# **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**

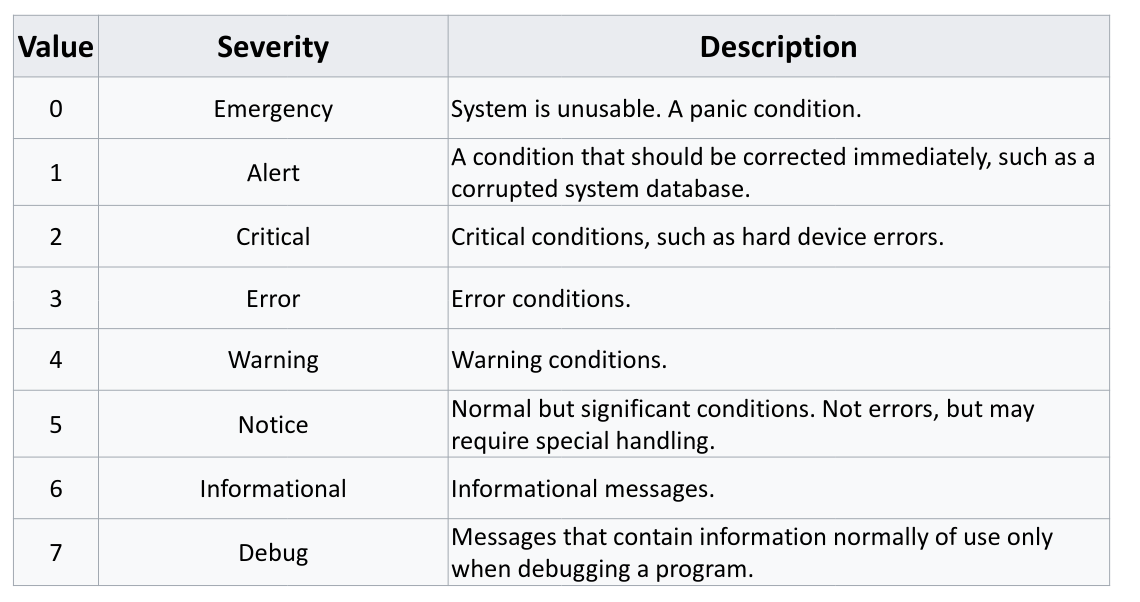
The format of the messages is:

