1995

Simple network management protocol

Latha Sundaresan

Simple Network Management Protocol

RIT Master's Project
December 4, 1995

Author: Latha Sundaresan
Latha_Sundaresan@wb.xerox.com

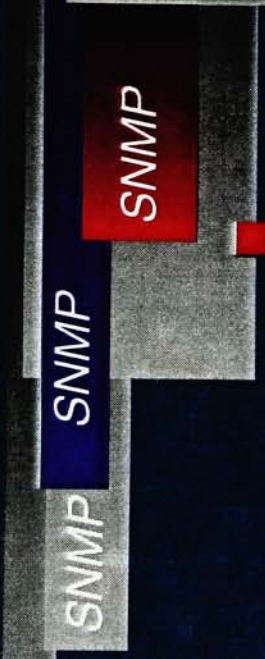
Advisor: Mr. Timothy Wells, RIT
Reader: Mr. Angelo Caruso, Xerox Corporation

Simple Network Management Protocol

SNMP SNMP SNMP

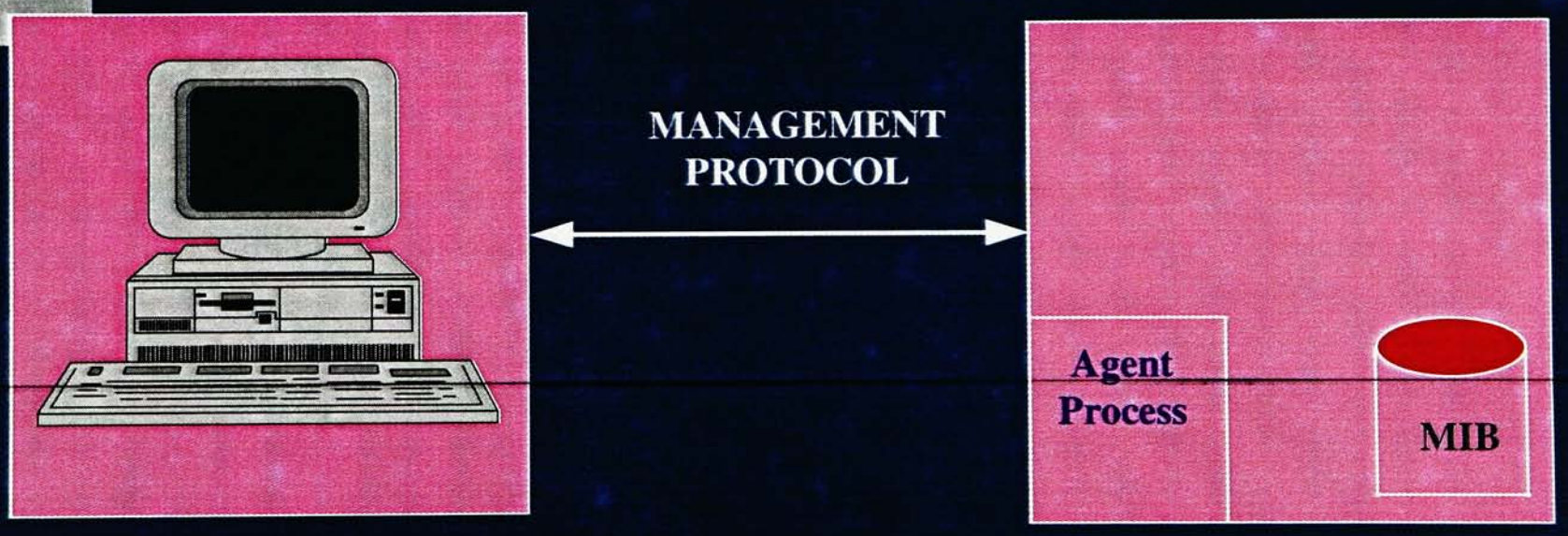
- Introduction
- Overview of Network Management Architecture
- Introduction to Simple Network Management Protocol
- Example of Practical Usage of SNMP
- Conclusion

Network Management Architecture



- Management Station
  - Main Interface for the human network manager into the system
  - Interface for Monitor and Control
- Management Agent
  - Responds to requests from Management Station
  - Could be a Workstation, Printer or a Bridge

