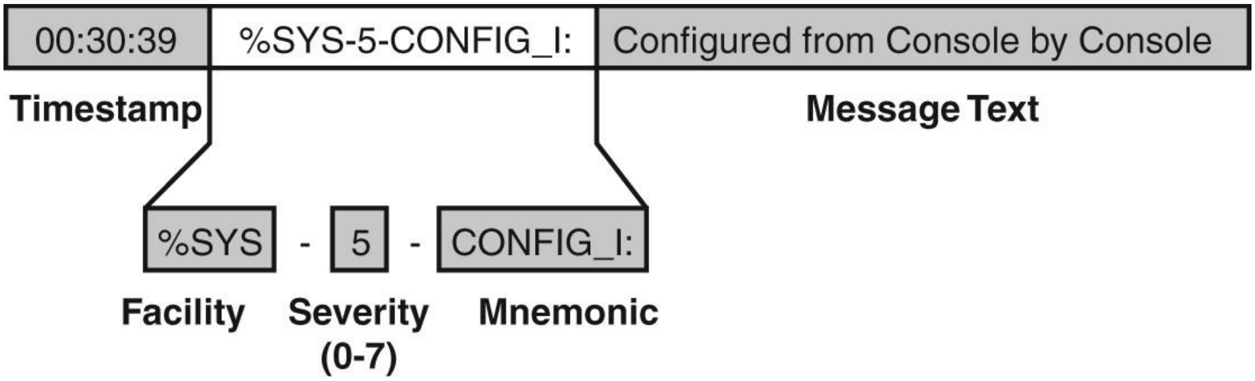
Syslog:

- Syslog stands for System Logging, standard protocol used to send system log.
- Cisco network devices Routers and Switches use Syslog to send system messages.
- Cisco network devices use debug output to a local logging process inside the device.
- Syslog is used on a variety of devices to give system information to the system admin.
- Most Cisco devices use the syslog protocol to manage system logs and system alerts.
- Logging can be used for fault notification, network forensics, and security auditing.
- Syslog messages can be output to the console, local buffer or a remote syslog serve.
- Logs can include content flow, configuration changes and new software installs etc.
- Logging helps to detect unusual network traffic, network device failures, issue etc.

Syslog Severity Level		
Level Name	**Level**	**Router Messages**
Emergency	0	System-Unusable Messages (Missing Fan Tray)
Alert	1	Take Immediate Action (Temperature Limit Exceeded)
Critical	2	Critical Condition (Memory Allocation Failures)
Error	3	Error Message (Interface Up/Down)
Warning	4	Warning Message (File Written to Server)
Notice	5	Normal but Significant Condition (Line Protocol Up/Down)
Informational	6	Information Message (Access-List Violation)
Debug	7	Debug Messages and Log FTP Commands



TIMESTAMP	This is the time and date message generated.
FACILITY-SUBFACILITY	Reports protocol, module or process that generated the message.
SEVERITY	This is level from 0-7 specifies how important the message is.
MNEMONIC	A code that identifies the action reported.
MESSAGE TEXT	A plain text description of the event.

Local Logging:

- Everything happens on router or switch can be logged.
- By default, syslog messages are only displayed to the console.
- Because the **logging console** command is enabled by default.
- By default, the router sends all log messages to its console port.
- Only users physically connected to the router console port can view messages.
- This can be turned off with the **no logging** command.
- For local logging, Cisco IOS can save syslog messages to the internal buffer.
- Syslog messages can be output to the console or a remote syslog server.
- The logging is basically the process that generated the syslog message.

Terminal Logging:

- It is like console logging, but it displays log messages to the router's VTY lines instead.
- This is not enabled by default. To enable it to use this command: `R1# terminal monitor`

Buffered Logging:

