) are controlled by the logging process, which distributes system logging messages to the various destinations:

logging buffered - send syslog messages to internal memory buffers.
Varies by platform. For most platforms, logging to the buffer is disabled by default.

logging console - send syslog messages to all available TTY lines.
The logging monitor function is disabled.

logging monitor - send syslog messages to all available terminal lines.
The default varies by platform. In general, the default is to log all messages.

logging host - send syslog messages to a remote host.
System logging messages are not sent to any remote host.

Logging On Cisco Routers

logging host
To log system messages and debug output to a remote host, use the **logging host** command in global configuration mode. To remove a specified logging host from the configuration, use the **no** form of this command.

logging host {{*ip-address* | *hostname*} [**vrf** *vrf-name*] | **ipv6** {*ipv6-address* | *hostname*}} [**discriminator** *discr-name* | [[**filtered** [**stream** *stream-id*] | **xml**]] [**transport** {[**beep** [**audit**] [**channel** *chnl-number*] [**sasl** *profile-name*] [**tls cipher** [*cipher-num*] **trustpoint** *trustpt-name*]]] | **tcp** [**audit**] | **udp**} [**port** *port-num*]] [**sequence-num-session**] [**session-id** {**hostname** | **ipv4** | **ipv6** | **string** *custom-string*}]

no logging host {{*ip-address* | *hostname*} | **ipv6** {*ipv6-address* | *hostname*}}

Don’t let the buttload of options scare you. All you really need to configure is the IP address/hostname of your syslog server:

```
r1(config)#logging host 10.100.1.100
r1(config)#
```

‘logging’ or ‘logging host’

You can use either, ‘logging host’ gives you additional options (platform/IOS based):

```
r1(config)#logging host 10.100.1.100
r1(config)#do sh run | i logging
logging 10.100.1.100

r1(config)#logging 10.100.1.100
r1(config)#do sh run | i logging
logging 10.100.1.100

r1(config)#logging 10.100.1.100 ?
  <cr>

r1(config)#logging host 10.100.1.100 ?
  xml  Enable logging in XML
  <cr>
```

Configuring Syslog Server On A Cisco Router

```
r1(config)#logging host 10.100.1.100
```

That’s it. Seriously.

Of course, you’ll probably want/need to tweek a few things depending on your environment.

Common Syslog Options - Facility

logging facility - To configure the syslog facility in which error messages are sent, use the logging facility command in global configuration mode. To revert to the **default of local7**, use the no form of this command.

Each Syslog message includes a priority value at the beginning of the text. The priority value ranges from 0 to 191 and is made up of a Facility value and a Level value.

The Facility value is a way of determining which process of the machine created the message. Since the Syslog protocol was originally written on BSD Unix, the Facilities reflect the names of Unix processes and Daemons.
The priority value is calculated using the following formula:
Priority = Facility * 8 + Level

If you are receiving messages from a Unix system, it is suggested you use the 'User' Facility as your first choice. **Local0 through to Local7 are not used by Unix and are traditionally used by networking equipment. Cisco routers for example use Local6 or Local7.**

