Asante

SIMPLE NETWORK MANAGEMENT PROTOCOL

INTRODUCTION

The Simple Network Management Protocol (SNMP) is an application layer protocol used to manage network resources. This standardization gives network administrators the ability to monitor network performance.

Background

The computer networks of today are growing at a tremendous rate. Technology continually allows consumers and businesses to build bigger and better networks at more affordable prices. With the increase in the size and number of computer networks, the need for efficient management of resources has emerged as a pressing issue for network administrators. Administrators are constantly maintaining their networks in order to maximize efficiency. The Simple Network Management Protocol was developed to assist in network resource management.

History

SNMP is a network management specification that has become the standard for the exchange of network information. Prior to SNMP and other network management software, administrators would have to be physically attached to network devices in order to access configuration and troubleshooting data. SNMP was designed to facilitate this process while reducing the complexity of network management. The specifications for this protocol can be found in Request For Comments 1157 (RFC 1157).

Established in the late 1980s, SNMP was developed to tackle the management of emerging TCP/IP networks. The Internet Engineering Task Force (IETF) had the task of producing a standard to which LAN-based internetworking devices such as hubs, bridges, and routers could be monitored. SNMP has grown to be the most accepted application layer protocol used for this chore. It allows different network products to be managed by the same management application by setting a standard to which vendors of network products can interoperate with one another. SNMP does this by using a subset of the Abstract Syntax Notation One (ASN.1) encoding scheme.

Versions

There are three versions of SNMP: SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2) and SNMP version 3 (SNMPv3). SNMPv1 (RFC 1157) was easy to implement but had numerous security problems. SNMPv2 (RFC 1902) offered enhanced security and functionality, but was still lacking features in security

authentication and encryption. SNMPv3, which was designed to be backward compatible with the first two versions, addresses these concerns by including access control, authentication, and privacy of management information. SNMPv3 was just recently released and can be found in the RFC drafts 2271-2275 and 3410-3415.

FUNCTIONALITY

A system of network components works together to form the functionality of SNMP.

Components

The SNMP has three basic components: the Structure of Management Information (SMI), the Management Information Base (MIB), and the SNMP agents (see Figure 1).

- The Structure of Management Information (SMI)
  The SMI defines the data types that are allowed in the MIB. It sets aside a unique naming structure for each managed object. How the managed objects are contained in the MIB is set forth in RFC 1155. Typically MIB objects have six attributes. An object will have a name, an object identifier, a syntax field, an access field, a status field, and a text description.

- Management Information Base (MIB)
  The MIB is a collection of network information. This information is stored in a database of managed objects that can be accessed using network-managing protocols such as SNMP. The managed objects contained in MIB are defined in RFC 1156.

  A managed object can represent a characteristic of a certain managed device. The MIB object may hold a value associated with the number of packets that have come in since the last system reset. It may store the number of clock ticks since the last reset or even a specific administrative state of a device.

  These values are stored in scalar and tabular forms. Scalar objects define a singular object instance. A tabular object defines a group of object instances that are found in MIB tables.

- SNMP Agents
  All network devices that are to be SNMP managed need to be fitted with an agent that executes all the MIB objects that are relevant. The agent provides the information contained in the MIB to management applications when asked.

SNMP polls for information gathered by a network agent. The agent collects data from the network device it is located on and stores it in the MIB. When polled, the agent will send the information back to the SNMP manager.

Implementation

Architecture

An SNMP-managed network includes management stations and network devices. The management stations execute management applications like SNMP, which monitor network performance. Network agents are responsible for maintaining network statistics for management stations. When asked, each managed network device is expected to communicate such information for processing.

SMI enables a vendor to write an SMI-compatible management object. This object is run through a MIB compiler to create an executable code. The code is installed in network devices and management consoles that in turn generate network reports.

