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 neighbor adjacency coming up

Syslog Format

- All vendors comply with this industry standard
- The format of the messages is:
    - Seq no:time stamp: %facility-severity-MNEMONIC:description
- Example:
- The form:

Syslog Severity Levels

Code	Severity	Keyword	Description	General Description
0	Emergency	emerg (panic)	System is unusable.	A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.
1	Alert	alert	Action must be taken immediately.	Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
2	Critical	crit	Critical conditions.	Should be corrected immediately, but indicates failure in a primary system, an example is a loss of a backup ISP connection.
3	Error	err (error)	Error conditions.	Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.
4	Warning	warning (warn)	Warning conditions.	Warning messages, not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
5	Notice	notice	Normal but significant condition.	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
6	Informational	info	Informational messages.	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.
7	Debug	debug	Debug-level messages.	Info useful to developers for debugging the application, not useful during operations.

A common mnemonic used to remember the syslog levels down to top is:
"Do I Notice When Evenings Come Around Early".

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 Lines - 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 Syslogservers
- 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

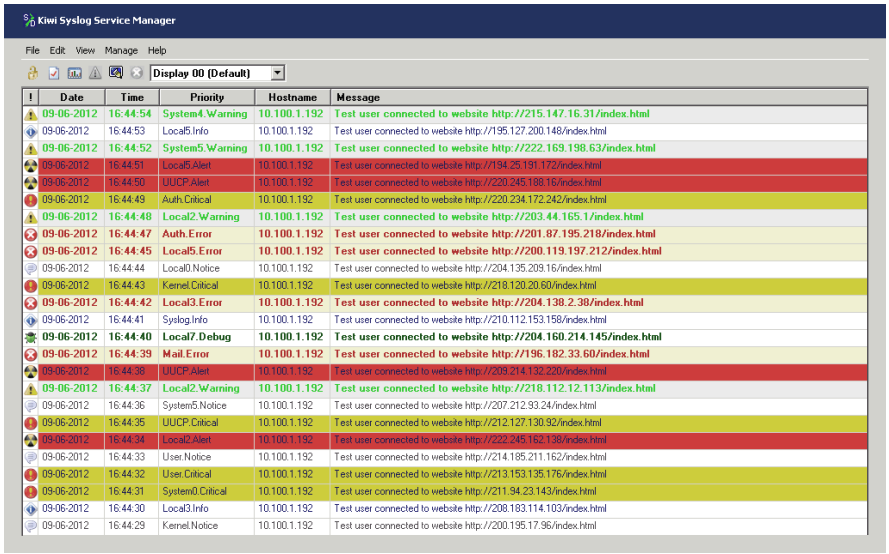
Internal Logging Locations Configuration

- R1(config)# no logging console (disables logging to the console)
- 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 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

```
R1(config)# logging 10.0.0.100
R1(config)# logging trap debugging
```



SIEM Security Information and Event Management

- A basic Syslog server provides a centralized location for Syslog logging messages

- A Security Information and EVent Management (SIEM) system provides a centralized location for all logging messages and will typically provide advanced analysis and correlation of events

View Log Buffer and Configuration
R1# Show logging

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

With no logging synchronous

```
R1(config)# interface f3/0
R1(config-if)# shutdown
R1(config-if)# do show ip inter
f*Jul 15 22:10:17.123: %LINK-5-CHANGED: Interface FastEthernet0/1, changed
state to administratively downace brief
```

With Logging Synchronous

```
R1(config)# interface f3/0
R1(config-if)# logging synchronous
R1(config-if)# shutdown
R1(config-if)# do show ip inter
f*Jul 15 22:10:17.123: %LINK-5-CHANGED: Interface FastEthernet0/1, changed
state to administratively down
R1(config-if)# do show ip inter  #Creates a new line where you left off
```

Debug and Terminal Monitor

- Show and Debug commands can be used to view specific info 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 industry-standard framework and protocol for network monitoring released in 1988
- 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