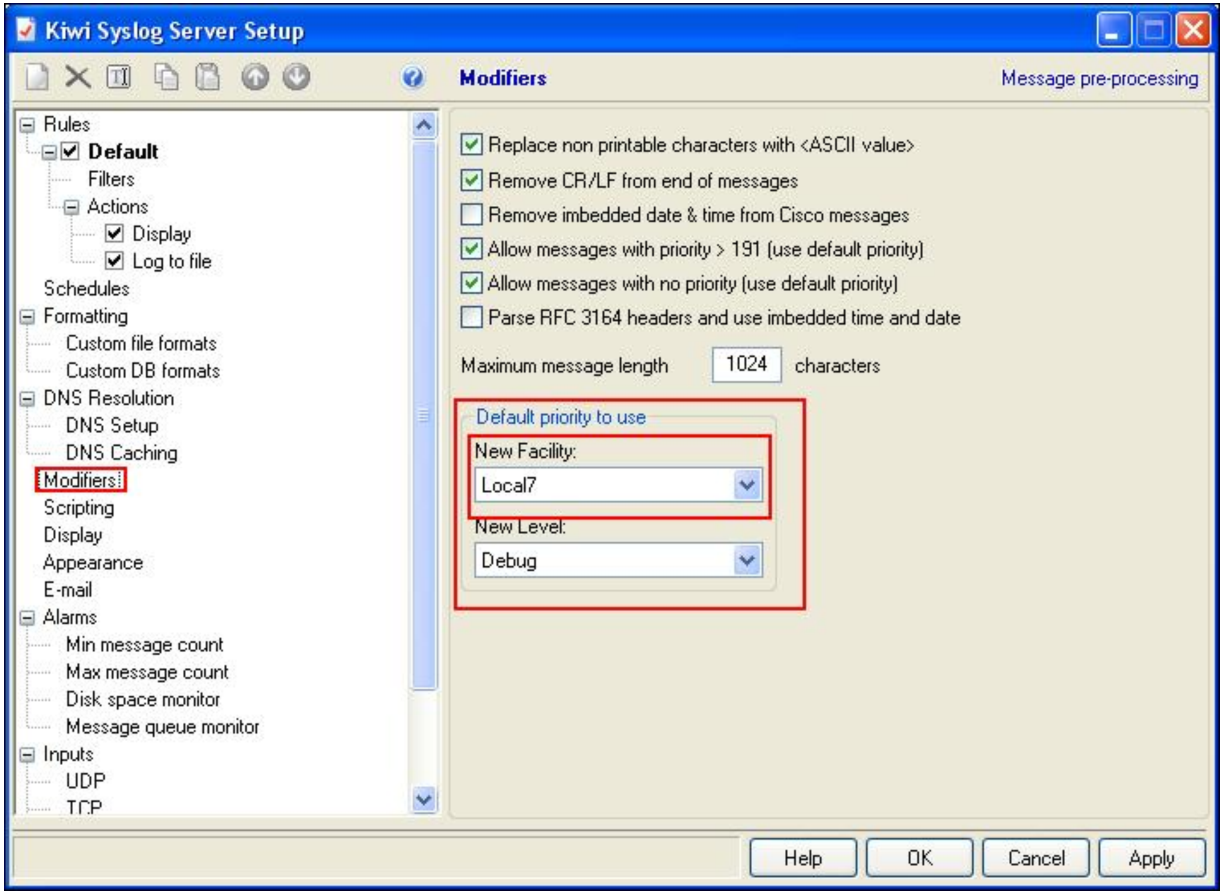
Common Syslog Options - Facility

You will want to check with your syslog administrator to verify which syslog facility you should use. Depending on the syslog server, a syslog facility mismatch may mean that syslog messages will not be accepted on the syslog server. More likely, the syslog messages will be miscategorized on the syslog server.

```
r1(config)#logging facility ?
  auth     Authorization system
  cron     Cron/at facility
  daemon   System daemons
  kern     Kernel
  local0   Local use
  local1   Local use
  local2   Local use
  local3   Local use
  local4   Local use
  local5   Local use
  local6   Local use
  local7   Local use
<-- Output Truncated -->
```

Packet Lab

Common Syslog Options - Facility



Modifiers

Message pre-processing

☑ Replace non printable characters with <ASCII value>

☑ Remove CR/LF from end of messages

□ Remove imbedded date & time from Cisco messages

☑ Allow messages with priority > 191 (use default priority)

☑ Allow messages with no priority (use default priority)