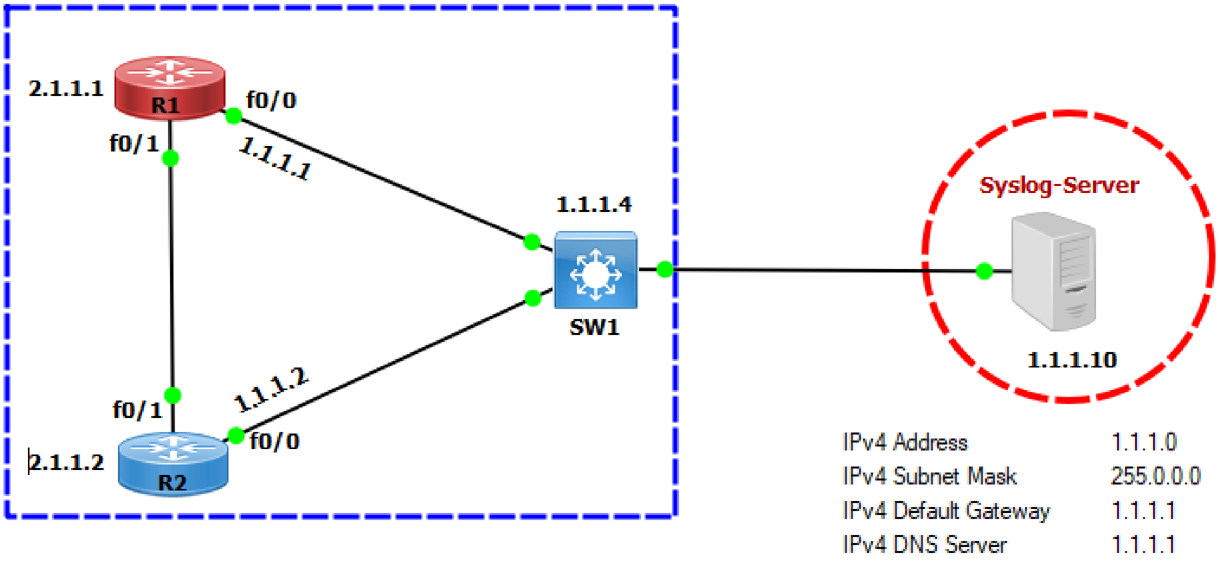
- This type of logging uses Cisco Router's & Switches RAM for storing log messages.
- Buffer has fixed size to ensure that the log will not deplete valuable system memory.
- Router accomplishes this by deleting old messages as new messages are added.
- To enable it use configuration mode command: `R1 (config)# logging buffered`

Syslog Server Logging:

- Router can use syslog to forward log messages to external syslog servers for storage.
- Syslog Server Logging method of type of logging is not enabled by default in devices.

SNMP Trap Logging:

- The router can use SNMP traps to send log messages to an external SNMP server.

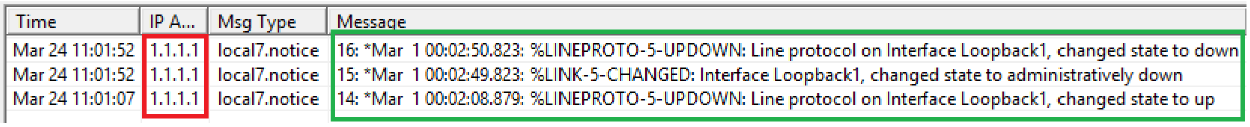


IPv4 Address	1.1.1.0
IPv4 Subnet Mask	255.0.0.0
IPv4 Default Gateway	1.1.1.1
IPv4 DNS Server	1.1.1.1

R1 Configuration	
R1(config)#interface f0/0 R1(config-if)#ip address 1.1.1.1 255.0.0.0 R1(config-if)# no shutdown	R1(config)#interface f0/1 R1(config-if)#ip address 2.1.1.1 255.0.0.0 R1(config-if)#no shutdown
R1(config)#router rip R1(config-router)#network 0.0.0.0	R1# show ip int br R1# show ip route
R2 Configuration	
R2(config)#interface f0/0 R2(config-if)#ip address 1.1.1.2 255.0.0.0 R2(config-if)# no shutdown	R2(config)#interface f0/1 R2(config-if)#ip address 2.1.1.2 255.0.0.0 R2(config-if)#no shutdown
R2(config)#router rip R2(config-router)#network 0.0.0.0	R2# show ip int br R2# show ip route
SW1 Configuration	
SW1(config)#interface vlan 1 SW1(config-if)#ip address 1.1.1.4 255.0.0.0 SW1(config-if)# no shutdown	SW1(config)#router rip SW1(config-router)#network 0.0.0.0 SW1# show ip int br

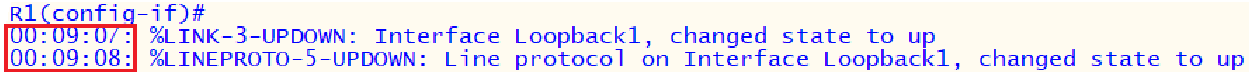
Logging Configuration	
R1 (config)# logging 1.1.1.10	R1(config)# logging buffered informational
R1 (config)# logging host 1.1.1.10	R1(config)# logging buffered 64000
R1 (config)# logging buffered	R1(config)# no service timestamps
R1 (config)# logging trap <1-7> R1 (config)# logging trap notifications R1 (config)# logging traps 5	R1(config)# service sequence-number
R1 (config)# no logging console	R1# terminal monitor
R1 (config)# logging console <Level>	R1# terminal no monitor
R1# clear logging	R1# show logging

External Syslog Server show up R1 logs.



