Syslog

- Logging messages on Cisco devices comply with the Syslog standard
- A Syslog message is generated when something happens on the device, such as an interface going down or an OSPF neighbour adjacency coming up

Syslog Format

- The format of the messages is:
  - seq no:time stamp: %facility-severity-MNEMONIC:description

- Example:

```
*Oct  3 00:44:12.627: %LINK-5-CHANGED: Interface
FastEthernet0/0, changed state to administratively down
```

Syslog Format

- The format of the messages is:
  - seq no (optional)

*

Syslog Format

- The format of the messages is:
  - seq no:time stamp

```
*Oct  3 00:44:12.627
```

Syslog Format

- The format of the messages is:
  - seq no:time stamp: %facility

```
*Oct  3 00:44:12.627: %LINK
```

Syslog Format

- The format of the messages is:
  - seq no:time stamp: %facility-severity

```
*Oct  3 00:44:12.627: %LINK-5
```

Syslog Format

- The format of the messages is:
  - seq no:time stamp: %facility-severity-MNEMONIC

```
*Oct   3 00:44:12.627: %LINK-5-CHANGED
```

Syslog Format

- The format of the messages is:
  - seq no:time stamp: %facility-severity-MNEMONIC:description

```
*Oct  3 00:44:12.627: %LINK-5-CHANGED: Interface
FastEthernet0/0, changed state to administratively down
```

Syslog Severity Levels

Value	Severity	Description
0	Emergency	System is unusable. A panic condition.
1	Alert	A condition that should be corrected immediately, such as a corrupted system database.
2	Critical	Critical conditions, such as hard device errors.
3	Error	Error conditions.
4	Warning	Warning conditions.
5	Notice	Normal but significant conditions. Not errors, but may require special handling.
6	Informational	Informational messages.
7	Debug	Messages that contain information normally of use only when debugging a program.

Logging Locations

- Syslog messages can be logged to various locations:
  - **Console line** - events will be shown in the CLI when you are logged in over a console connection. All events logged by default
  - **VTY Terminal lines** - events will be shown in the CLI when you are logged in over a Telnet or SSH session. Not enabled by default
  - **The logging buffer** – events saved in RAM memory, you can view them with the 'show logging' command. All events logged by default
  - **External Syslog servers**

Logging Locations

- You can specify the same or different severity levels to log for each location
- All messages of that severity level and higher will be logged
- For example, if you set a logging level of 3 for the console, events with severity levels 0, 1, 2 and 3 will be logged there
- If you set a logging level of 7 for an external Syslog server, events from all severity levels 0–7 will be logged there

