Simple Network Management Protocol (SNMP)

Introduction

A major explanation for its universal acceptance is its relative simplicity, as well as being the dominant network management standard on the Internet. Nonetheless, the development of an SNMP application was not as simple as one wishes. The creation of management applications for managing the number of networked devices that need to be handled needed significant efforts.

.

SNMP is able to provide enhanced tools for end-to - end management in all areas of the growing Internet industry.ow, as more SNMP tools are available, the problem is improving. SNMP versions such as SNMP V1, SNMP V2c and SNMP V3 are also available. SNMP is ready to provide end-to - end management in all areas of the growing Internet industry with enhanced resources.

What exactly is SNMP?

It is a part of the Transmission Control Protocol feature suite of the Internet Framework (TCP/IP).The only structured network management system in use today is SNMP management. The SNMP standards set includes a basis for defining information on management and a protocol on information sharing. The SNMP model takes administrators and employees into account. A manager is a software module responsible on behalf of the network management applications and users for the control of a part or the entire configuration. An agent is a

software module in a managed system which maintains and provides information to the manager via SNMP.. A management information exchange can be initiated by the manager (via polling) or by the agent (via a trap).

Agents act as collectors who collect and send managed resource data in order to respond to a manager's request. The default SNMP ports are UDP ports 161 and 162. The agent listens to and answers requests on port 161 and records asynchronous traps on port 162, unless separate ports are instructed. SNMP adapts resources to which proxies are not used to implement SNMP software. A SNMP agent supplies information for one or more Non-SNMP devices on behalf of a proxy.

When did SNMP start?

Protocol was started in 1980’s.It was designed to be simple so that there would be nothing to be in the way of it's deployment. There were several factors in it's design. The first was interoperability meaning you could deploy it and be assured it would work across all platforms. The next was robustness meaning that it would not easily fail. The next was low overhead. Therefore it limited itself to the UDP or User Datagram Protocol. This meant that the deployer was responsible for lost and retransmitted packets and this was considered essential. The last was in ease of debugging the protocol.

How Does SNMP work?

The simple network management protocol (SNMP) used for controlling connected devices for any administrative purposes. For instance, SNMP may be used by all of the following devices to manage IP network devices:

1. Network router
2. Network switch
3. Printer
4. NAS server
5. ADSL ISP router / modem
6. Linux / UNIX / Windows servers
7. Workstation and more.

Administrators can find or manage network performance, solve problems or even optimize it further. SNMP works at the Application Layer of the Internet Protocol Suite (Layer 7 of the OSI model).

SNMP basic Components

SNMP consists of

- SNMP Manager
- Managed Devices
- SNMP agent

SNMP Manager

A manager or management system is a separate entity that is responsible to communicate with the SNMP agent implemented network devices. This is typically a computer that is used to run one or more network management systems.

SNMP Manager's key functions

- Queries agents
- Gets responses from agents
- Sets variables in agents
- Acknowledges asynchronous events from agents

Managed Devices

A managed device or the network element is a part of the network that requires some form of monitoring and management

For example: Routers, Switches, servers, workstations, printers etc.

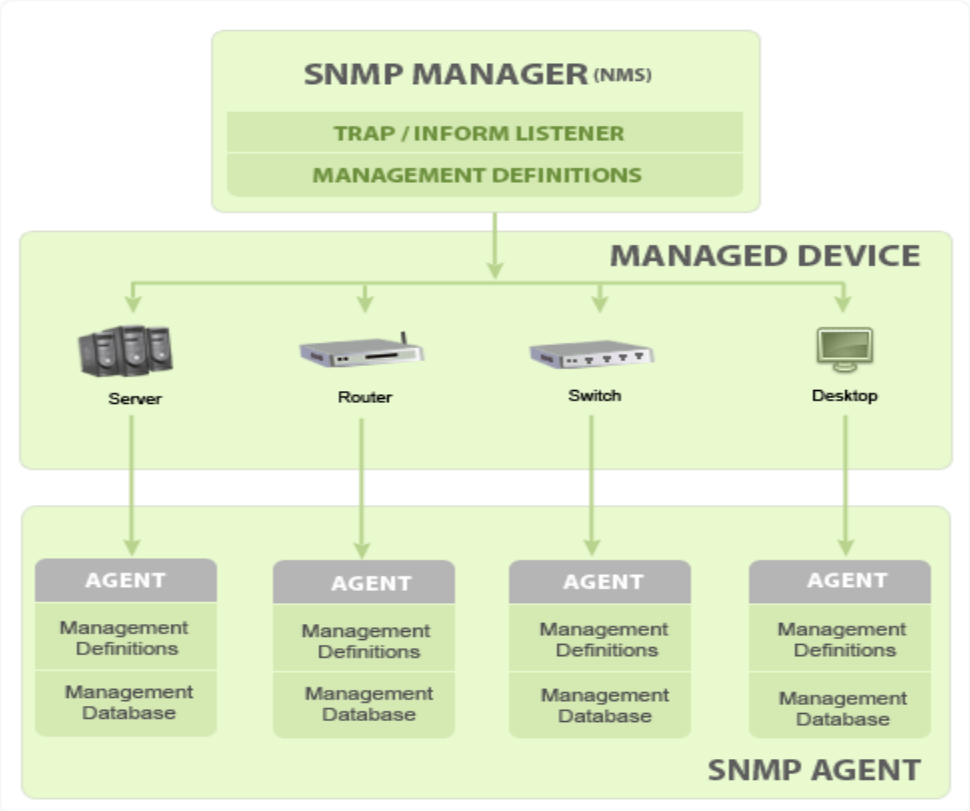
SNMP Agent

The agent is a program that is packaged within the network element. Enabling the agent allows it to collect the management information database from the device locally and makes it available to the SNMP manager, when it is queried for.