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 Severity Levels**



## **Logging Locations**

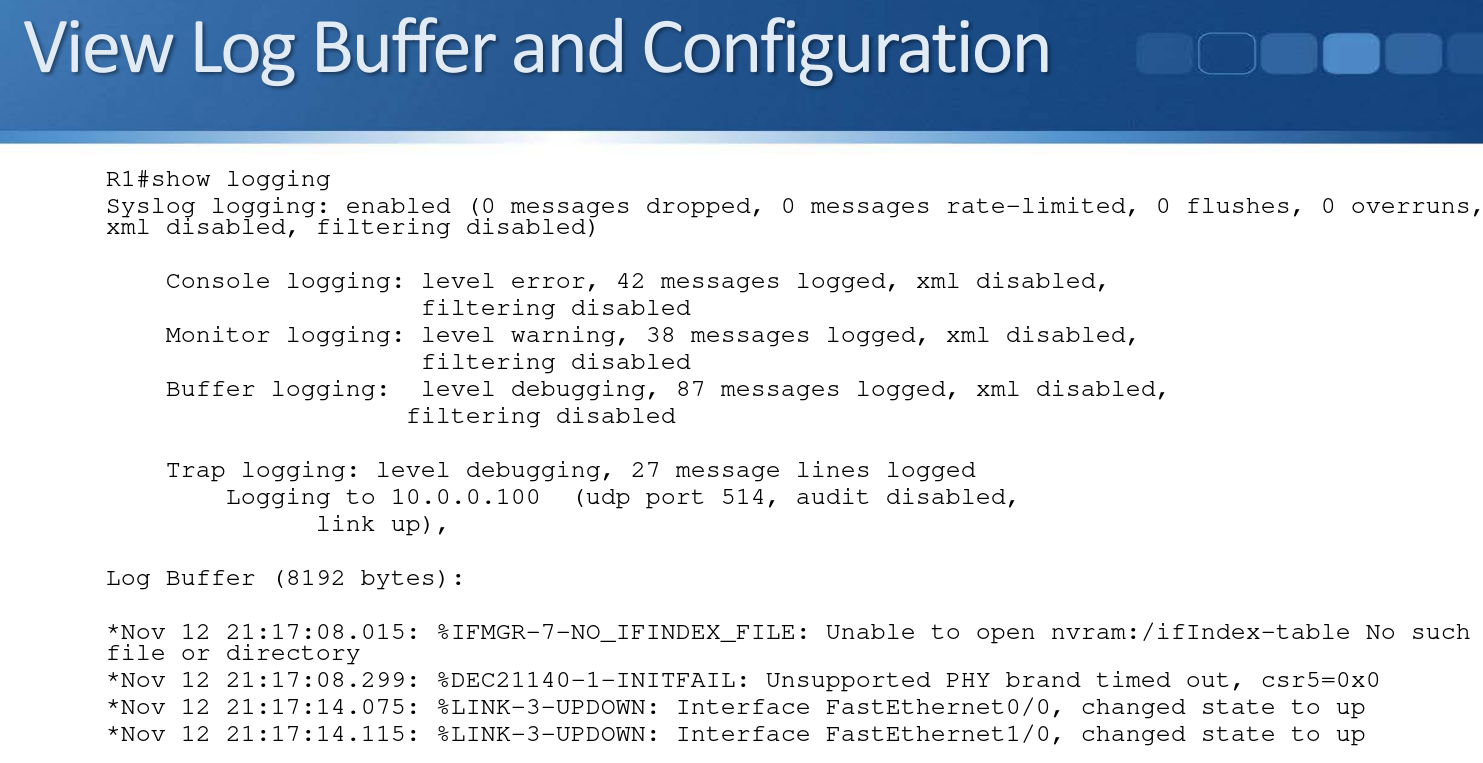
* Syslog messages can be logged to various locations:
  + **Console line** - events will be shown in the CLI when you are logged in over a console connection. All events logged by default
  + **VTY Terminal line**s - events will be shown in the CLI when you are logged in over a Telnet or SSH session. 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**
* 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)

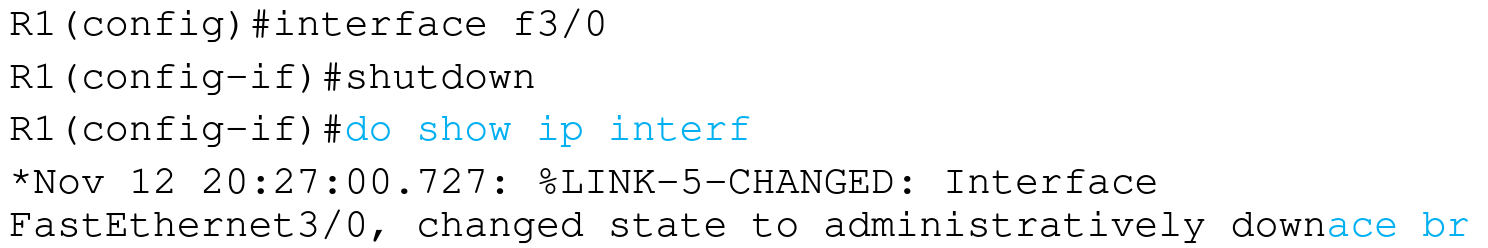
**Logging to an External Syslog Server**