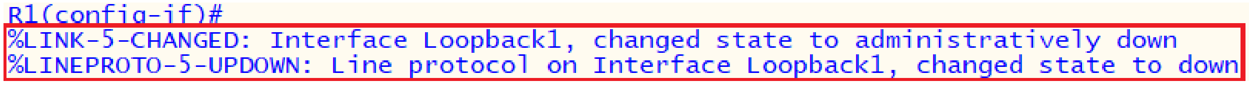
Time	IP A...	Msg Type	Message
Mar 24 11:01:52	1.1.1.1	local7.notice	16: *Mar 1 00:02:50.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to down
Mar 24 11:01:52	1.1.1.1	local7.notice	15: *Mar 1 00:02:49.823: %LINK-5-CHANGED: Interface Loopback1, changed state to administratively down
Mar 24 11:01:07	1.1.1.1	local7.notice	14: *Mar 1 00:02:08.879: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

Logs with Timestamp



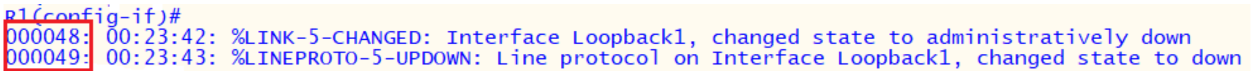
```
R1(config-if)#
00:09:07: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
00:09:08: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
```

Logs without Timestamp.



```
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to down
```

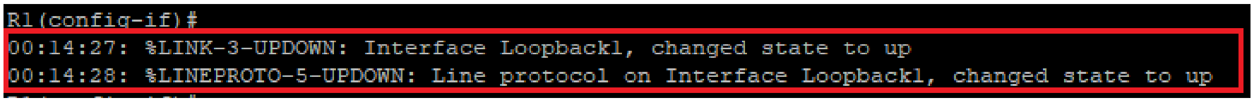
Logs with sequence number after enable service sequence-number.



```
R1(config-if)#
000048: 00:23:42: %LINK-5-CHANGED: Interface Loopback1, changed state to administratively down
000049: 00:23:43: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to down
```

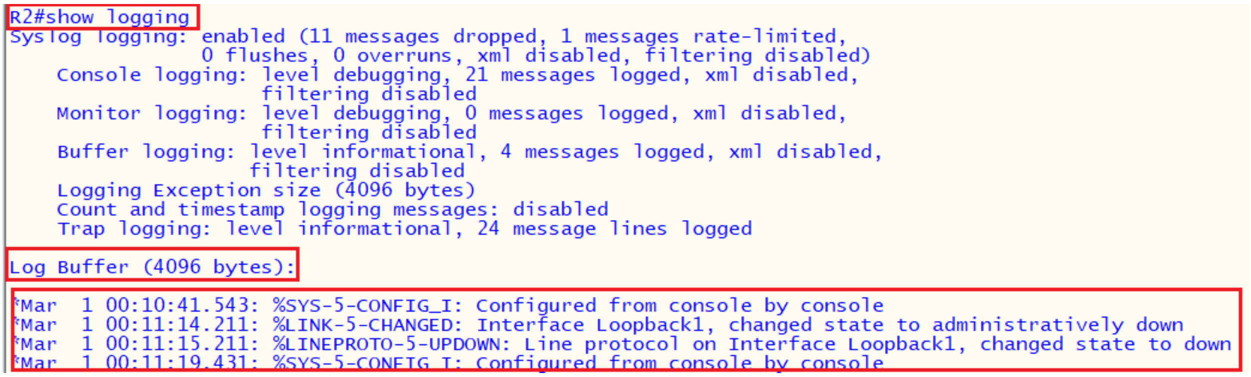
```
R1(config)#line vty 0 4
R1(config-line)#password 123
R1(config-line)#login
R1(config)#enable password 123
R1#terminal monitor
```

After enable, terminal monitor logs show up on remote telnet screen.



```
R1(config-if)#
00:14:27: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
00:14:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
```

By default, syslog messages are only displayed to the console.
Below is local logging in console.



```
R2#show logging
Syslog logging: enabled (11 messages dropped, 1 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 21 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level informational, 4 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 24 message lines logged

Log Buffer (4096 bytes):

*Mar  1 00:10:41.543: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 00:11:14.211: %LINK-5-CHANGED: Interface Loopback1, changed state to administratively down
*Mar  1 00:11:15.211: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to down
*Mar  1 00:11:19.431: %SYS-5-CONFIG_I: Configured from console by console
```