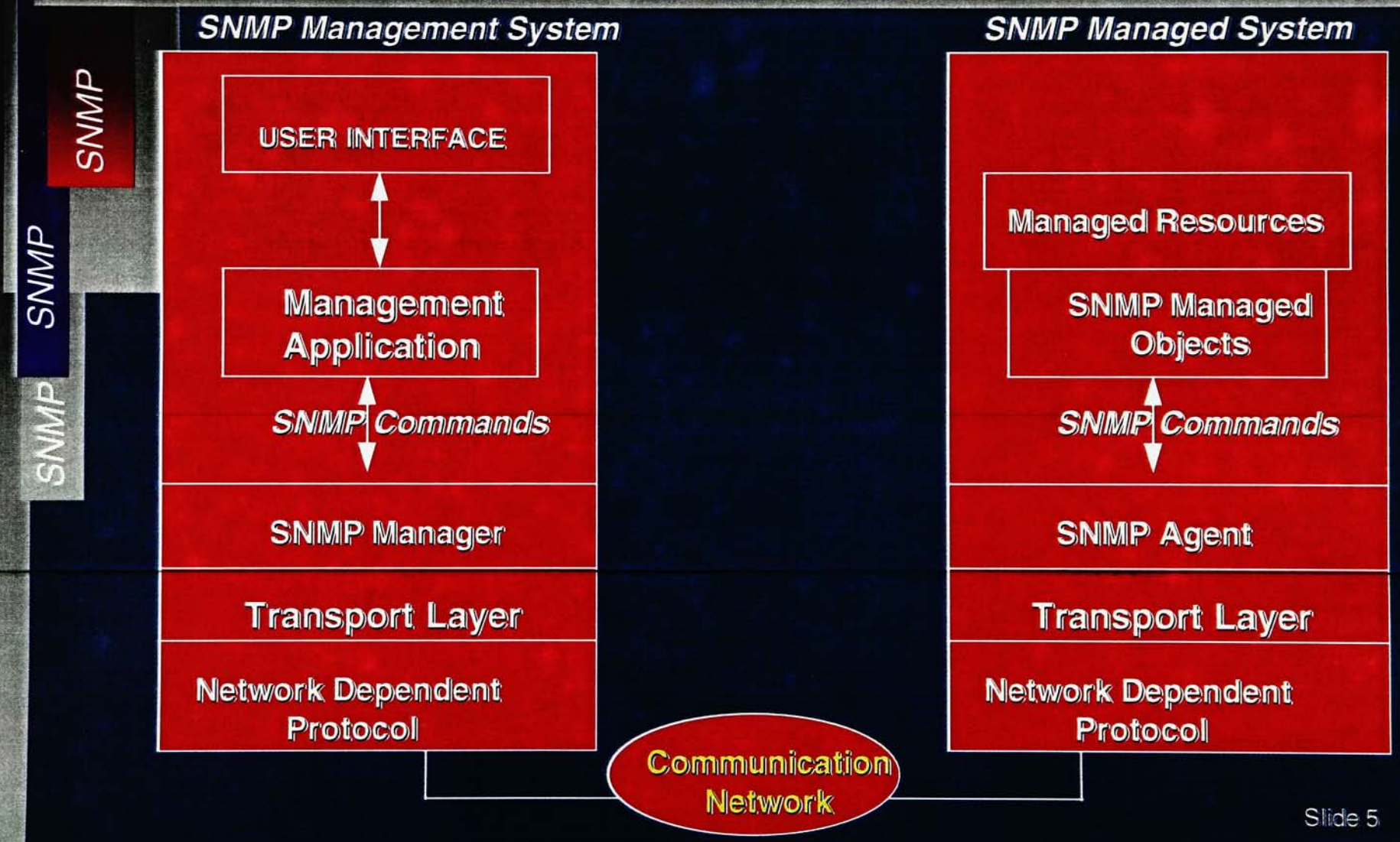
Network Management Architecture



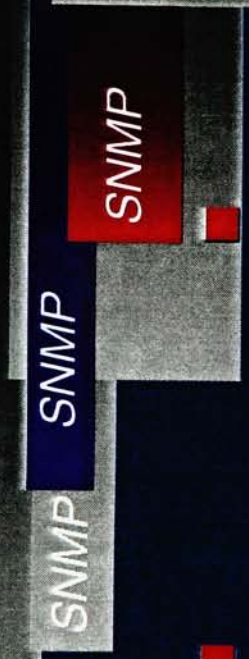
Network Management Architecture

- Management Information Base (MIB)
  - Database of Managed Objects
  - Management Station performs monitoring by retrieving the value of MIB objects
- Network Management Protocol
  - Management Station and Agents are linked by network management protocol