SNMP agent's key functions

- Collects management information about its local environment.
- Stores and retrieves management information as defined in the MIB.
- Signals an event to the manager.
- Acts as a proxy for some non–SNMP manageable network nodes.

SNMP communication diagram

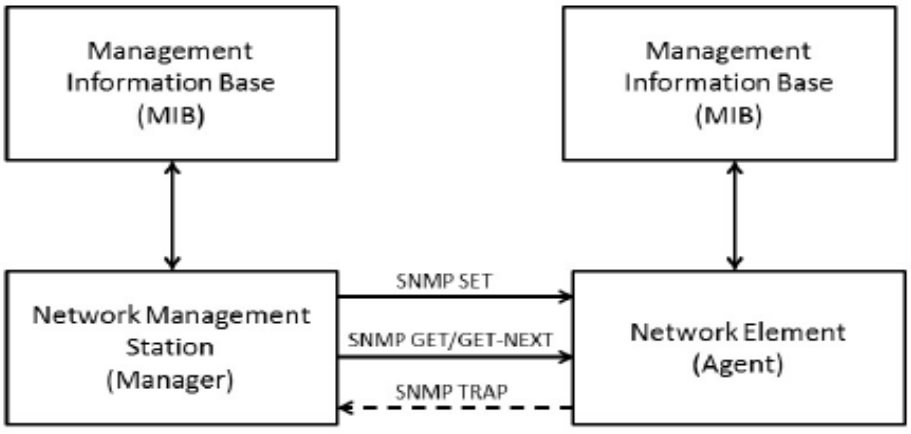


SNMP Architecture

SNMP uses a hierarchical architecture of management systems and organizations as well as many modules to execute its monitoring services. A SNMP agent is provided by Windows Server 2003 and is configured to deal with any SNMP management. The building blocks for SNMP and the SNMP agent Windows Server 2003 are given as follows:

- SNMP management systems and agents
- Management Information Base (MIB)
- SNMP Messages
- SNMP Communities
- The communication process between SNMP managers and agents

SNMP is divided into the management and agent roles that overlap in several situations, the internal architecture of the implementation of the Window Server 2003.



SNMP messages –

Different variables are:

1. **GetRequest –**
   SNMP manager sends this message to request data from SNMP agent. It is simply used to retrieve data from SNMP agent. In response to this, SNMP agent responds with requested value through response message.
2. **GetNextRequest –**
   This message can be sent to discover what data is available on a SNMP agent. The SNMP manager can request for data continuously until no more data is left. In this way, SNMP manager can take knowledge of all the available data on SNMP agent.
3. **GetBulkRequest –**
   This message is used to retrieve large data at once by the SNMP manager from SNMP agent. It is introduced in SNMPv2c.
4. **SetRequest –**
   It is used by SNMP manager to set the value of an object instance on the SNMP agent.
5. **Response –**
   It is a message send from agent upon a request from manager. When sent in response to Get messages, it will contain the data requested. When sent in response to Set message, it will contain the newly set value as confirmation that the value has been set.

6. **Trap –**

   These are the message send by the agent without being requested by the manager. It is sent when a fault has occurred.
7. **InformRequest –**

   It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to set trap continuously until it receives an Inform message. It is same as trap but adds an acknowledgement that trap doesn't provide.

SNMP security levels –

It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are 3 security levels namely:

1. **noAuthNoPriv –**

   This (no authentication, no privacy) security level uses community string for authentication and no encryption for privacy.
2. **authNopriv –** This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.
3. **authPriv –** This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses DES-56 algorithm

Advantages

-Widely Accepted and works good for device monitoring
-basic monitoring MIBs are (like IF-MIB) are well defined and implemented in most of the devices
-Vendor specific MIBs also defined , provides additional support
-Very good for Fault management

Disadvantages

- Wont scale, large retrieval are slower
- Its complex to implement MIBs than CLI commands
- Config rollback is not so easy
- SNMP provide data centric view , difficult to relate to task centric view from operator point of view
- MIBs lacks proper description , understanding will be difficult

SNMP versions

Since the inception SNMP, has gone through significant upgrades. However SNMP Protocol v1 and v2c are the most implemented versions of SNMP. Support to SNMP Protocol v3 has recently started catching up as it is more secured when compare to its older versions, but still it has not reached considerable market share.

SNMPv1:

This is the first version of SNMP protocol, which is defined in RFCs 1155 and 1157

SNMPv2c:

This is the revised protocol, which includes enhancements of SNMPv1 in the areas of protocol packet types, transport mappings, MIB structure elements but using the existing SNMPv1 administration structure ("community based" and hence SNMPv2c). It is defined in RFC 1901, RFC 1905, RFC 1906, RFC 2578.

SNMPv3:

SNMPv3 defines the secure version of the SNMP. SNMPv3 protocol also facilitates remote configuration of the SNMP entities. It is defined by RFC 1905, RFC 1906, RFC 3411, RFC 3412, RFC 3414, RFC 3415.

Though each version had matured towards rich functionalities, additional emphasis was given to the security aspect on each upgrade. Here is a small clip on each editions security aspect.

CONCLUSION

In conclusion, if you have to handle Enterprise data delivery, SNMP is a great choice.The new versions that provide protection and other enhancements make the protocol a better way to communicate data and hold the multiplatform details because it is one of today’s most used protocols.