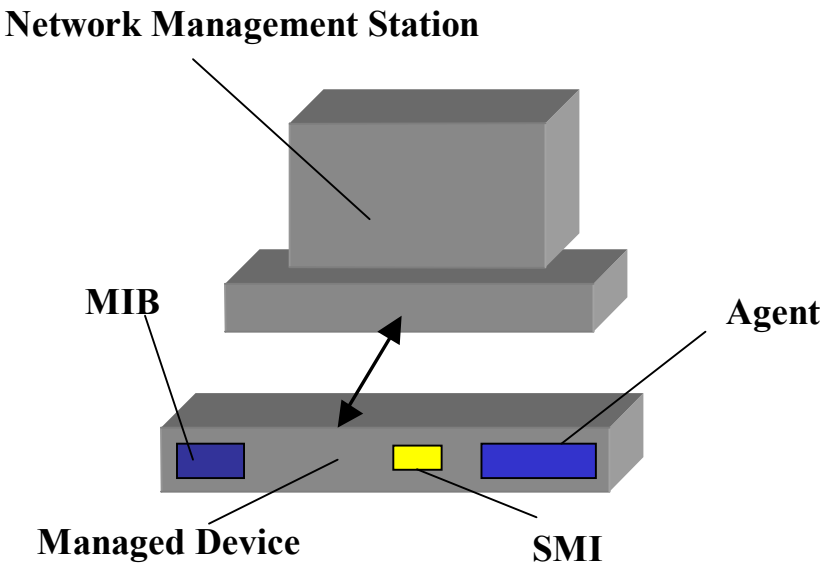

Figure 1: SNMP Components

Commands

SNMP is a network management application. This application contains several basic commands, including **read, write, trap,** and **traversal operations.**

- The ***read*** command enables system manager to monitor managed devices. It allows for the examination of different variables that the network device may be collecting.

- The ***write*** command allows the system manager to control managed devices. It lets the values stored in the variables to be changed.
- The ***trap*** command is used by a managed device to send updates to the system manager. If the managed device needs to report anything significant regarding its network status, it will use a trap command.
- ***Traversal operations*** let the system manager retrieve information found in variable tables. It allows a network manager to sort through information in a step-by-step fashion.

SNMPv1 Protocol Operations

Among the SNMP commands are specific protocol operations that facilitate in the requests and responses of managed network devices. The most basic operations include: **Get, GetNext, Set,** and **Trap** (see Figure 2).

- ***Get*** is used by the SMI to retrieve the value of an object instance from an agent.
- ***GetNext*** is used by the SMI to retrieve the value of the next object instance from a table within an agent. It allows the administrator to step through objects in tabular form.
- The ***Set*** function is used to write a value to an object instance within an agent.
- ***Traps*** are used by agents to send information to the network management system.

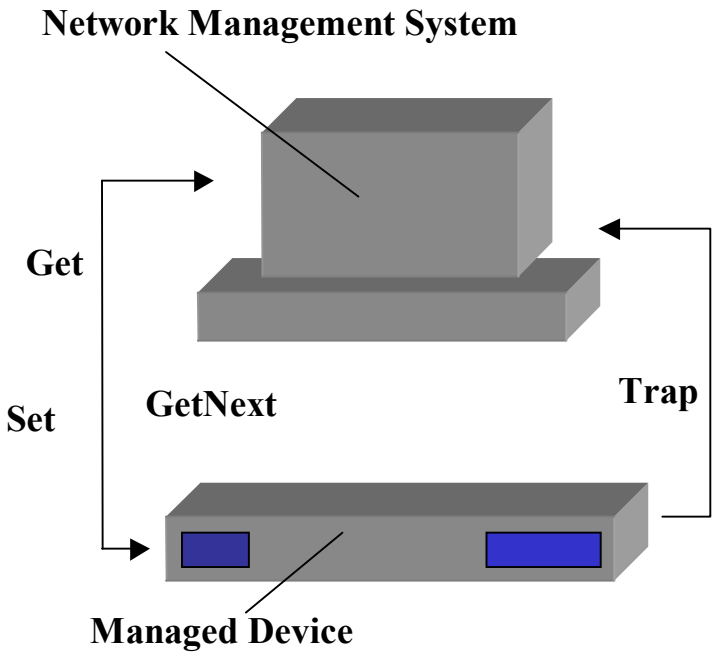

Figure 2: SNMP Operations

BENEFITS

Implementation of an SNMP-compliant network offers significant benefits. These benefits allow a network administrator control in managing a healthy and efficient network.

Control
The benefits of running an SNMP-compliant application include the abilities to prevent, detect, and correct network-related issues. SNMP is easy-to-use and allows administrators the control they need to maintain a healthy network. It provides administrators with a network management mechanism that efficiently monitors network performance.

Popularity
SNMP is virtually supported by every enterprise network equipment manufacturer in the world. Its centralized management system is an extremely effective and widespread solution to network management. Because TCP/IP networks have become so popular, implementation and compatibility have become easy.

Efficiency
SNMP also utilizes the User Datagram Protocol (UDP) to deliver packets called protocol data units (PDUs). UDP is a quick method of transmitting data because it has low overhead costs. Unlike TCP, UDP lacks much of the acknowledgement

features that guard against broken transmissions. Thus, the intermittent messages SNMP sends and the constant flow of status updates and alerts are kept at a minimum compared to TCP.