SNMP Architecture



SNMP Architecture



- Managers
  - Atleast one network node acts as a manager
  - Managers can read or change variables in MIB of a remotely managed device
- Agents
  - Respond to queries from a manager
  - Maintain a local MIB

Objects and Object Identifiers

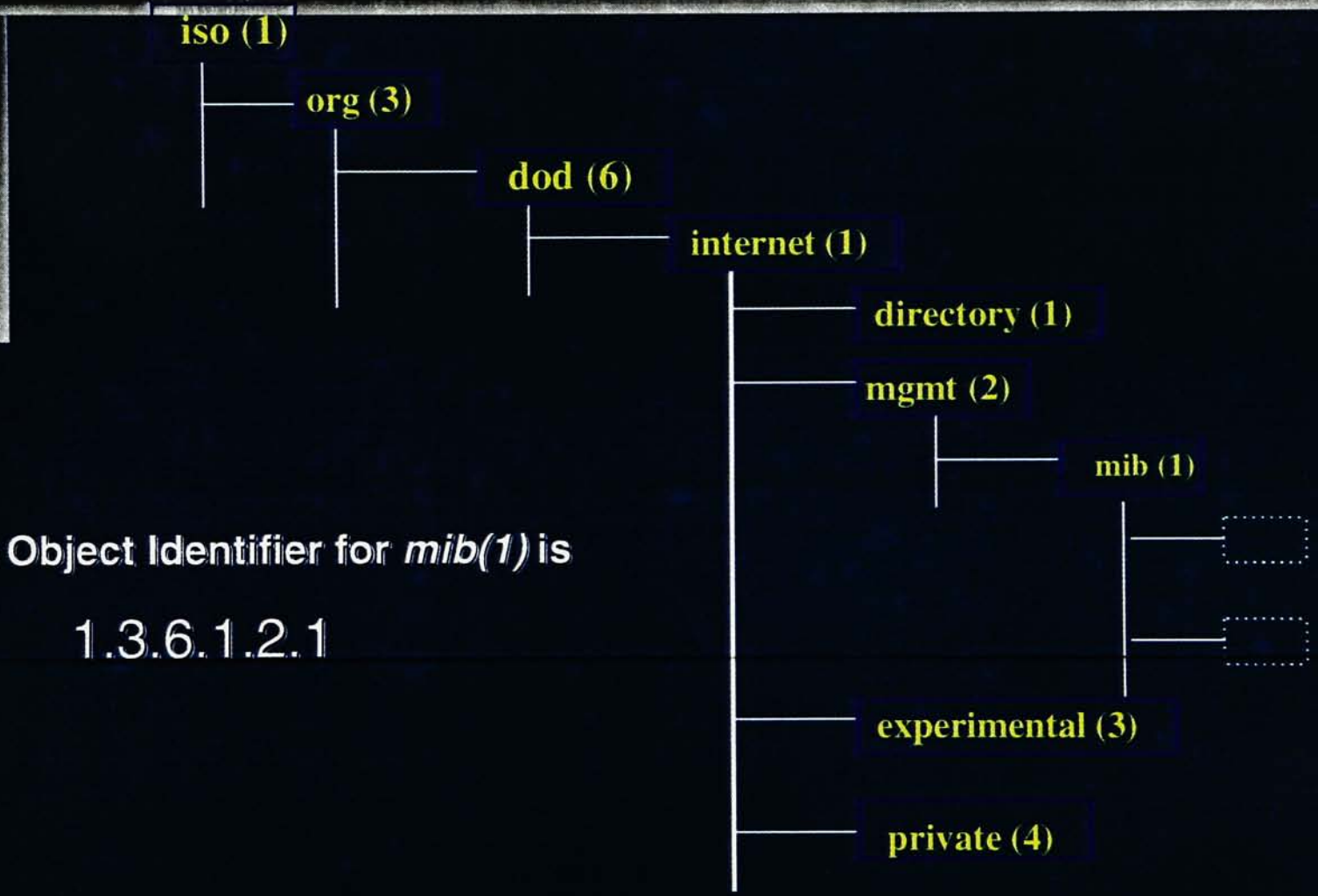
SNMP

SNMP

SNMP

- Object
  - Represents resource to be managed
  - MIB contains collection of such objects
- Object Identifier
  - Associated with each type of object in a MIB
  - Consists of a sequence of integers called subidentifiers
  - Sequence read from left to right defines location of the object in the MIB tree