□ Parse RFC 3164 headers and use imbedded time and date

Maximum message length 1024 characters

Default priority to use

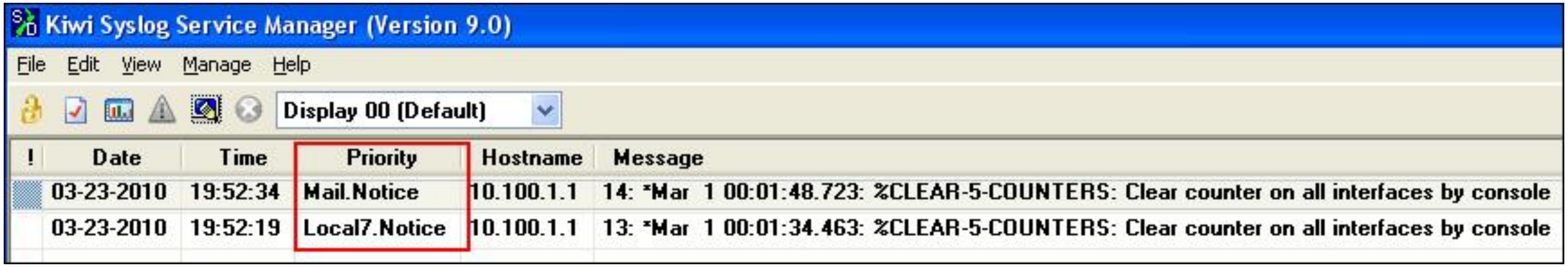
New Facility: Local7

New Level: Debug

Packet Lab

Common Syslog Options - Facility

```
r1(config)#logging facility mail
```


Kiwi Syslog Service Manager (Version 9.0)
File Edit View Manage Help
Display 00 (Default)

!	Date	Time	Priority	Hostname	Message
▨	03-23-2010	19:52:34	Mail.Notice	10.100.1.1	14: *Mar 1 00:01:48.723: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
	03-23-2010	19:52:19	Local7.Notice	10.100.1.1	13: *Mar 1 00:01:34.463: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console

Common Syslog Options – Trap Level

logging trap - To limit messages logged to the syslog servers based on severity, use the **logging trap** command in global configuration mode. To return the logging to remote hosts to the default level, use the **no** form of this command.

logging trap *level*

Default - Syslog messages at level 0 to level 6 are generated, but will only be sent to a remote host if the **logging host** command is configured.

This command determines which of the 8 levels of syslog messages (see next slide) is sent to the syslog server. By default, levels 0 to 6 (informational) are sent to the syslog server. When you configure this command, the router will send all syslog messages for the level you specify as well as all levels below it. For example 'logging trap 4' will send syslog messages at level 0 to 4.

```
r1#show logging | b Trap
   Trap logging: level informational, 25 message lines logged
      Logging to 10.100.1.100, 8 message lines logged, xml disabled
```

Syslog Trap Levels

Level	Level Keyword	Syslog Definition
0	emergencies	LOG_EMERG
1	alerts	LOG_ALERT
2	critical	LOG_CRIT
3	errors	LOG_ERR
4	warnings	LOG_WARNING
5	notifications	LOG_NOTICE
6	informational	LOG_INFO
7	debugging	LOG_DEBUG

The default logging level varies by platform but is generally 7.

Packet Lab

Common Syslog Options – Trap Level

```
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>
```

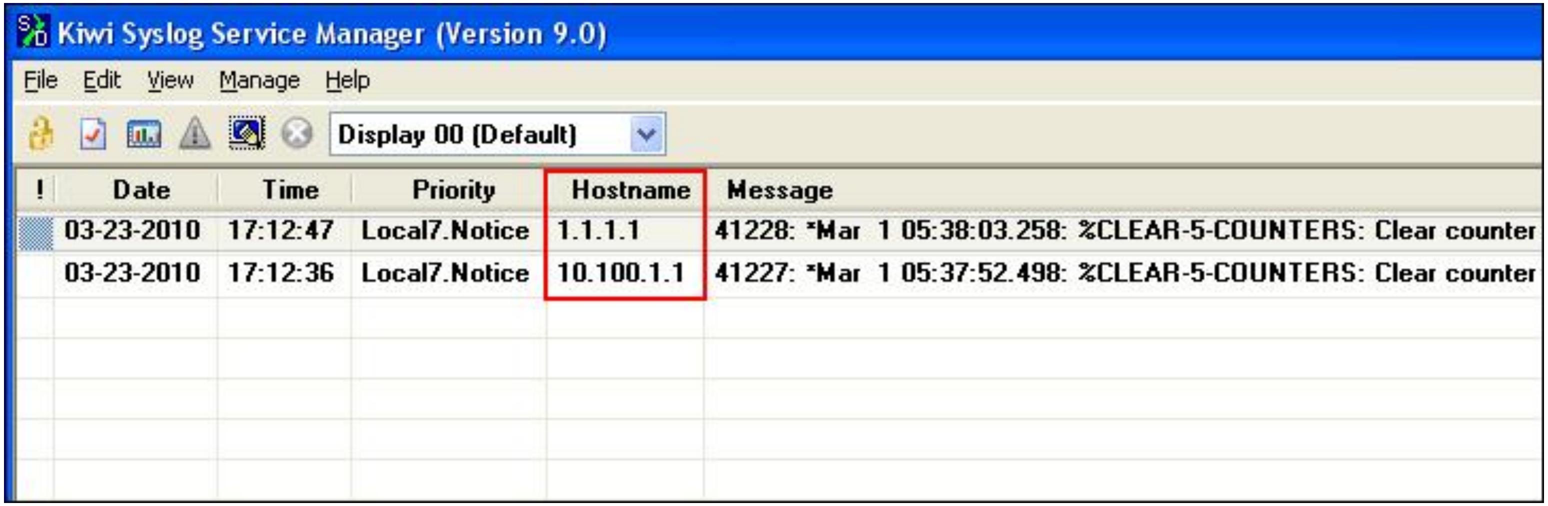
For those of you pursuing Cisco certification, you’ll want to commit these severity levels and names/labels to memory.