* More Advance so not needed but these are the type of messages

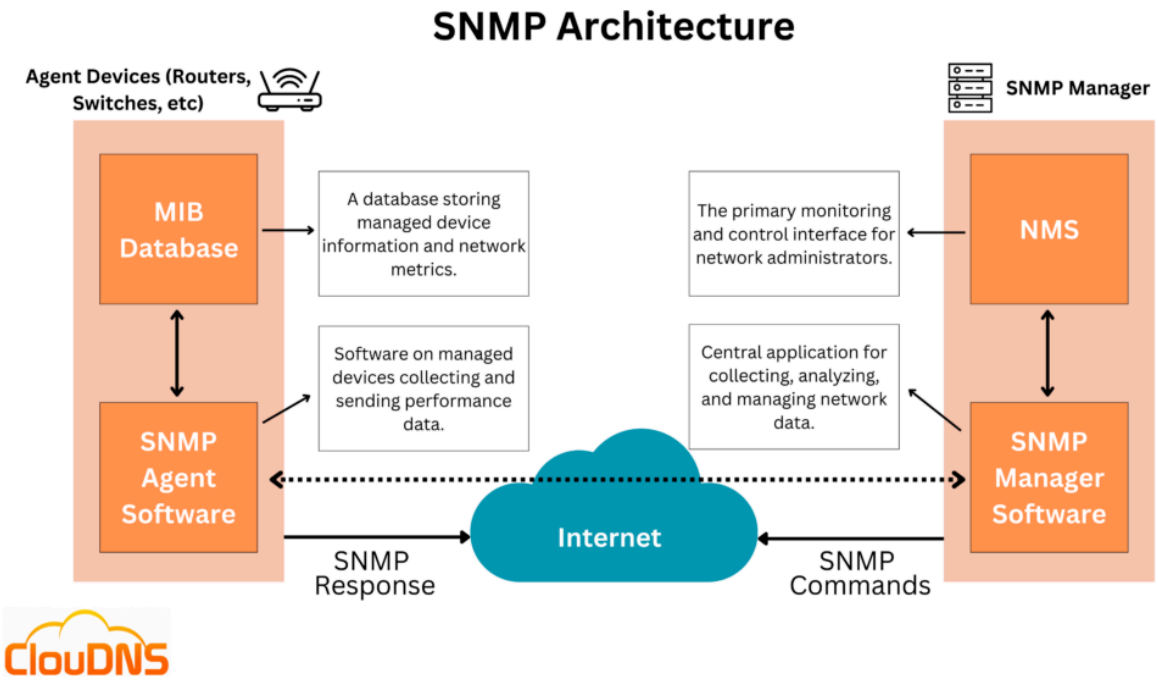
MIB – Management Information Base

- The **Management Information Base (MIB)** is a standardized database used by SNMP to organize data variables on managed devices.

- Both the **SNMP Manager** and **SNMP Agent** must share the same MIB definitions so they know which variables can be queried or updated.

A MIB acts as a structured database of information about a managed device. The device stores this information locally in its MIB. When an SNMP Manager (NMS) sends a query, the device references its MIB and responds with the requested value.

MIBs use a standard format defined by **Abstract Syntax Notation One (ASN.1)** — a machine-independent data representation language developed by the **ITU-T**. ASN.1 ensures that SNMP data can be exchanged consistently across different systems and platforms, making it readable by any SNMP-compliant management station regardless of the device vendor.



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’s the preferred version but is not supported on all devices

SNMPv2c Community String

- SNMPv2c uses Community strings rather than a username and password to authenticate the SNMP Manager and Agent to each other
- Matching community strings to 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 Manager to set

SNMPv2c Configuration Example

```
R1(config)# snmp-server contact neil@flackbox.com
R1(config)# snmp-server location Flackbox Lab
(Optional, identifies the Agent to the Manager)

R1(config)# snmp-server community Flackbox1 ro
R1(config)# snmp-server community Flackbox2 rw

R1(config)# snmp-server host 10.0.0.100 Flackbox1
R1(config)# snmp-server enable traps config
(When a configuration change is made a trap will be sent to the NMS system
at 10.0.0.100 using the ro community string)
```

SNMP Security Best Practice

- Most devices use a default ro Community string of ‘public’ and a default rw Community of ‘private’
- Attackers can use this to read or set information on your devices
- Best practice is to disable SNMP on devices where it’s not used
- Use SNMPv3 with secure passwords on devices where it’s used
- If SNMPv3 is not supported, use non-default Community strings

SNMPv3 configuration

- The SNMP Manager and Agent recognize 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

```
# Define a new SNMP group with authentication and privacy (encryption)
R1(config)# snmp-server group Flackbox-group v3 priv

# Create a user assigned to the group with SHA authentication and AES-128
encryption
R1(config)# snmp-server user flackuser Flackbox-group v3 auth sha
AuthPASS123 priv aes 128 PrivPASS456
```

- Flackbox-group is the name of the group.
- flackuser is the SNMPv3 username.
- AuthPASS123 is the authentication password (SHA).
- PrivPASS456 is the privacy (encryption) password (AES-128).