* 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*

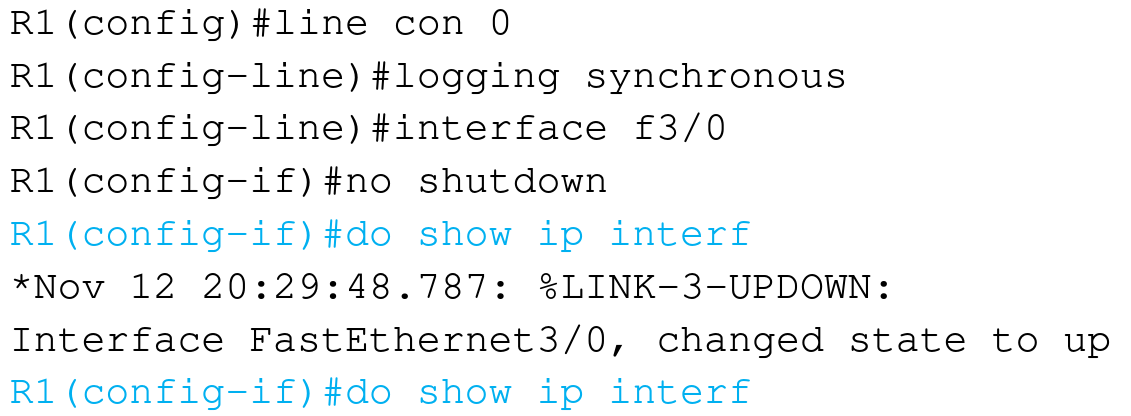


## **Logging Synchronous**

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



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



## **Debug and Terminal Monitor**

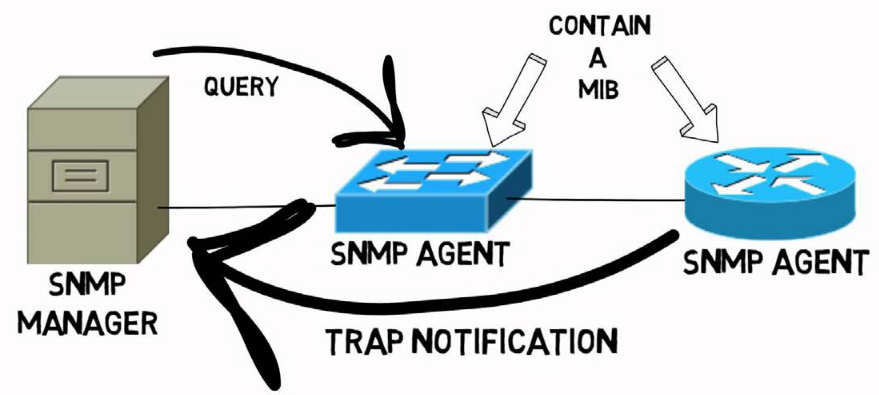
* Show and Debug commands can be used to view specific information over and above the standard Syslog messages
* Show output shows a static point in time state
* Debug output dynamically updates in real time
* Be careful with debug commands in production environments, a large amount of output can overwhelm 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

# **Simple Network Management Protocol (SNMP)**

* Simple Network Management Protocol (SNMP) is an open standard for network monitoring.
* An SNMP Manager (the SNMP server) can collect and organize information from an SNMP Agent, which is SNMP software which runs on managed devices such as routers and switches.
* The SNMP Manager is commonly called an SNMP Server or NMS (Network Management System).
* The SNMP Manager can pull information from the device (‘Get’) or the device can push it to the server (‘Trap’).
* For example the Manager could query traffic statistics from the device or the device could report an HSRP state change.
* The standard also includes support for modifying Agent information from the SNMP Manager to change device behaviour.

## **MIB Management Information Base**

* Data variables on SNMP managed systems are organized in a Management Information Base (MIB).
* The SNMP Manager and Agent need to share the MIB so they know which variables can be reported on.



