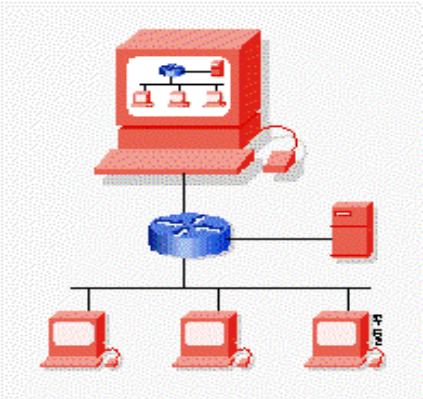
Net Management Protocols - Made Simple



Network Management is used to automate the processes of monitoring and adjusting the performance of a network, as well as providing reports about network activity.

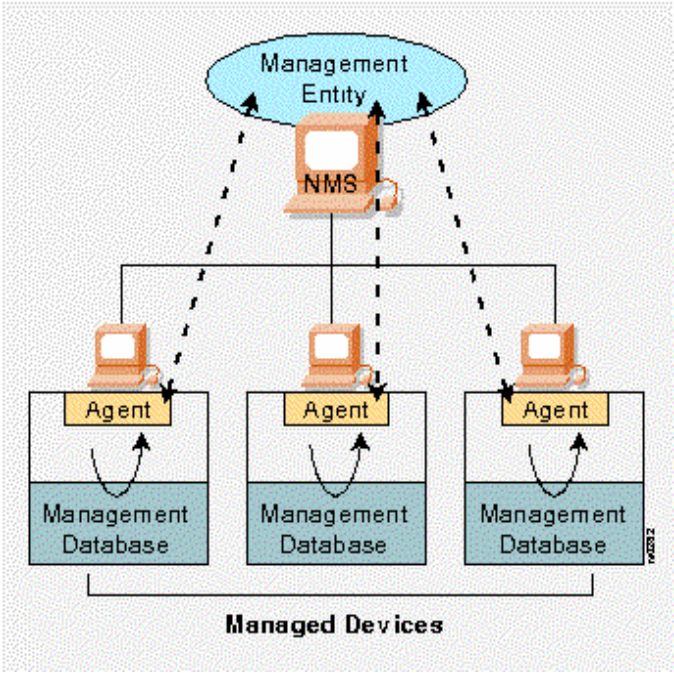
SNMP (Simple Network Management Protocol) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite.

SNMP allows network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP Basic Components: There are three key components of an SNMP managed network:

Managed device -- A managed device is a network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make this information available to network management systems (NMSs) using SNMP.

Managed devices, sometimes called network elements, can be routers, switches and bridges, hubs, computer hosts, or printers.



Agent -- An agent is a network management software module that resides in a managed device. It has local knowledge of management information and translates that information into a form compatible with SNMP.

Network management system (NMS) -- An NMS executes applications that monitor and control managed devices. They provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network.

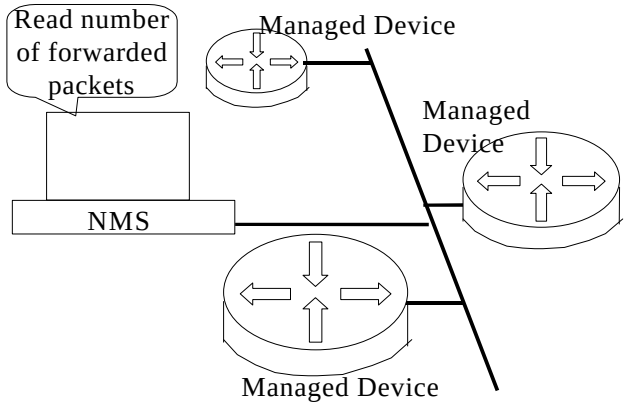
SNMP Basic Commands: Managed devices are monitored and controlled using four basic SNMP commands:

Read -- The read command is used by a network management system (NMS) to monitor managed devices. The NMS examines different variables that are maintained by managed devices.

Write -- The write command is used by an NMS to control managed devices. The NMS changes the values of variables stored within managed devices.

Trap -- The trap command is used by managed devices to asynchronously report events to the NMS. When

OPERATION OF SNMP COMMANDS



certain types of events occur, a managed device sends a trap to the NMS.

Traversal operations -- are used by the NMS to determine which variables, a managed device supports and to, sequentially gather information in variable tables (such as a routing table).

SNMP MIB (Management Information Base): A MIB is a collection of information that is organized hierarchically. MIBs are accessed using a network management protocol such as SNMP. MIBs are composed of managed objects and are identified by object identifiers. A managed object (sometimes called a MIB object, an object, or a MIB) is one of any number of specific characteristics of a managed device. An object identifier (or object ID) uniquely identifies a managed object in the MIB hierarchy.