Common Syslog Options – Source-Interface

logging source-interface - To specify the source IP or IPv6 address of system logging packets, use the **logging source-interface** command in global configuration mode.

Normally, a syslog message contains the IP or IPv6 address of the interface it uses to leave the router. The **logging source-interface** command specifies that syslog packets contain the IP or IPv6 address of a particular interface, regardless of which interface the packet uses to exit the router.

```
r1(config)#logging source-interface loopback 0
```



!	Date	Time	Priority	Hostname	Message
▨	03-23-2010	17:12:47	Local7.Notice	1.1.1.1	41228: *Mar 1 05:38:03.258: %CLEAR-5-COUNTERS: Clear counter
	03-23-2010	17:12:36	Local7.Notice	10.100.1.1	41227: *Mar 1 05:37:52.498: %CLEAR-5-COUNTERS: Clear counter

Common Syslog Options – Origin-ID

logging origin-id - To add an origin identifier to system logging messages sent to remote hosts, use the **logging origin-id** command in global configuration mode. To disable the origin identifier, use the **no** form of this command.

The origin identifier is added to the beginning of all system logging (syslog) messages sent to remote hosts. The identifier can be the hostname, the IP address, the IPv6 address, or any text that you specify. The origin identifier is not added to messages sent to local destinations (the console, monitor, or buffer).

The origin identifier is useful for identifying the source of system logging messages in cases where you send syslog output from multiple devices to a single syslog host.

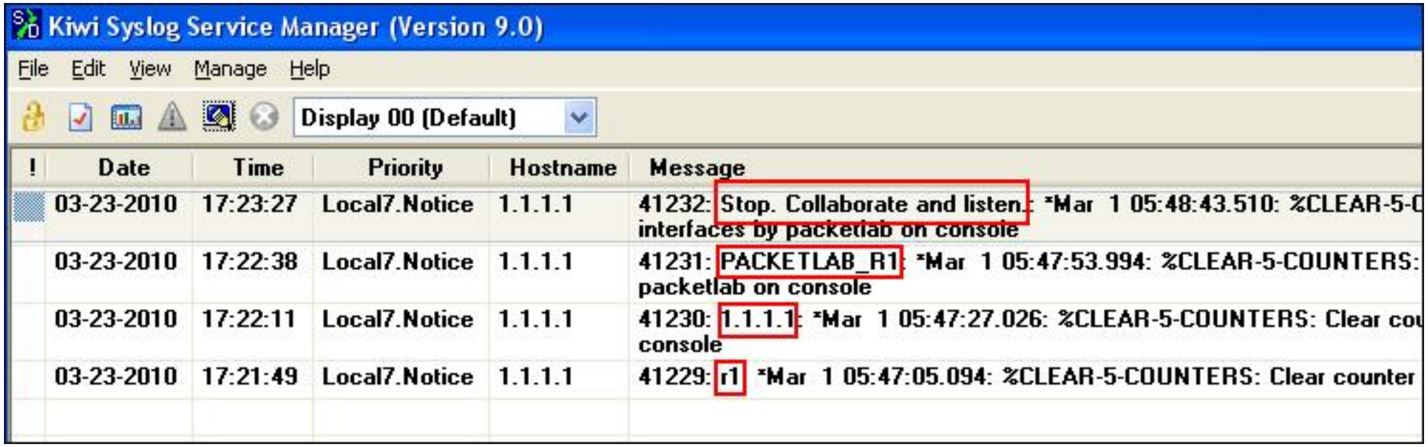
When you specify your own identification string using the **logging origin-id string** *user-defined-id* command, the system expects a string without spaces.