Object Identifier Tree



SNMP

SNMP

SNMP

The Object Identifier for *mib(1)* is

1.3.6.1.2.1

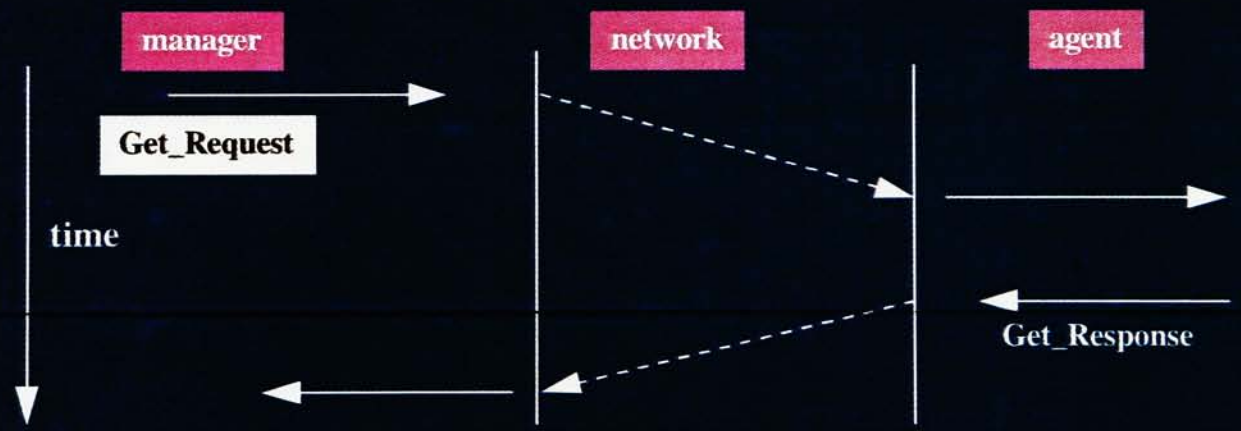
SNMP protocol Messages

SNMP

SNMP

SNMP

- Get_Request Message
  - Manager retrieves management information from the agent



SNMP Protocol Messages

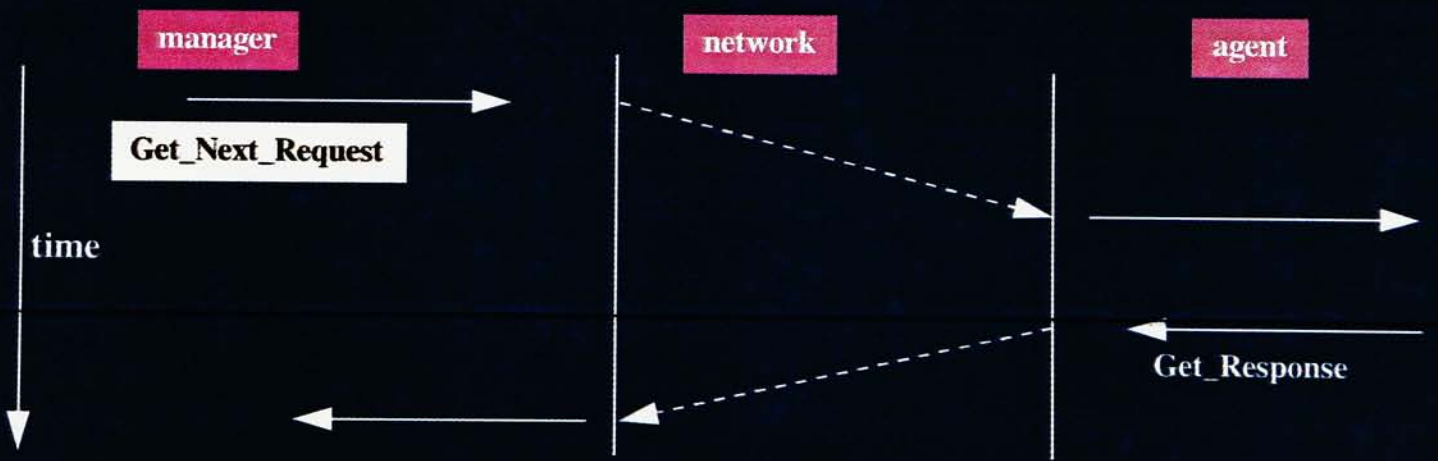
SNMP

SNMP

SNMP

Get_Next_Request

- Returns the value of the next variable instance in the MIB tree rather than the one specified in the request