SNMP must account for and adjust to incompatibilities between managed devices. Different computers use different data-representation techniques, which can compromise the ability of SNMP to exchange information between managed devices.

There are two versions of SNMP:

SNMP Version 1 (SNMPv1) is the initial implementation of the SNMP protocol. SNMPv1 operates over such

protocols as User Datagram Protocol (UDP), Internet Protocol (IP), OSI connectionless Network Service (CLNS), and Novell Internet Packet Exchange (IPX) etc

to name a few. SNMPv1 is widely used and is the de facto network management protocol in the Internet community.

SNMP Version 2 (SNMPv2) is the successor to SNMPv1. SNMPv2 takes care of the deficiencies found in SNMPv1. The deficiencies were: lack of manager-to-manager communication, the inability to do bulk data transfer, and a lack of security.

SNMPv1 can generate considerable traffic when managers communicate with agents. That's because a single SNMPv1 transaction can exchange only a limited amount of data, forcing management workstations and agents to often generate multiple transactions. The result is a heavy load on the network.

To help streamline these exchanges, SNMPv2 adds a new command, GetBulkRequest. This command is very

useful in retrieval of tables which generate a lot of network traffic. A table represents a related set of information about a resource (ex. a router) or activity (the traffic over a TCP connection). It is organised as a collection of rows of variables, with each row having the same sequence of variables.

With SNMPv1, you could retrieve information from such a table only one row at a time. If we want to get the entire routing table, a tedious series of get/response transactions, one for each row is needed.

Using GetBulkRequest, a manager can retrieve the entire table with one transaction and even retrieve additional nontable information in that same transaction.

SNMPv2 adds another command - the Inform command, which is used for manager-to-manager co-operation. For example, through Inform, a manager notifies another manager when an unusual event occurs, like the loss of a physical link or an excessive rate of traffic at some point in the network. Such unsolicited notifications provide an ideal tool for configuring a decentralised network.

SNMP Management: SNMP is a distributed management protocol. A system can operate exclusively as either a network management system (NMS) or an agent, or can perform the functions of both.

When a system is operating as both an NMS and as an agent, another NMS might require that the system query managed devices and provide a summary of the information learned, or that it report locally stored management information.

SNMP Security: SNMP lacks any authentication capabilities, resulting in vulnerability to a variety of security threats:

Masquerade - consists of an unauthorized entity attempting to perform management operations by assuming the identity of an authorized management entity.

Modification of information -- This consists of an unauthorized entity attempting to alter a message generated by an authorized entity so that the message

results in unauthorized accounting management or configuration management operations.

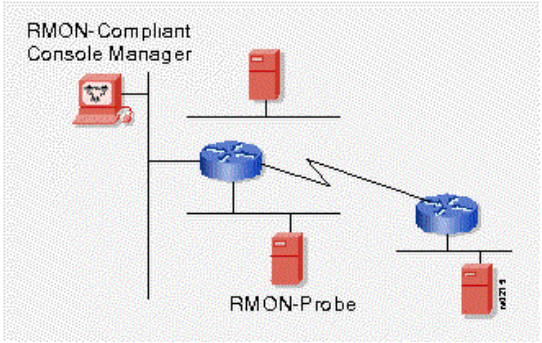
Message sequence and timing modifications -- These consist of an unauthorized entity reordering, delaying, or copying and later replaying a message generated by an authorized entity.

Disclosure -- This consists of an unauthorized entity learning values stored in managed objects, or learning of notifiable events by monitoring exchanges between managers and agents.

Because SNMP does not implement authentication, many vendors do not implement Set operations, thereby reducing SNMP to a monitoring facility.

RMON MIB (Remote MONitoring - Management Information Base) addresses the limitations of SNMP in growing distributed networks.

SNMP has two distinct polling disadvantages. (Polling is



nothing but the process of obtaining information from the agents' MIB.) The disadvantages are:

1) It does not scale well. In large networks, we have more agents and hence more network management traffic, thereby contributing to congestion problems.

2) It places the burden of collection on the network management console. Management stations that can easily collect information on eight segments might not be able to keep up when monitoring 48 segments.

RMON allows us to manage networks with minimal disruption to network activity and it makes minimal demands on the available resources. The RMON MIB allows SNMP to monitor remote devices more effectively and more pro-actively.

The key to RMON's monitoring effectiveness is its ability to store the history of statistical data at the probe, thereby removing the need for continual polling to build a view of network performance trends. The above figure shows an RMON-probe capable of monitoring an Ethernet segment and transmitting statistical information back to an RMON-compliant console.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network fault diagnosis, planning, and performance tuning information.

Send in your Feedback , Comments & Suggestions to:

Harish Kumar S, SSO Trg Centre, Hyderabad.