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

SNMPv3 Configuration - Group
R1(config)# snmp-server group Flackbox-group v3 ?
    Access

R1(config)# snmp-server group Flackbox-group v3 priv

- Access can be used to reference an access-list which limits the device to communicating with the IP address of the NMS server only
- Contexts are used on switches to specify which VLANs are accessible via SNMP

SNMPv3 Configuration - Views
- Views can be used to limit what information is accessible to the NMS server
- If you don’t specify a read view then all MIB objects are accessible to read
- If you don’t specify a write view then no MIB objects are accessible to write
- The NMS server gets read only access to all MIBs by default
- The notify view is used to send notifications to members of the group. If you don’t specify any then it will be disabled by default

SNMPv3 Configuration - User

```
R1(config)# snmp-server group Flackbox-group v3 auth ?
      Md5   Use HMAC MD5 algorithm for authentication
      Sha   Use AES algorithm for encryption (most secure but slower)
      Des   Use 56 bit DES algorithm for encryption

R1(config)# snmp-server group Flackbox-group v3 auth sha AUTHPASSWORD priv
?
      128   Use 128 bit AES algorithm for encryption
      192   Use 192 bit AES algorithm for encryption
      256   Use 256 bit AES algorithm for encryption

R1(config)# snmp-server group Flackbox-group v3 auth sha AuthPASSWORD priv
aes 128 PRIVPASSWORD
```

Now, the user and group are set up on the router or switch. Next, configure a user on the NMS server with matching settings: the same username, authentication password, and privacy password. The NMS server will then be able to access the device and pull information from it.

Agent vs. Agentless (Probe) Monitoring

There are two main approaches to monitoring network devices:

- **Agent Monitoring**
  An **agent** is lightweight software installed directly on the monitored device. It provides deep monitoring and local access to APIs and system-level data.
    - Supports local services like Patch Management, Automation, Backup, and Antivirus
    - Enables direct integration with the NMS for richer features
- **Agentless (Probe) Monitoring**
  A **probe** is a standalone software or device that monitors devices remotely over the network without needing to install anything on the target device.
    - Uses protocols like **SNMP**, **TCP**, **Syslog**, and **WMI**
    - Cannot access local APIs or enable advanced monitoring features
    - Ideal for switches, routers, and appliances that can't run agents

Definition:

- **Agent** – Installed software that enables direct, local monitoring of a device

- **Probe** – External tool that gathers monitoring data remotely over the network

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 using information only (not pulling or setting from the server)
- NMS servers will typically support both syslog and SNMP

NMS vs SIEM

- There's 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

NMS	SIEM
a focus on collating network information and provide reports, early warning of and easier troubleshooting of network events	a focus on collating security information and provide reports, early warning of and easier troubleshooting of security events

Remote Monitoring(RMON)

Remote Monitoring, also called **RMON**, is an addition to the Simple Network Management Protocol (SNMP) and is implemented as a standard Management Information Base (MIB). RMON supports more comprehensive monitoring of Ethernet network operations. With RMON, remote traffic can be monitored from a central network location. Using a standard MIB, information is received by the administrator only after an information request is sent to the device. In contrast, RMON can utilize software, network devices, or both, to capture, record and present information.

MON Probe Supports Traffic Monitoring

Devices with RMON capabilities include **RMON probes**, which are physical hardware for temporary or permanent network installs. The RMON-enabled probe is often permanently installed to streamline traffic monitoring. Some devices come with RMON probes embedded into them. These can be switches, hubs, routers or other equipment. RMON alarm triggers can be set that warn of specific conditions, such as traffic errors. The alerts allow for proactive corrections. A management console can request statistics from an RMON device for analysis or forwarding to the administrator.

Two RMON Versions Supply Network Statistics

The RMON extension of the SNMP specifies nine groups of elements for Ethernet traffic monitoring. This means administrators can view statistics on: sent and dropped packets, user bandwidth demands, bytes transmitted, and specific network events. There are **two RMON versions**, RMON1 and RMON2. RMON1 performs inspections at Layers 1 and 2 of the OSI model. RMON2 can monitor higher traffic layers. SMON is associated with RMON; SMON allows for the in-depth monitoring of a switched network.