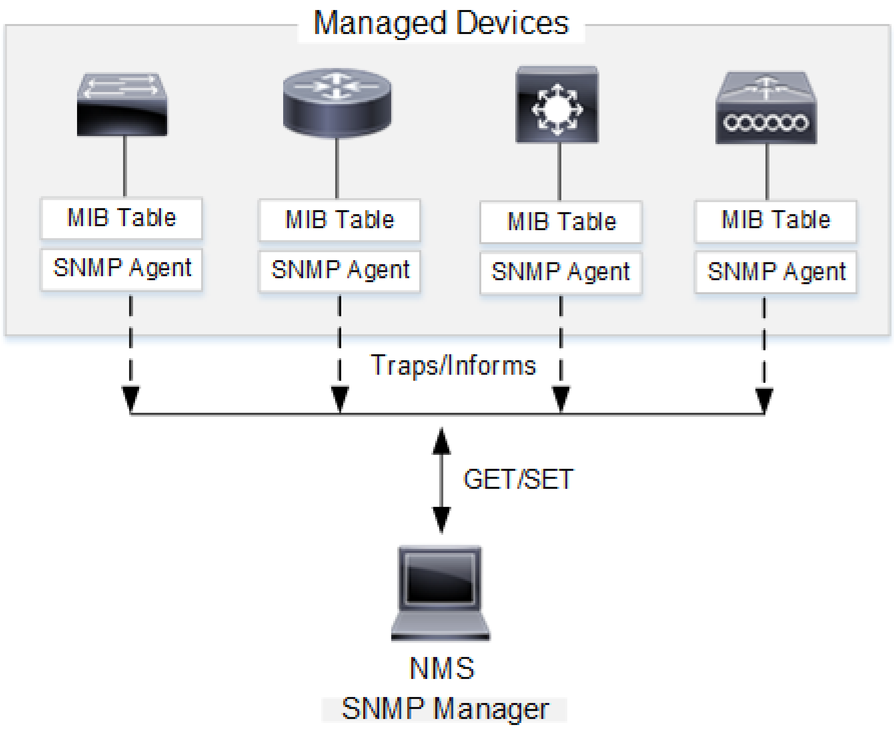
SNMP Monitoring Protocol

SNMP is an agent-based management protocol used for monitoring of network devices. It is enabled for performance monitoring along with operational status and errors . The following are standard SNMP architecture components for data communication.

- SNMP Manager
- SNMP Agents
- Managed Devices

Figure 1 SNMP Operation



Managed Devices

It is common to enable all network devices and servers for SNMP-based monitoring. In fact, Cisco network devices are already pre-installed with SNMP support. There are various IOS commands that enable operation of SNMP on each network device. There is often automated turn up of SNMP monitoring when each device is active on the production network.

SNMP Agents

All SNMP-enabled network devices have an SNMP agent. It is a software module that communicates between MIBs and SNMP manager. There are vendor specific hardware MIBs installed on each device that monitor and collect operational data. Initially network administrators will configure Cisco devices with IOS commands to enable SNMP features. The following are some examples of common MIBs for Cisco equipment.

- Cisco-OSPF-MIB
- Cisco-VLAN-MEMBERSHIP-MIB

SNMP agents send operational status information to an SNMP manager as a TRAP alert message. There are INFORM messages as well that are similar and only available with SNMPv3. The difference is that INFORM messages include an acknowledgment from SNMP manager.

SNMP Manager

SNMP agents send alert messages to an SNMP manager. SNMP manager is referred to as network management station (NMS). It is the centralized monitoring software that receives SNMP messages from network devices. SNMP manager must enable SNMP alerts required, polling interval and reporting. SNMP agent responds by collecting MIB data and forwarding to NMS. For example, report interface status of router-1 at five second intervals.

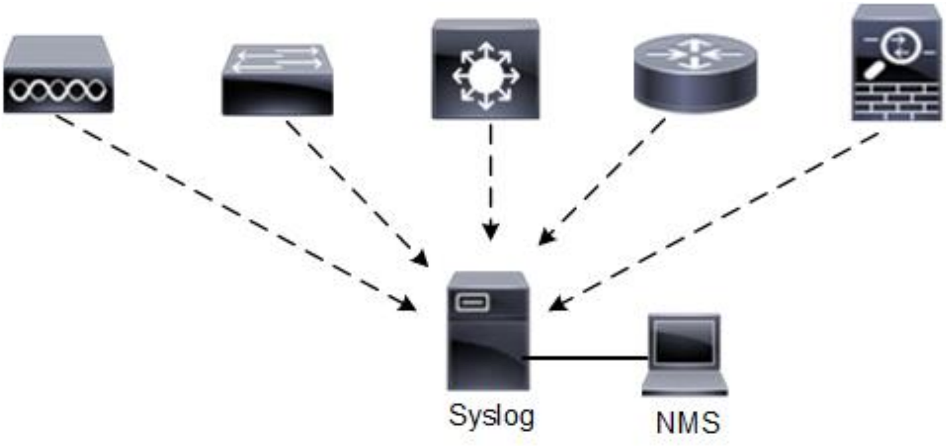
IP address of NMS is configured on each network device with an IOS command. SNMP agents will then forward all message TRAPS to that destination IP address. SNMPv2 authentication type used is community strings. It enables device authentication between SNMP agent and NMS for read-only or read-right access. Recently, SNMPv3 includes security enhancements such as message integrity, encryption and authentication.

Syslog Server

Syslog is an open standard protocol designed to enable communication between a network device and Syslog server. It is an external store for system messages that are generated by multiple network devices. Syslog enables centralized management and analysis of system messages. There is network monitoring software (NMS) available to access log files for reporting, troubleshooting and audit purposes.

- Syslog services provide an external system message store
- Syslog service provides more scalability that local store
- Syslog messaging is disabled by default

Figure 2 Syslog Server



Syslog defines eight severity levels for different system message types as shown with Table 1. The default logging level for Syslog messages is to receive informational (6) and lower messages. Debug messages (level 7) are not sent to Syslog in a default configuration.

Table 1 Message Logging Levels

***Level**	**Message**
0	emergencies
1	alerts
2	critical
3	errors
4	warnings
5	notifications
6	informational
7	debugging

* Message severity level sends all lower messages as well

Syslog logging facility permits classifying and storing messages from different sources to create separate log files. For example, Cisco has a default facility of local7 that permits multiple log files based on device type. You could create and classify log files based on event type as well. Syslog is UDP-based so that packets are sometimes dropped during periods of network congestion. There is no device authentication available between Cisco network devices and Syslog server.

Syslog Configuration

The following global IOS commands send system messages to a Syslog server at 192.168.3.1 address with timestamps enabled. In addition, all messages are sent with severity level 0 to debug (7).

```
router(config)# service timestamps log datetime msec
router(config)# service timestamps debug datetime msec
router(config)# logging on
router(config)# logging host 192.168.3.1
router(config)# logging trap 7
```

The **logging** command enables a Cisco device to log SNMP traps from 0 up to and including level 7. The traps are logged to the Syslog server.

```
router(config)# logging trap [level]
```

The **logging facility** command enables you to create separate log files based on message type such as hardware, protocol or module for example. Syslog enables seven logging facilities from local0 to local7 with the Cisco default ***local7.***

Cisco Default Logging Configuration

- Logging service is enabled
- Syslog server is disabled
- Logging facility is local7
- Informational (Level 6) messages and lower enabled
- System messages are enabled on console
- System messages are disabled on VTY lines (terminal monitor)
- System messages are stored in local buffer memory