To use spaces (multiple words) or additional syntax, enclose the string with quotation marks (" ").

Common Syslog Options – Origin-ID

```
r1(config)#logging origin-id ?
  hostname  Use origin hostname as ID
  ip        Use origin IP address as ID
  string    Define a unique text string as ID
  <cr>
r1(config)#logging origin-id hostname
```

Syslog server messages with hostname, IP, string (with and without spaces):



!	Date	Time	Priority	Hostname	Message
	03-23-2010	17:23:27	Local7.Notice	1.1.1.1	41232: Stop. Collaborate and listen.: *Mar 1 05:48:43.510: %CLEAR-5-C interfaces by packetlab on console
	03-23-2010	17:22:38	Local7.Notice	1.1.1.1	41231: PACKETLAB_R1: *Mar 1 05:47:53.994: %CLEAR-5-COUNTERS: packetlab on console
	03-23-2010	17:22:11	Local7.Notice	1.1.1.1	41230: 1.1.1.1: *Mar 1 05:47:27.026: %CLEAR-5-COUNTERS: Clear cou console
	03-23-2010	17:21:49	Local7.Notice	1.1.1.1	41229: r1: *Mar 1 05:47:05.094: %CLEAR-5-COUNTERS: Clear counter

Verification

The primary verification command is the ‘show logging’ command.

```
r1#show logging
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0 flushes, 0 overruns, xml disabled)
    Console logging: level debugging, 41567 messages logged, xml disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled
    Buffer logging: level debugging, 41502 messages logged, xml disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 41234 message lines logged
        Logging to 10.100.1.100, 13 message lines logged, xml disabled
Log Buffer (4096 bytes):
*Mar  1 05:37:52.498: %CLEAR-5-COUNTERS: Clear counter on all interfaces by packetlab on console
```

You will most likely get more and clearer information with ‘show run | i logging’

Packet Lab

Benefits of Using Syslog Server

Normally this slide at the beginning of the lesson, but I wanted to touch on some of the features/technologies involved with using a syslog server with Cisco devices before talking about the benefits:

Persistence – Syslog messages stored in a Cisco device's buffer are lost on reload or when cleared. Also, once the buffer is full, it will overwrite itself. Syslog servers allow you to store syslog messages for longer periods of time…even permanently.

Event correlation across devices – Logs are a great way to troubleshoot network events. With a syslog server you can view the logs of multiple devices in a single source.

Time stamps – Syslog servers generally use their own timestamp as well as the timestamp in the syslog messages. This is great for network devices that do not have their time synchronized with the rest of the network.

Searching/Sorting – Syslog servers generally give you much better tools to search/sort syslog messages.

Storage of logs – Much like persistence, but I mean to highlight long-term storage here. This is beneficial, and sometimes mandated.

Summary

While using a syslog server is usually considered a necessity in larger networks, I would argue that even very small networks can benefit greatly from implementing a syslog server. In some industries a syslog server may be mandated as part of a larger security/audit process. Using a remote syslog server rather than just the local logging buffer on Cisco devices gives you a number of advantages such as message persistence, event correlation across devices, and advanced message searching/sorting to name a few examples.

Basic syslog server configuration on a Cisco device is ridiculously easy (‘logging host x.x.x.x’) but there are a number of basic configuration options that you will want to be aware of. This lesson touches on the most often used options.