A

Seminar Report

on

Simple Network Management Protocol

Submitted in partial fulfillment of the requirement for the award of degree
Of Computer Science

SUBMITTED TO: **SUBMITTED BY:**

www.studymafia.org
www.studymafia.org

Preface

I have made this report file on the topic **Simple Network Management Protocol (SNMP),** I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to …………..who assisting me throughout the prepration of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Introduction

The Simple Network Management Protocol (SNMP) is by far, the dominant protocol in network management. A key reason for its widespread acceptance, besides being the chief Internet standard for network management is its relative simplicity. Implementing SNMP management in a networked device is far more straightforward than most other standard or non-standard approaches to network management.

Despite that, SNMP application development has not been as simple as one would like. It has required significant effort to develop management applications to manage the variety of networked devices to be managed.

This situation is now changing for the better, as more SNMP tools are available. There are also different versions of SNMP available, such as SNMP V1, SNMP V2c, and SNMP V3. With improved tools, SNMP is poised to deliver end-to-end management for all areas of the growing internet industry.

What is SNMP?

Simple Network Management Protocol (SNMP) is an application–layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices. It is a part of Transmission Control Protocol Internet Protocol (TCP⁄IP) protocol suite.

SNMP is one of the widely accepted protocols to manage and monitor network elements. Most of the professional–grade network elements come with bundled SNMP agent. These agents have to be enabled and configured to communicate with the network management system (NMS).

SNMP Management

SNMP management has become the dominant standardized network management scheme in use today. The SNMP set of standards provide a framework for the definition of management information along with a protocol for the exchange of that information. The SNMP model assumes the existence of managers and agents.

A manager is a software module responsible for managing a part or the entire configuration on behalf of the network management applications and users. An agent is a software module in a managed device responsible for maintaining local management information and delivering that information to a manager via SNMP. A management information exchange can be initiated by the manager (via polling) or by the agent (via a trap).

Agents function as collection devices that gather and send data about the managed resource in response to a request from the manager. UDP ports 161 and 162 are the default ports reserved for SNMP. The agent listens for requests and replies to them over port 161 and reports asynchronous traps on port 162, unless it is instructed to use different ports. SNMP accommodates resources that do not implement the SNMP software by means of proxies. A proxy is an SNMP agent that maintains information on behalf of one or more non-SNMP devices.

How does SNMP work?

The simple network management protocol (SNMP) use for monitoring of network-attached devices for any conditions that warrant administrative attention. For example all of the following devices can use SNMP for managing devices on IP networks:

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.

Administrator can find or manage network performance, solve problem 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.

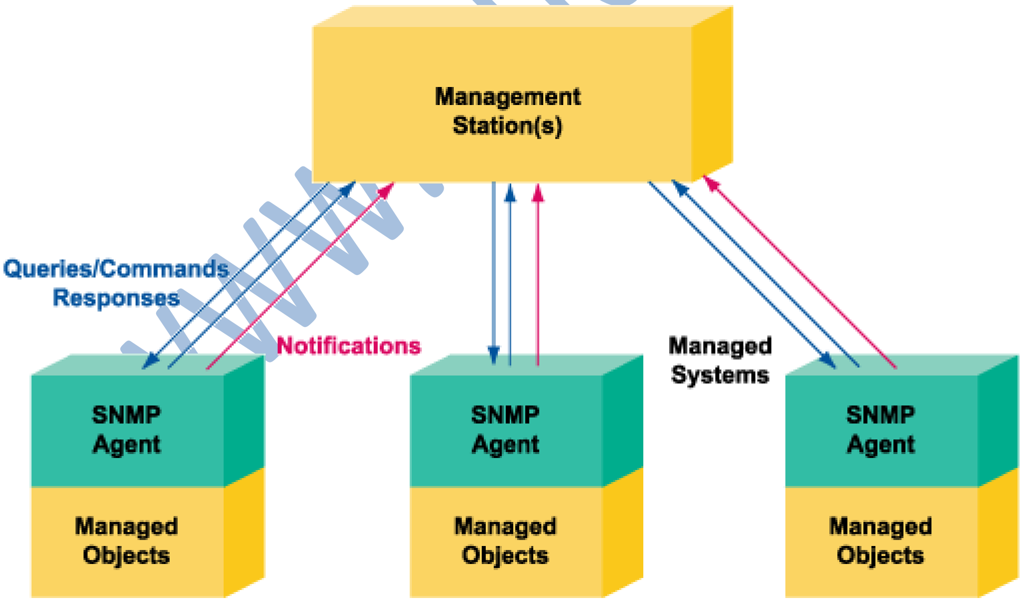
- Acts as a proxy for some non–SNMP manageable network node.

SNMP Architecture

To perform its monitoring services, SNMP uses a distributed architecture of management systems and agents and several related components. Windows Server 2003 provides an SNMP agent that is designed to be capable of interacting with any SNMP manager. The following components are the building blocks of SNMP and the Windows Server 2003 SNMP agent:

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

The internal architecture of the Windows Server 2003 implementation of SNMP is divided into management and agent functions, which, in some cases, overlap. The following figure illustrates how the Windows Server 2003 SNMP structure fits into the layers of the underlying TCP/IP protocol architecture.



Basic commands of SNMP

The simplicity in information exchange has made the SNMP as widely accepted protocol. The main reason being concise set of commands, here are they listed below:

- **GET:** The GET operation is a request sent by the manager to the managed device. It is performed to retrieve one or more values from the managed device.
- **GET NEXT:** This operation is similar to the GET. The significant difference is that the GET NEXT operation retrieves the value of the next OID in the MIB tree.
- **GET BULK:** The GETBULK operation is used to retrieve voluminous data from large MIB table.
- **SET:** This operation is used by the managers to modify or assign the value of the Managed device.
- **TRAPS:** Unlike the above commands which are initiated from the SNMP Manager, TRAPS are initiated by the Agents. It is a signal to the SNMP Manager by the Agent on the occurrence of an event.
- **INFORM:** This command is similar to the TRAP initiated by the Agent, additionally INFORM includes confirmation from the SNMP manager on receiving the message.
- **RESPONSE:** It is the command used to carry back the value(s) or signal of actions directed by the SNMP Manager.

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.

SNMP SECURITY

- Lacks authentication. Vulnerable to the variety of security threats.
- Vulnerable to masquerading, modification of information, time modifications, message sequencing and disclosures.
- Message sequence and timing modifications occurs when an entity who is unauthorized reorders, delays, or copies and later replays a message generated by an authorized entity.
- As SNMP does not implement any authentication Set operations are not implemented by many vendors.

Languages of SNMP

- **Structure of Management Information (SMI)**
  Specifies the format used for defining managed objects that are accessed via the SNMP protocol
- **Abstract Syntax Notation One (ASN.1)**
  Used to define the format of SNMP messages and managed objects (MIB modules) using an unambiguous data description format
- **Basic Encoding Rules (BER)**
  Used to encode the SNMP messages into a format suitable for transmission across a network

CONCLUSION

By implementing the SNMP technology, Ingenico has again demonstrated its desire to provide customers with the best-suited and most cost-effective solutions available. This widespread, light protocol is easy to deploy, and allows Ingenico terminals to be integrated into an existing SNMP environment if needed.