The control network administrators have with SNMP is extremely beneficial. With it, they are able to monitor and change network performance according to its needs. This proves vital with growing networks.

LIMITATIONS

As with most good things, SNMP has its drawbacks. The drawbacks found in SNMP include the simplistic nature of its transmission protocol and its security.

Simplicity
Because SNMP uses UDP as its transmission protocol, it lacks many reliability and security issues. UDP runs on a very rudimentary level, using only the most basic transmission segments. While this connectionless protocol runs with fewer network resources, it does not ensure the data is correctly received. As networks increase in size, an increase in polling may be required to manage the system. This can increase the overhead of resources and would be inefficient.

Security
Security has been a big concern with SNMPv1 and SNMPv2. Neither provides adequate security features such as management message authentication and encryption. With these holes in security, an unauthorized user could execute network management functions. Networks can be brought to a crawl if a malicious user carries out these actions. Deficiencies such as these have led many operations to have read-only capability. SNMPv3 addresses these issues and provides security enhancements in this area.

ALTERNATIVE

The Common Management Information Protocol (CMIP) is another alternative to network management. Developed by the International Organization for Standardization (ISO), CMIP was designed to address the same problems SNMP addresses. However, CIMP takes up more system resources and is designed to run on the ISO protocol stack. Most systems today use TCP/IP.

ADVANCED FEATURES

Asante incorporates SNMPv1 in its family of IntraCore switches. This protocol is provided as a standard because Asanté understands the necessities required in managing a successful and efficient networking system. With the SNMP functionality, the basic

features include separate read and write communities, and a trap authentication. There are also 4 configurable trap receivers.

In addition to SNMP, Asanté offers numerous other features that aid in delivering the most productive networking environment.

Asante OneView
To further enhance the facilitation of network management, Asanté offers the IntraCore 3524 series, which is bundled with the Asanté OneView management architecture. OneView's powerful architecture allows network administrators to manage the network via a command line prompt (telnet), Simple Network Management Protocol (SNMP), or web browser interfaces over in-band Ethernet, or out-of-band serial communications via telnet. Enterprises may stack and manage up to 8 switches, or 194 ports under a single IP address—a feature that greatly eases management of the network and gives network administrators greater control over configuration.

VLAN
Virtual Local Area Networks (VLANs) are logical groupings of network users that are connected to administratively defined ports on a switch. This grouping of end stations may differ from the physical segmentation of a LAN. The benefit of such architecture is improved performance and manageability of a network. Each VLAN can represent its own broadcast domain, thus allowing for controlled broadcast traffic.

The IntraCore family of switches is compliant with the IEEE 802.1Q standard governing the structure and implementation of VLANs. Asante switches offer an unprecedented number of VLANs with support for VLAN tagging for enterprise services.

Spanning Tree Protocol (STP)
The spanning tree protocol is defined by the IEEE 802.1D standard. This protocol monitors a network for redundant loops. Loops are detrimental to a network because they consume bandwidth and add overhead. STP uses an algorithm to first create a topology database. From this, STP then looks for loops and shuts down any redundant pathways. Network links are formed through a variety of governing priorities and costs.

Asante's IntraCore switches use the spanning tree protocol to maximize network efficiency. Displayable are the bridge ID, designated root, root port, root port cost, hello time, maximum age, and forward delays. Each port can be further individually configured for STP parameters such as port priority and path costs.

Quality of Service
Quality Service (QoS) is a term that refers to the prioritization of network traffic. Its goal is to provide predictable data transmission through improved and

controlled methods of detecting error rates, availability, bandwidth, and latency. This technology is increasing in popularity due to the concern for the continuous transmission of high-bandwidth video and multimedia information.

The highest level of IEEE 802.1p Priority Queues is supported in the family of IntraCore switches. Asante provides QoS software that maximizes efficiency in packet prioritization. Multiple priority queues ensure that mission critical applications get the bandwidth and priority they need.

Link Aggregation

Link aggregation, or port trunking, is a method of combining physical network links into a single logical link to improve bandwidth. This allows for the creation of redundant links that increase the channels of communication permissible for Fast Ethernet and Gigabit Ethernet technologies. The benefits include that of a higher link availability, increased link capacity, and cost efficiency. Implementation of link aggregation can be done on existing hardware compliant with the IEEE 802.3ad protocol.

All of Asante's IntraCore switches incorporate this important feature of port trunking. Asante IntraCore 3524 offers 2 trunk groups for 10/100 ports (4 ports for each group) and 1 trunk for 2 Gigabit ports. Load sharing on link aggregation is supported based on destination address.