
Networkforyou
Welcome
To
Network for you
Syslog Server
Networkforyou

Syslog:

- Syslog is stand for System Logging Protocol
- Syslog is a standard for message logging and often used on network devices.
- Syslog shown messages and is able to store them on the local device or Syslog Server
- When every anything happening on the router or switch Cisco IOS informs us with the help of syslog.
- By default there syslog message are only outputted to the console not through Telnet or SSH
- We can enable syslog message to Telnet or SSH by typing **terminal monitor** command.
- We can check Syslog messages local history on device by typing show **logging** command. But if device restart then it will lose. As it is store in buffered we can increase sized of buffer by typing **Logging buffered 16384 (size Bytes)** etc.
- We can check with command : **sh logging | include log Buffer**
- Local history is good but it stored in RAM and when it reload it will gone.
- Generally in Production networks we use a **central server called Syslog Server**.
- Syslog is protocol a standard and you can configure routers and switches to forward syslog messages to the syslog server like given command : **logging host (systemlogserverIPaddress)**
- Example: **logging host 192.168.1.1**

Syslog Server:

1. Kiwi Syslog Server Free Edition by solar winds
2. Snmpsoft syslog Watcher
3. Paessler PRTG Syslog
4. Splunk Light
5. The Dude
6. Whatsup Syslog Server Free Tool

And many more…..

Syslog Format:

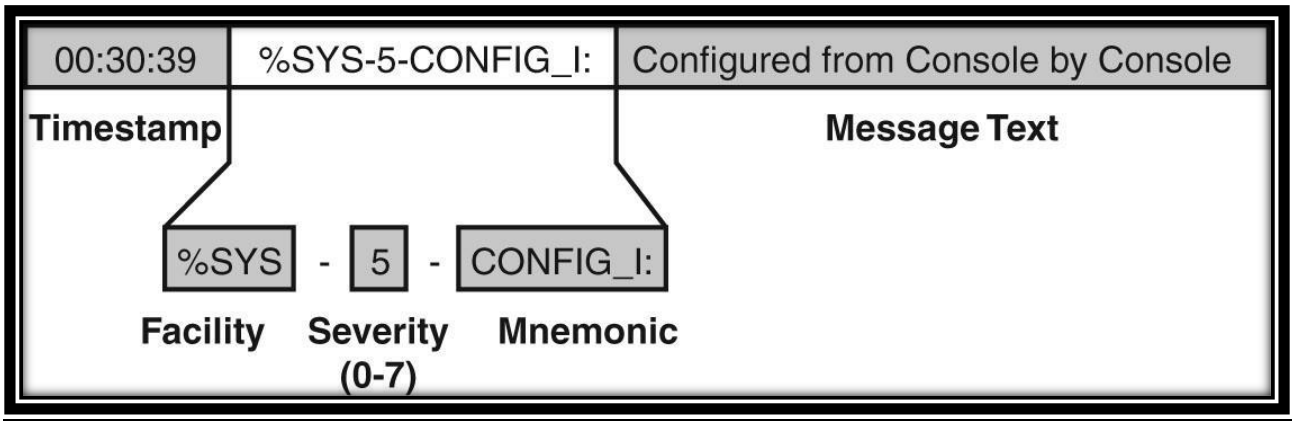
The format of the message is:

Seq no: time stamp: %facility-severity-MNEMONIC:description

*May 25, 21:08:39.088: SYS-5-CONFIG_I: Configured from console by console

*May 25, 21:09:54.099: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down

*May 25, 21:09:54.099: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down.



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.

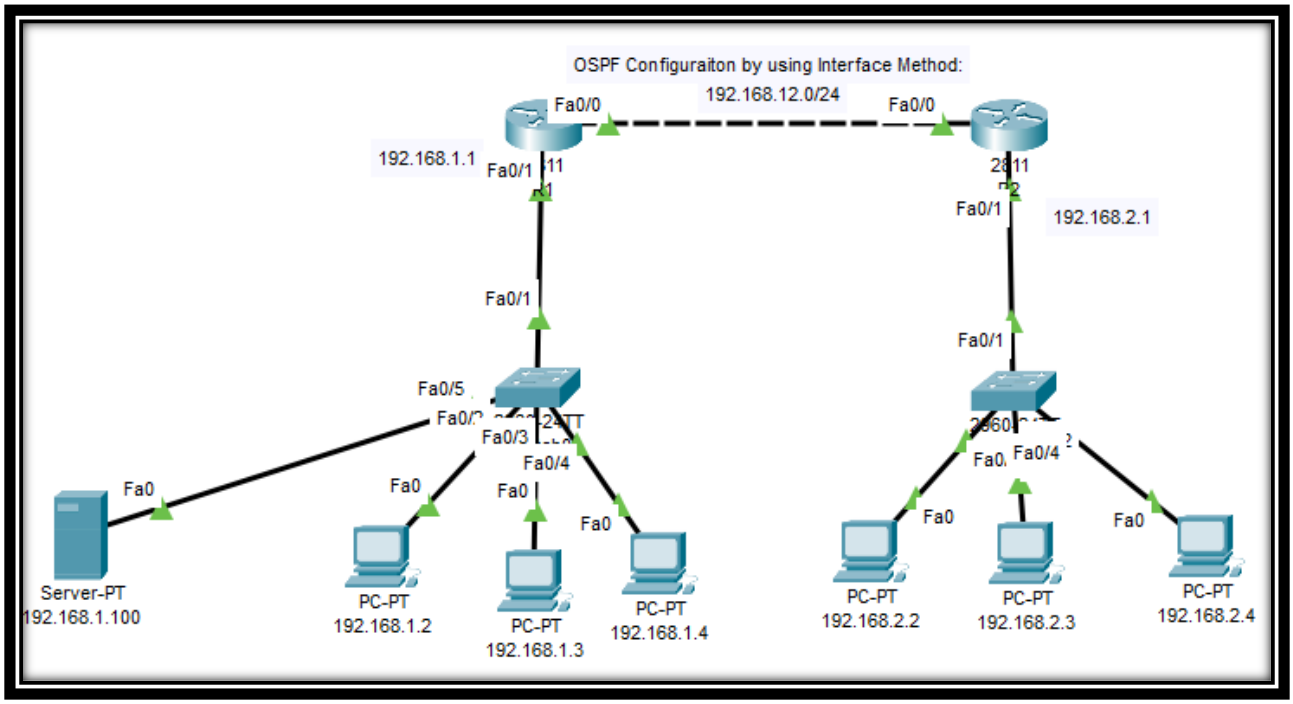
MESSAGE TEXT: A plain text description of the event.

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

6	Informational	Informational messages
7	Debug	Messages that contain information normally of use only when debugging a program

Lab time:



R1 Configuration	R2 Configuration
en config t hostname R1 int f0/0 ip add 192.168.12.1 255.255.255.0 no sh	en config t hostname R2 int f0/0 ip add 192.168.12.2 255.255.255.0 no sh

int f0/1 ip add 192.168.1.1 255.255.255.0 no sh router ospf 1 router-id 1.1.1.1 int f0/0 ip ospf 1 area 0 int f0/1 ip ospf 1 area 0 ntp server 192.168.1.100 logging host 192.168.1.100 Service timestamps log datetime msec	int f0/1 ip add 192.168.2.1 255.255.255.0 no sh router ospf 1 router-id 2.2.2.2 int f0/0 ip ospf 1 area 0 int f0/1 ip ospf 1 area 0 ntp server 192.168.1.100 logging host 192.168.1.100 Service timestamps log datetime msec