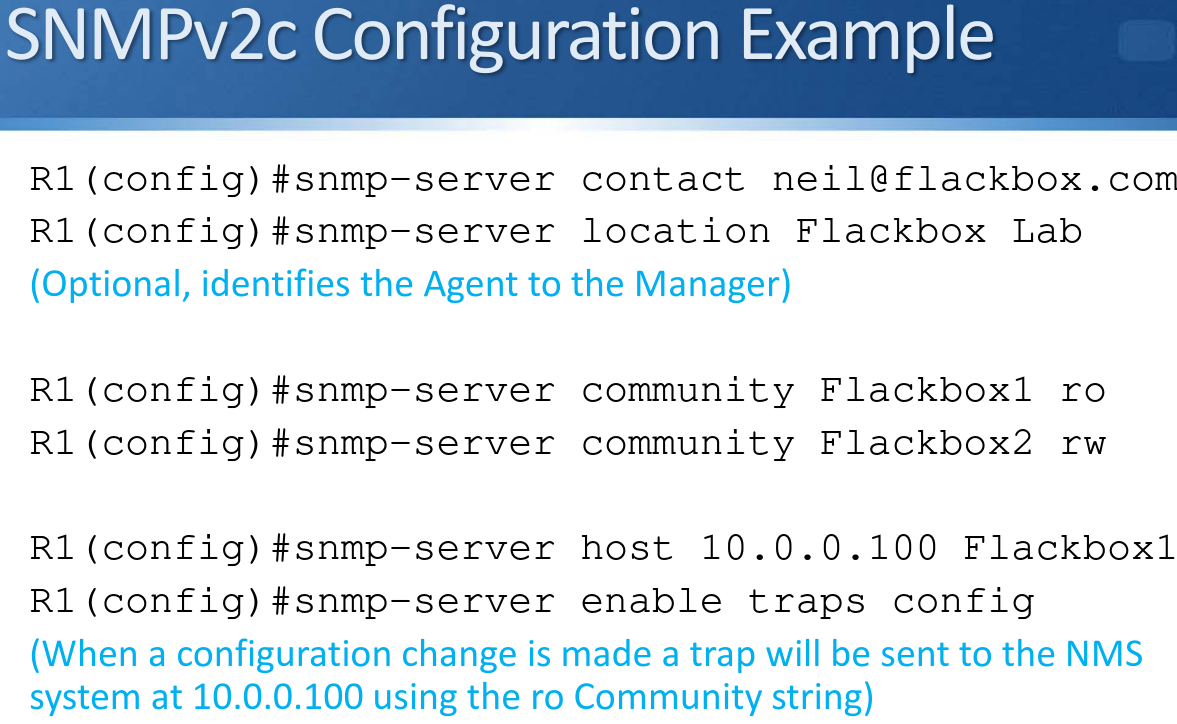
## **SNMP Versions**

* Three significant versions of SNMP have been developed and deployed.
* SNMPv1 uses plain text authentication between the Manager and Agent using matching Community strings.
* SNMPv2c also uses plain text Community strings. It supports bulk retrieval.
* SNMPv3 supports strong authentication and encryption. It is the preferred version but is not supported on all devices.

## **SNMPv2c Community Strings**

* SNMPv2c uses Community strings rather than a username and password to authenticate the SNMP Manager and Agent to each other
* Matching community strings need to be set on both sides for the Manager and Agent to communicate
* The read only (ro) community is used by the Manager to read information
* The read write (rw) community is used by the Manager to set information

