Another use of SNMP

By Martin Alfonsi
May 22, 2000

The need exists for a product, designed to permit companies to monitor and manage their facility infrastructure (i.e. Physical Security, Access Control, CCTV, Fire Systems, HVAC, Lighting, Elevator Controls, Emergency Power Systems, Utilities, Multi-media, etc.). The ability to remotely manage such disparate components is made possible through the use of SNMP.

What is SNMP?

SNMP is an acronym for Simple Network Management Protocol. One of the many Internet Protocols, SNMP is designed to give a user the ability to remotely manage disparate computer devices in a network in order to maximize efficiency and productivity.

There are five areas of network management:

1) Security Management - Includes all actions and information used to prevent access, use or alteration of the network and physical and logical isolation of key network components.
2) Fault Management - Observing how well a network is working, is a router down, has a device disappeared etc Fault Management includes both Reactive and Proactive fault detection.
3) Configuration Management - Collecting and setting information on
    a. Inventory - the set of devices (hardware and software) on a network and their associated static information.
    b. Configuration - map of how components are interconnected.
    c. Provisioning - the setting of changeable parameters that detail how each device will function.
4) Performance Management - Monitoring how well the network is functioning. Throughput, bandwidth usage etc. This includes analysis of both real time and historic data.
5) Accounting Management - Used to determine the cost of operating and maintaining a network and to monitor usage (for billing).
6) Asset Management - Provides the statistical record keeping of equipment and personnel.
7) Planning Management - Involves analysis of data to permit proactive changes in order to insure the health and security of the network.

SNMP is the tool you can use that allows a single workstation to remotely manage and control thousands of network devices. Information can be collected to aid in determining the state and health of a network and it's component parts.

How are devices managed?

A device on a network can either be managed locally or remotely.

When managed locally, a human operator is required to set dip switches, watch LEDs, press buttons etc. The more devices on a network, the harder it is to manage them locally.

When managed remotely, the device must have a *management port* that can be accessed either by modem or through a network. The *management port* must be designed to permit a remote operator to accomplish many of the same tasks that can be accomplished locally. Obviously in a network with thousands of devices it is advantageous to be able to provide remote management. However, if each vendor employs a different method of allowing remote management, then the problems may be reduced, but certainly not eliminated.

SNMP provides standardization to the process of remote monitoring and control. SNMP is a component of the Internet protocol suite and as such the Internet community develops and standardizes the implementation of the protocols in order to transport and manage applicable data.

SNMP is universally supported. Since it is a standard, many vendors of internet capable equipment allow the use of the same type of SNMP management interface.

SNMP is extendible. It has been designed to support any type of device that may be part of a network. Vendors are free to determine the details of the information and management provided, but the mechanism is standardized.

SNMP is portable. As part of its design and implementation, SNMP is entirely operating system independent.

SNMP is lightweight. In it's basic form, SNMP consumes a small amount of resource. It use does not dramatically affect workload or bandwidth utilization.

There are two basic parts to SNMP. The Manager and the Agent. The Manager typically runs on a computer or workstation and is used to collect management information from the agents and pass on commands for operations to be performed. Conversely the agent sends information to the manager regarding state or event and receives and processes commands received.
Any network device is 'being managed' when it is actively being monitored by an agent. It then becomes a 'managed node' and becomes a member of a 'management community'. The 'agent' is software or firmware that runs as a process on the node. The agent provides information to the manager as requested, and may send un-requested information known as 'traps'.

When the agent is actually running on the 'node' it is managing, the node is said to 'support SNMP management'. If the agent is not running on the node it is reporting on, it is said to be a 'proxy agent'.

Managed objects are commonly manipulated using *Get, GetNext and Set* commands, which are defined by SNMP protocol. The pattern for the organization of the data being exchanged is normally called a *MIB (Management Information Base).* This information is stored as a *MIB Variable´* whose instances are controlled by the agent. Most MIB variables are static and exist as long as the agent exists. Some are dynamic and come and go as needed by the agent. A logical collection of management data is usually referred to as a MIB database, while the actual data is referred to as MIB data.

The MIB is structured like a tree. The top level provides the most general information while each branch of the tree gets more detailed.

Information is exchanged between Managers and Agents via Protocol Data Units (PDUs). Since PDUs are sent over a network, they are 'encapsulated' into data envelopes (like any other network data) with headers, trailers and payloads.

SNMP is a request-and-response protocol. The manager sends a request to an agent (*Get, GetNext and Set)* and the agent responds to indicate the request was performed or if an error occurred. There is a special type of unsolicited message from an agent called a *trap*, which reports an unexpected event.

This is all very theoretical and an understanding is necessary only to foster awareness of the practical use of SNMP, which is through a SNMP Management Application.

SNMP Management Application

Commercial SNMP Management software is now available from a number of sources. The most notable being HP's Open View, IBM's NetView and Novell's Manage Wise. As networks grow and proliferate we can expect more offerings in this area. Many of these new management applications are designed to operate on workstations with an operating system such as Windows NT, UNIX, Linux etc, however some are being written as embedded applications found within test equipment such a Fluke LanMeter,, Trippe Power Administrator etc

Although all have some type of character-based interface, more are developing easy to use and intuitive graphical user interfaces.

Network Management Applications are designed to be as generic as possible so that any MIB can be viewed, or any trap received and decoded. The more robust applications, such as HP's Open View provide automatic network discovery, network topology map generation, MIB compiler and browser, trap log and polling managers. Although there are a number of custom management applications, they have a drawback in that they only support one brand or class of devices. It may take a number of custom management applications to properly manage a diverse network.

In very large networks, the shear volume of data and events may easily overwhelm all but the most robust Management Application Systems. This is especially true when there are a large number of different devices. Therefore many Network Administrators are turning to *Intermediate Management Systems.*

These are nothing more than a layer of Network Management Applications that sit between the devices and the top layer. Generally all signals from a given class or type of managed node is handled by a dedicated Intermediate Management System, certain signals are passed up to the Enterprise Wide Management System. This system then acts as both Manager and Agent. To the devices that are being monitored, it is a manger, but to the Enterprise Wide Network Management Application it appears as an agent. Intermediate managers can also be used as a gateway to translate one management protocol to another. This is especially helpful when either the source or destination is not SNMP compliant. This will be especially true in implementing an SNMP solution in the Command and Control environment.

SNMP

Our goal is to develop the ability to provide Enterprise Wide Monitoring over a diverse span of nodes that are reporting from a variety of systems such as:

- Physical Security,
- Access Control,
- CCTV,
- Fire System,
- Building Automation,
- HVAC,
- Lighting,
- Elevator Controls,
- Emergency Power Systems,
- Utilities,
- Multi-Media

Although some of these systems now provide SNMP compliant messages, most do not. In fact there is no accepted messaging standard within these industries.

Therefore we will design and develop a series of software elements that will act as Intermediate Management Systems. This software based upon existing technology and proven drivers, will be used to convert the diverse signals to uniform SNMP compliant messages that can be processed and monitored by a generic best of breed Management Application System such as OpenView or NetView.

By using SNMP to communicate through an Enterprise Class product such as Open View provides a multitude of possible actions and reactions resulting from an alarm or event. Event logging, paging and problem escalation are second nature to SNMP Management Applications. Quick to implement modular components help to gain control over any environment.

Since SNMP is a lightweight network application its use will help to maximize existing bandwidth while providing a seamless solution. SNMP combined with Open View integrates existing security devices and controls into the management console at the event level. Integrating these capabilities with centralized managament provides the most comprehensive Command and Control solution available