Netwok Monitoring with Syslog

Syslog is a powerful network monitoring tool which helps administrators to manage complex networks.it aggrigate logs/events from multiple sources and helps administrator to monitor from a single location.The logging server software must simplify log management, and help admins filter and focus on messages that truly matter

Syslog protocols are used to send logging/event messages to a separate network devices called syslog servers.

Syslog messages usually include information to help identify basic information about where, when, and why the log was sent: ip address, timestamp, and the actual log message.Syslog messages are plain text sent using UDP port 514.

Every syslog message contains two parts, a severity level and a facility. The severity level goes from 0 to 7 with 0 being the most severe to 7 being simply informational.Facilities are service identifiers that categorize events and messages for easier reporting

Syslog Priority (highest to lowest):

0	**Emergency (highest)**	**system is ususable**
1	Alert	action must be taken immediately
2	Critical	critical conditions
3	Error	error conditions
4	Warning	warning conditions
5	Notice	Normal but significant conditions
6	Informational	Informational messages
7	Debug (lowest)	debug level messages

The most common facilities related errors are

- IP
- OSPF
- SYS (operating system related)
- Route Switch Processor (RSP)
- Interface (IF)