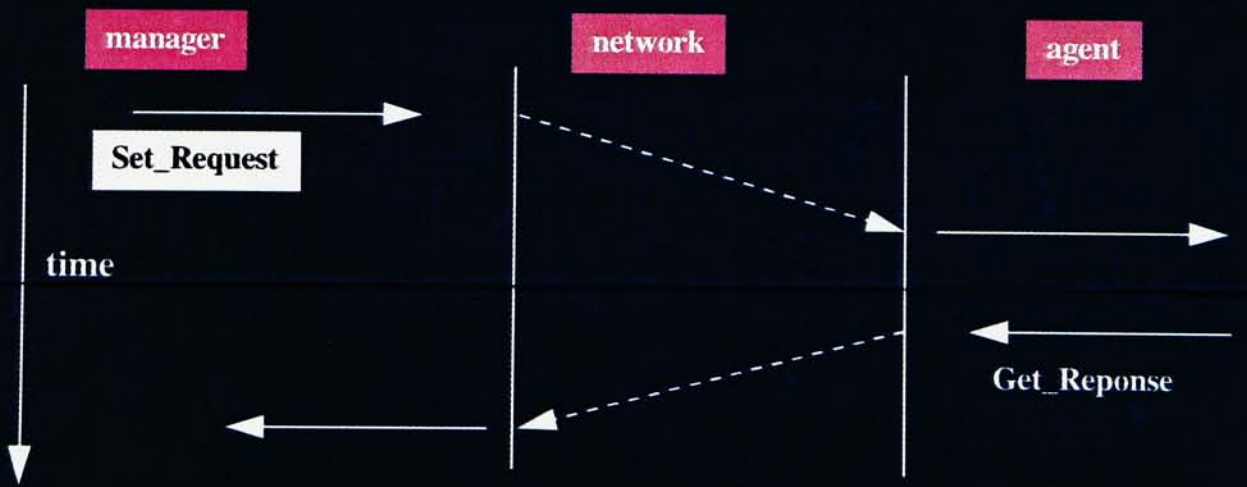
SNMP Protocol Messages

SNMP

SNMP

SNMP

- Set_Request
  - Manager stores management information with the agent



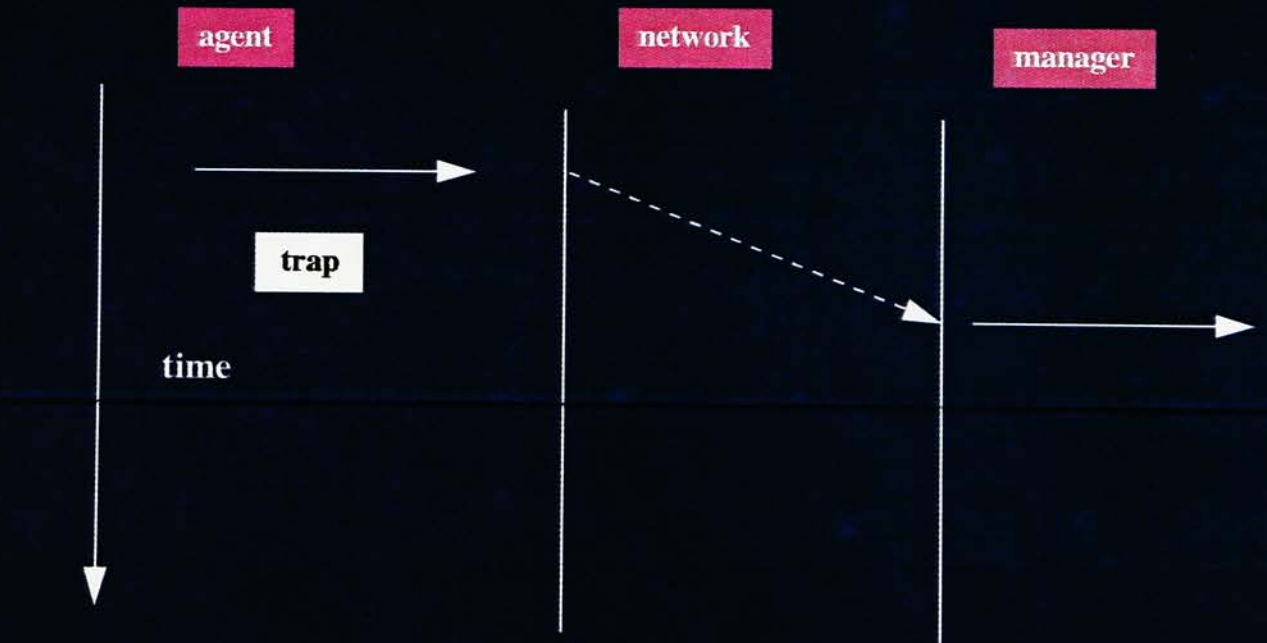
SNMP Protocol Messages

SNMP

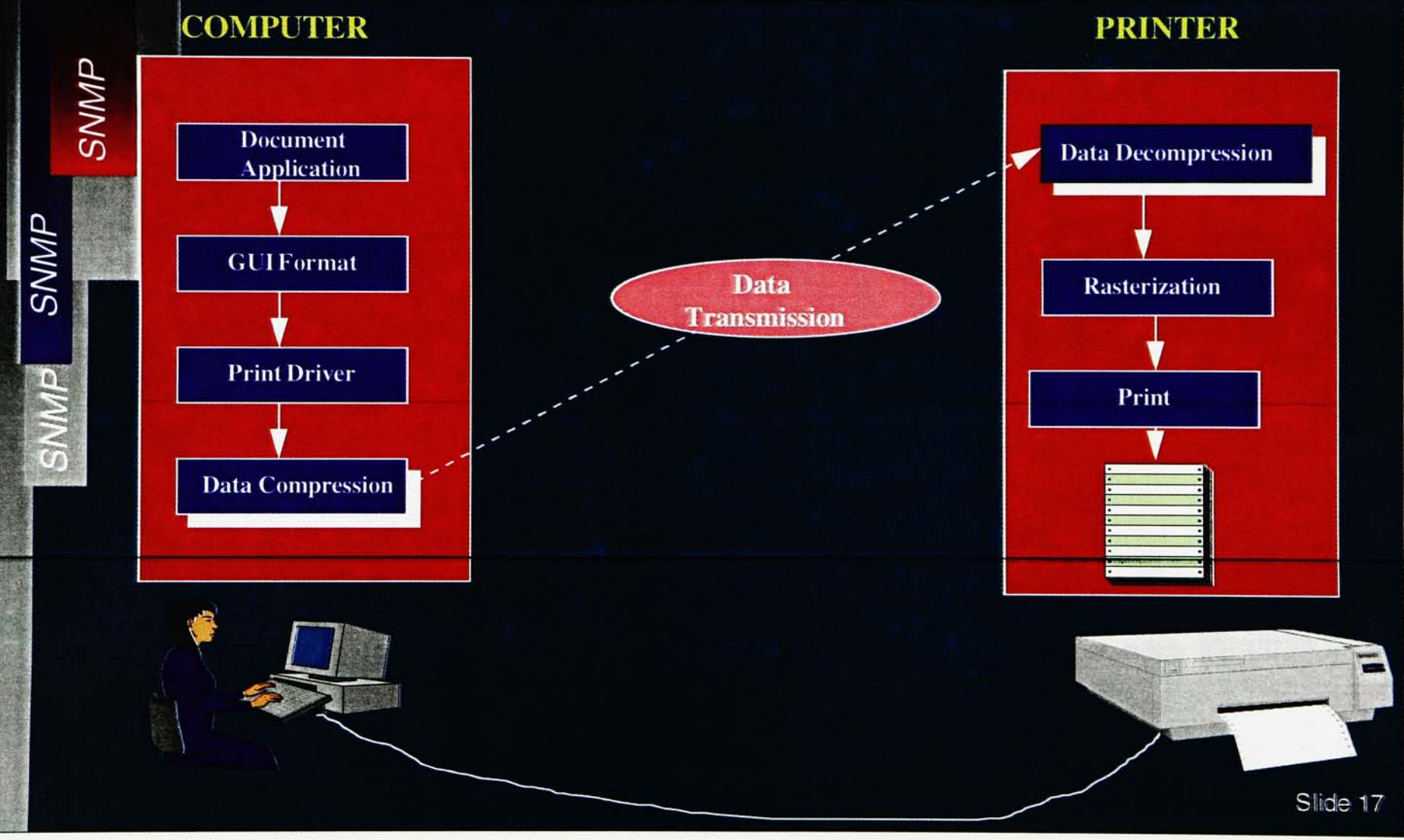
SNMP

SNMP

- Trap
  - Agent reports an extraordinary event



General Printing Architecture



Practical Usage of SNMP

SNMP
SNMP
SNMP

- XPrint 4900 Series
  - Color Laser Printers
  - Black and White and Color Printing
  - Hitachi 600-dpi CMYK
  - Powered by 25MHZ 29030 microprocessor
  - Adobe PostScript Level-2

