**Syslog**

**A syslog process runs on a network device and sends event messages to a logging server (syslog server/viewer)**

* **Provides info about device to a network of a central location**

A ‘syslog’ refers to the log messages in transit or stored on the computer

Port 6154 (over TLS) and 514 are the ports used for syslog

When a message is sent to the syslog, it’ll contain a number referring to the facility e.g. kernel, user, daemon, auth, mail etc.

Rsyslog.conf

* Configure syslog