## **SNMPv2 Configuration**

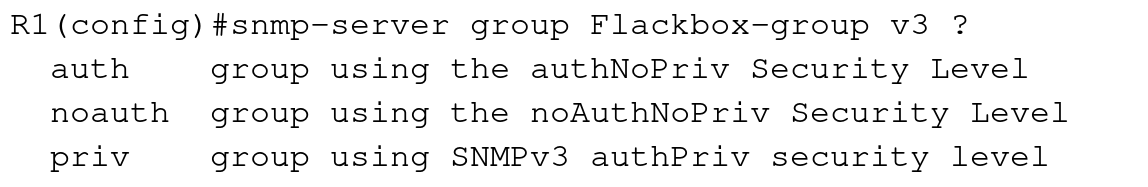


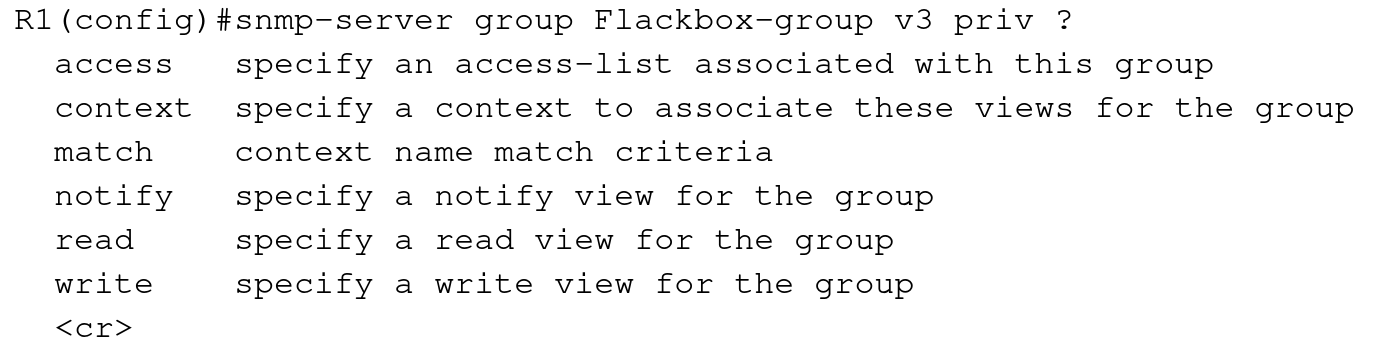
## **SNMPv3 Configuration**

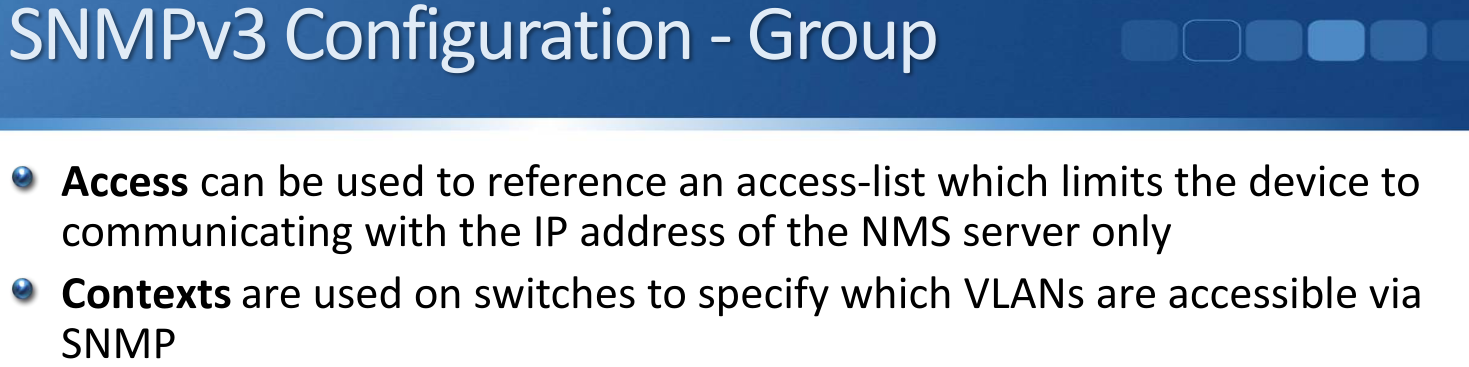
* The SNMP Manager and Agent recognise each other through simple unencrypted community strings in SNMP version 1 and 2
* SNMPv3 supports authentication and encryption
* The SNMPv3 security model works with users and groups
* A matching user account is set up on the NMS server and network device
* Settings are derived from the group the user is a member of