Practical Usage of SNMP

SNMP SNMP SNMP

- 4900 Model
  - First Generation Model
  - Hitachi 600-dpi modified
- 4920 Model
  - Explained in next slide
- 4925 Model
  - Identical to 4920
  - Prints collated copies of jobs

Practical Usage of SNMP

SNMP
SNMP
SNMP

- 4920 Model
  - Prints 12 pages/min B/W, 3 pages/min full color
  - Has 16 MB memory
  - Can be connected to PC's, Mac's and SUN OS
  - Multiple workstations can be connected to 4920 simultaneously
  - Allows manual control of printer functions by using control panel

Printer Management Mechanism

- 4900 Management Mechanism
  - Uses postscript parameter for printer management
  - If printer is busy, printer services has to wait for unknown time
- 4920 Management Mechanism
  - Uses SNMP to communicate
  - Gets a response even if the printer is busy printing jobs

SNMP Mechanism for Xprint 4920 (Manager)

SNMP
SNMP
SNMP

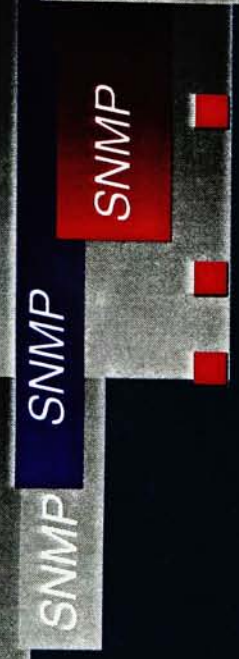
- User asks for information via the Printer Services application
- Printer Services application
  - Builds the list of all objects which are required
  - Provides community name for authentication
  - Passes these to the SNMP manager with a request to get the object values
- SNMP manager constructs the PDU and transmits it over the network

SNMP Mechanism for 4920 (Agent)

- Agent is a piece of software that is on the receiving end

- In our implementation of the agent we have 4 functions associated with every object in the MIB
  - Get: Returns the value of the object
  - Set: Sets the value of the object
  - Test: Tests to see if it is okay to set an object
  - Next: Returns value of next object in the MIB

SNMP Mechanism for 4920 (Agent)



- Agent software does an authentication check on the input message
- If authentication fails the message is discarded
- If authentication check succeeds then
  - Agent extracts the OID's of the objects
  - Agent executes the required function associated with the object to get the values
  - It constructs a response PDU and sends it across the network to the manager

Conclusion

SNMP

SNMP

SNMP

- *Future of SNMP is very rosy*
- *Expansion beyond TCP/IP is in progress*
- *Will continue to be successful*

R·I·T

Rochester Institute of Technology

Wallace Library
Post Office Box 9887
Rochester, New York 14623-0887
716-475-2562 Fax 716-475-6490

SAMPLE statements to reproduce an RIT thesis:

→ **PERMISSION GRANTED**
Title of thesis _____

I _____ hereby **grant permission** to the Wallace Memorial Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction will not be for commercial use or profit.

Date: _____ **Signature of Author:** _____

→ **PERMISSION FROM AUTHOR REQUIRED**
Title of thesis SIMPLE NETWORK MANAGEMENT PROTOCOL

I LATHA V SUNDARESAN **prefer to be contacted** each time a request for reproduction is made. I can be reached at the following address:

164 COUNTRY MANOR WAY,
APT #2
WEBSTER, NY 14580

PHONE: 716-265-4802

Date: Dec 4, 1995 **Signature of Author:** _____

→ **PERMISSION DENIED**
Title of thesis _____

I _____ hereby **deny** permission to the Wallace Memorial Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part.

Date: _____ **Signature of Author:** _____

Rochester Institute of Technology
Computer Science Department

Simple Network Management Protocol

by Latha Sundaresan

A thesis, submitted to
The Faculty of the Science Department
in partial fulfillment of the requirements for the degree of
Master of Science in Computer Science.

Approved by: _____

Timothy D. Wells
with committee members
Fereydoun Kazamian
Walter Wolf

December 4, 1995

Table Of Contents

LIST OF FIGURES

1 INTRODUCTION

Computer networking is expanding in leaps and bounds. What started as a research project has become a valuable resource to the research, academic and other communities. There are immense problems involved when we try to interconnect and communicate among different machines such as computers, switches, and private branch exchanges (PBXs). The difficulty of managing these resources is becoming increasingly complex as networks add more components, more functions and more users. In recognition of this fact, the International Standards Organization (ISO) has been working on the development of several Open Systems Interconnection (OSI) network management standards for a number of years. A large number of vendors like AT&T, DEC and British Telecom have all made major contributions to the OSI standards discussed in this book.

