SNMP and Syslog

- **SNMP version 1 (SNMPv1)**—This was the first implementation, operating within the structure management information specification, and described in RFC 1157.
- **SNMP version 2 (SNMPv2)**—This version was improved to support more efficient error handling and is described in RFC 1901. It was first introduced as RFC 1441. It is often referred to as SNMPv2c.
- **SNMP version 3 (SNMPv3)**—This version improves security and privacy. It was introduced in RFC 3410.

These are the main runtime components in an SNMP-enabled environment:

- **SNMP-managed devices and resources**—These are the devices and network elements on which an agent runs.
- **SNMP agent**—This software runs on the hardware or service being monitored by SNMP, collecting data on various metrics like CPU usage, bandwidth usage or disk space. As queried by the SNMP manager, the agent finds and sends this information back to SNMP management systems.
- **SNMP manager**—(also referred to as SNMP server) This component functions as a centralized management station running an SNMP management application on many different operating system environments. It actively requests agents send SNMP updates at regular intervals.
- **Management information base (MIB)**—This data structure is a text file (with a .mib file extension) that describes all data objects used by a particular device that can be queried or controlled using SNMP including access control. Inside the MIB there are many different managed objects which can be identified by Object Identifiers. An Object Identifier (OID) is a MIB identifier that is used to delineate between devices within the MIB. OIDs are uniquely generated as numeric identifiers used for access to MIB objects.

- **Get Request**—A request to retrieve the value of a variable or list of variables.
- **Set Request**—Sent by the SNMP manager to the agent to issue configurations or commands.
- **GetNext Request**—Sent by the SNMP manager to agent to find the values of the next record in the MIB's hierarchy.
- **GetBulk Request**—Sent by the SNMP manager to the agent to obtain large tables of data by performing multiple GetNext Request commands.
- **SNMP Response**—Sent by the agent to the SNMP manager, issued in reply to a
- **SNMP Trap**—Asynchronous trap messages from SNMP agents alert an SNMP manager that a significant event such as an error or failure, has occurred.
- **SNMP Inform**—Confirms receipt of a trap.

UDP 162 goes from Agents to Managers

UDP 162 goes from Managers to Agents

GetRequest/GetResponse

GetNextRequest/Respoinse
Get Bulk /

Agent to Manager

Trap, Response, Inform (Confirms receipt of Trap