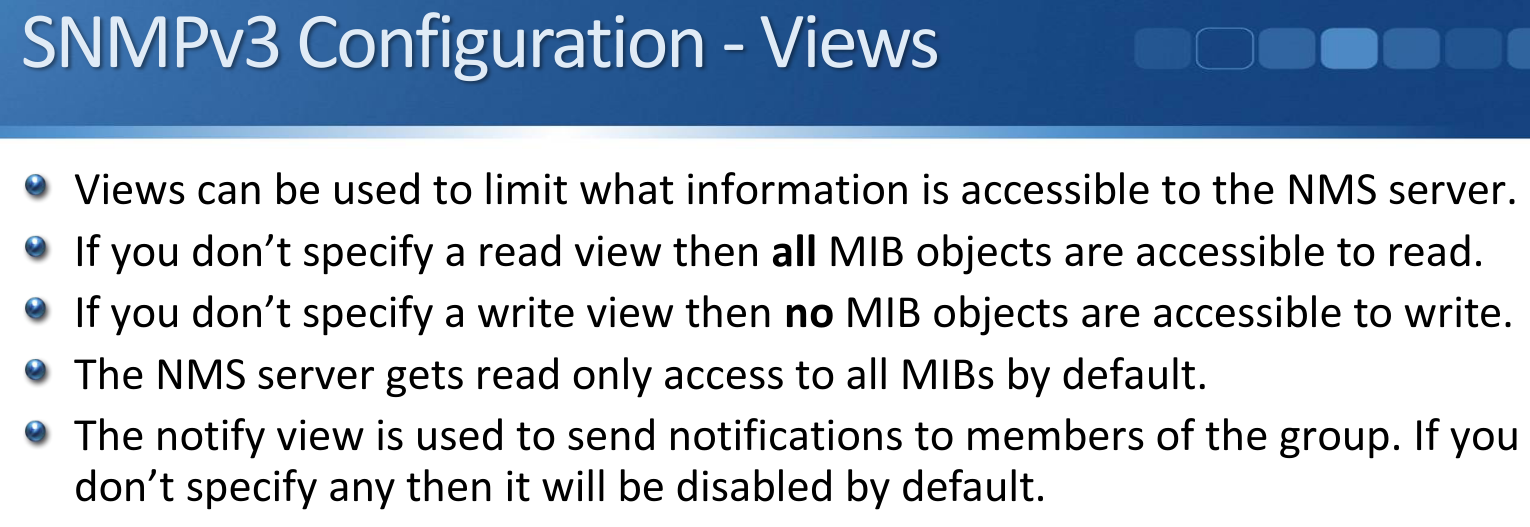
**SNMPv3 Security Levels**

* 3 different security levels are available. They are configured at the group level:
  + noAuthnoPriv - no authentication password is exchanged and the communications between the agent and the server are not encrypted. The username serves as replacement for community string.
  + AuthNoPriv - Password authentication is used. No encryption is used for communications between the devices.
  + AuthPriv - Password authentication is used. Communications between the agent and the server are also encrypted.

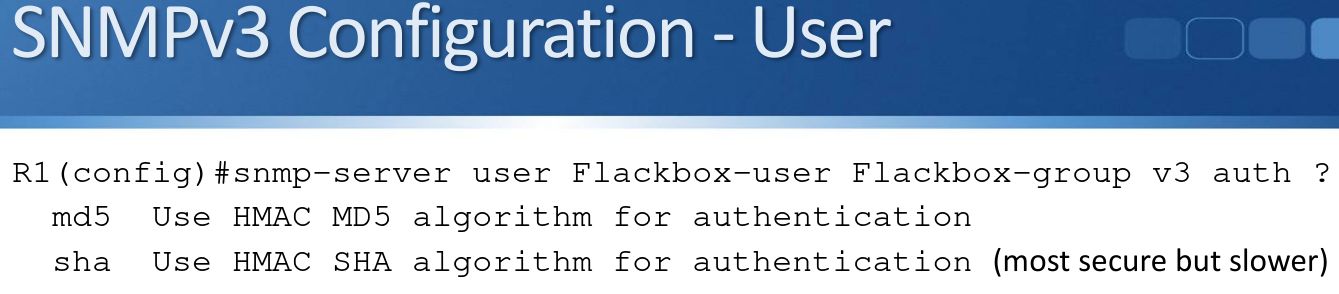












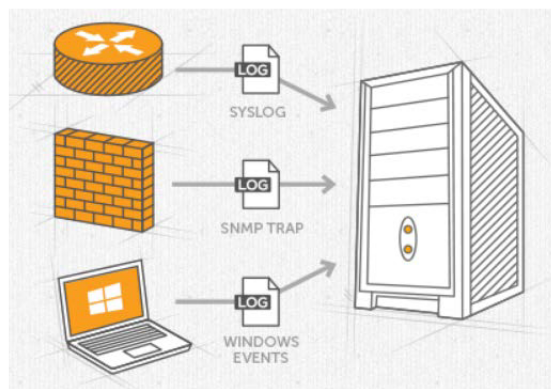






# **Syslog vs SNMP**

* Both Syslog and SNMP provide logging functionality.
* Syslog can often provide more granular detail than SNMP but it has support for the device pushing information only (not pulling or setting from the server).
* NMS servers will typically support both Syslog and SNMP



## **NMS vs SIEM**

* There is some overlap between NMS and SIEM products. Both can gather logging information from network infrastructure devices such as routers, switches and firewalls using protocols such as Syslog, SNMP and NetFlow.
* A product which is marketed as an NMS will have a focus on collating network information and provide reports, early warning of and easier troubleshooting of network events.
* A product which is marketed as a SIEM will have a focus on collating security information and provide reports, early warning of and easier troubleshooting of security events.