Internal Logging Locations Configuration

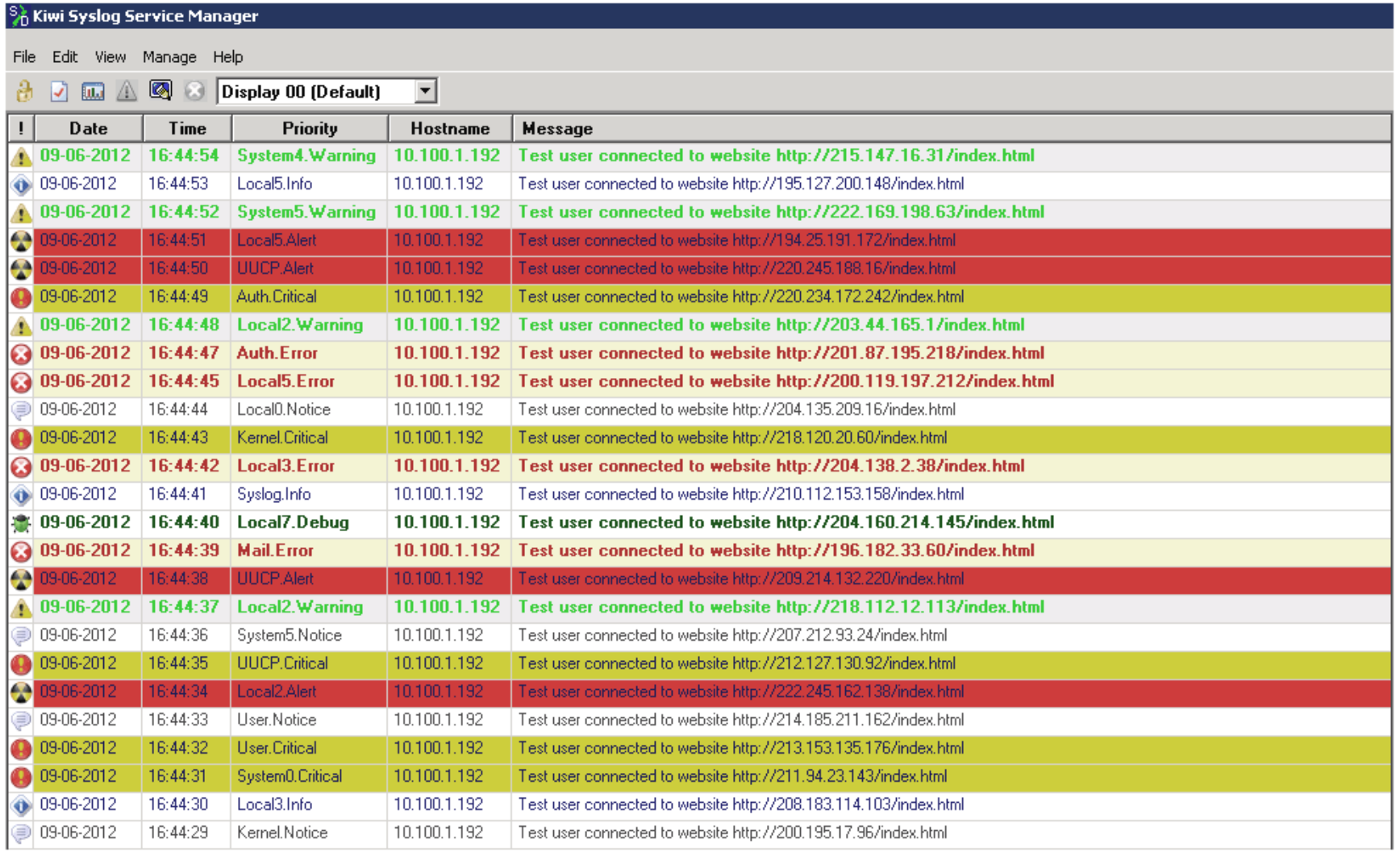
- `R1(config)#no logging console` (disables logging to the console line)
- `R1(config)#logging monitor 6` (events with severity level informational and higher will be logged to the VTY lines)
- `R1(config)#logging buffered debugging` (events with severity level 7 and higher will be logged to the buffer)

Logging to an External Syslog Server

- You can log to an external Syslog server to centralise event reporting
- You will typically set verbose logging to provide detailed troubleshooting information

```
R1(config)#logging 10.0.0.100
R1(config)#logging trap debugging
```

External Syslog Server



!	Date	Time	Priority	Hostname	Message
	09-06-2012	16:44:54	System4.Warning	10.100.1.192	Test user connected to website http://215.147.16.31/index.html
	09-06-2012	16:44:53	Local5.Info	10.100.1.192	Test user connected to website http://195.127.200.148/index.html
	09-06-2012	16:44:52	System5.Warning	10.100.1.192	Test user connected to website http://222.169.198.63/index.html
	09-06-2012	16:44:51	Local5.Alert	10.100.1.192	Test user connected to website http://194.25.191.172/index.html
	09-06-2012	16:44:50	UUCP.Alert	10.100.1.192	Test user connected to website http://220.245.188.16/index.html
	09-06-2012	16:44:49	Auth.Critical	10.100.1.192	Test user connected to website http://220.234.172.242/index.html
	09-06-2012	16:44:48	Local2.Warning	10.100.1.192	Test user connected to website http://203.44.165.1/index.html
	09-06-2012	16:44:47	Auth.Error	10.100.1.192	Test user connected to website http://201.87.195.218/index.html
	09-06-2012	16:44:45	Local5.Error	10.100.1.192	Test user connected to website http://200.119.197.212/index.html
	09-06-2012	16:44:44	Local0.Notice	10.100.1.192	Test user connected to website http://204.135.209.16/index.html
	09-06-2012	16:44:43	Kernel.Critical	10.100.1.192	Test user connected to website http://218.120.20.60/index.html
	09-06-2012	16:44:42	Local3.Error	10.100.1.192	Test user connected to website http://204.138.2.38/index.html
	09-06-2012	16:44:41	Syslog.Info	10.100.1.192	Test user connected to website http://210.112.153.158/index.html
	09-06-2012	16:44:40	Local7.Debug	10.100.1.192	Test user connected to website http://204.160.214.145/index.html
	09-06-2012	16:44:39	Mail.Error	10.100.1.192	Test user connected to website http://196.182.33.60/index.html
	09-06-2012	16:44:38	UUCP.Alert	10.100.1.192	Test user connected to website http://209.214.132.220/index.html
	09-06-2012	16:44:37	Local2.Warning	10.100.1.192	Test user connected to website http://218.112.12.113/index.html
	09-06-2012	16:44:36	System5.Notice	10.100.1.192	Test user connected to website http://207.212.93.24/index.html
	09-06-2012	16:44:35	UUCP.Critical	10.100.1.192	Test user connected to website http://212.127.130.92/index.html
	09-06-2012	16:44:34	Local2.Alert	10.100.1.192	Test user connected to website http://222.245.162.138/index.html
	09-06-2012	16:44:33	User.Notice	10.100.1.192	Test user connected to website http://214.185.211.162/index.html
	09-06-2012	16:44:32	User.Critical	10.100.1.192	Test user connected to website http://213.153.135.176/index.html
	09-06-2012	16:44:31	System0.Critical	10.100.1.192	Test user connected to website http://211.94.23.143/index.html
	09-06-2012	16:44:30	Local3.Info	10.100.1.192	Test user connected to website http://208.183.114.103/index.html
	09-06-2012	16:44:29	Kernel.Notice	10.100.1.192	Test user connected to website http://200.195.17.96/index.html

FLACKBOX
www.flackbox.com

SIEM Security Information and Event Management

- A basic Syslog server provides a centralised location for Syslog logging messages.
- A Security Information and Event Management (SIEM) system provides a centralised location for all logging messages and will typically provide advanced analysis and correlation of events.

View Log Buffer and Configuration

```
R1#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes, 0 overruns,
xml disabled, filtering disabled)

    Console logging: level error, 42 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level warning, 38 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 87 messages logged, xml disabled,
                    filtering disabled

    Trap logging: level debugging, 27 message lines logged
        Logging to 10.0.0.100  (udp port 514, audit disabled,
              link up),

Log Buffer (8192 bytes):

*Nov 12 21:17:08.015: %IFMGR-7-NO_IFINDEX_FILE: Unable to open nvram:/ifIndex-table No such
file or directory
*Nov 12 21:17:08.299: %DEC21140-1-INITFAIL: Unsupported PHY brand timed out, csr5=0x0
*Nov 12 21:17:14.075: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Nov 12 21:17:14.115: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
```

Logging Synchronous

- When working in a CLI session, by default any syslog messages will be printed into the middle of any commands you are currently typing

```
R1(config)#interface f3/0
R1(config-if)#shutdown
R1(config-if)#do show ip interf
*Nov 12 20:27:00.727: %LINK-5-CHANGED: Interface
FastEthernet3/0, changed state to administratively downace br
```

Logging Synchronous

- You can override this with the `logging synchronous` command
- This causes a new line to be printed where you were in the command

```
R1(config)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#interface f3/0
R1(config-if)#no shutdown
R1(config-if)#do show ip interf
*Nov 12 20:29:48.787: %LINK-3-UPDOWN:
Interface FastEthernet3/0, changed state to up
R1(config-if)#do show ip interf
```

Debug and Terminal Monitor

- Show and Debug commands can be used to view specific information over and above the standard Syslog messages
- Show output shows a static point in time state
- Debug output dynamically updates in real time
- Be careful with debug commands in production environments, a large amount of output can overwhelm the device
- Debug output is logged to the console line and buffer by default
- Use the `R1#terminal monitor` command to enable debug output to the VTY lines