Another major thrust into network management standards has been through the Internet activities. In the last few years Internet Activities Board (IAB) has assumed the lead in setting standards for internet and has come up with 2 network management standards. One protocol is intended to address short term solutions and is called Simple Network Management Protocol (SNMP) and the other addresses long term solutions and is called Common Management Information Services and Protocol over TCP/IP.

The focus of this paper is to look at Simple Network Management Protocol in detail to a certain extent and also to briefly discuss how it is used in a typical work environment Section 2 discusses Network Management in general. Section 3 is about Simple Network Management Protocol and Section 4 talks about how SNMP is used in a practical work environment and Section 5 concludes the paper.

2 NETWORK MANAGEMENT

This section discusses about general principles of network management, network standards and network architecture.

2.1 Why do we need Network Management

Networks are gaining importance and have become very critical in the business world. As networks grow in number the network and its associated resources become indispensable to the organization. If the network is disabled or a part of the network is down then the performance comes to an unacceptable level. If the network is large it cannot be put together and managed by human effort alone. To solve these problems, automated network management tools are to be used. Standardized tools are needed that can be used across a broad spectrum of product types - including end systems, bridges, routers and telecommunications equipment and can also be used in a mixed-vendor environment.

Very large corporations invest lot of money in network management. The network resources have to be monitored and controlled, to enable essential user needs to be satisfied at a reasonable cost. Successful network management, in large part, is a question of paying attention to the following three basic issues:

1. *Monitoring* network performance is essential. When a failure occurs before any plan of action can be made, managers need information about the network's status and how it is performing. This information is most valuable when it is in the form of real-time statistics and event logs.
2. *Controlling* the network means having the ability to change individual device variables, such as routing addresses and protocol filters. Usually, these decisions are based on data collected while monitoring performance or at the time the devices are configured.
3. *Administering* involves collecting information that outlines the network's history. Proper administration often leads to better planning and control. By combining these three ingredients, managers can build and manage reliable networks that better support their client's mission.

Unfortunately, all the above mentioned functions are not built into the average multi-vendor network. Further, they become feasible only when a universally supported

network management protocol exists for the exchange of information among all the critical network components. One such protocol is the Simple Network Management Protocol.

There are two network standards available now, the first one is Simple Network Management Family: The SNMP refers to a set of standards for network management, including a protocol, a database -structure specification, and a set of data objects. SNMP is adopted as a standard for TCP/IP (Transmission-control protocol/internet protocol) since 1989 and has been very popular since then. The second standard is the OSI Systems Management. This standard is large and complex and defines a set of general-purpose network-management applications, a management service and protocol, a database-structure and a set of data objects. The OSI view of network management subdivides the functionality of network management system into 5 components. They are as given below:

1. Configuration Management: This is responsible for detecting and controlling the state of the network for both logical and physical configurations.
2. Performance Management : This is responsible for evaluating the behavior of managed objects and the effectiveness of communications activities.
3. Fault Management : This functionality is responsible for the detection, isolation and correction of abnormal operation of the network.
4. Accounting Management : This facility is responsible for collecting and processing data related to resource consumption in the network.
5. Security Management : Responsible for controlling access to network resources through the use of authentication techniques and authorization process.

2.2 Why do we need Network Management Standards

In this section the paper discusses the need to have network management standards. The reasoning is illustrated with two figures. The Figure 1 illustrates the principal problem that occurs when management standards are not used. The hexagon in the

middle of the figure represents a network and its network management center, this center has the task of developing five different interfaces for the five vendors. The cost to develop and maintain these interface systems can be extraordinary, often resulting in complex software and unpredictable performance. In Figure 2 shows a standardized network management approach.

The network management standards allow a network control center to use one set of software to interact with the vendor's network management packages . This approach forces these vendors to place the standardized software in their own machines. These standards not only ease the task of interfacing different computers, terminals, multiplexers, etc., but they also give the network users more flexibility in equipment and software selection. The acceptance and use of a standard often leads to lower costs because a widely accepted standard can be mass-produced and perhaps implemented in very large scale intergrated (VLSI) chips. This approach frees a company's personnel to use this resource as a platform to design and implement value-added services for customers.

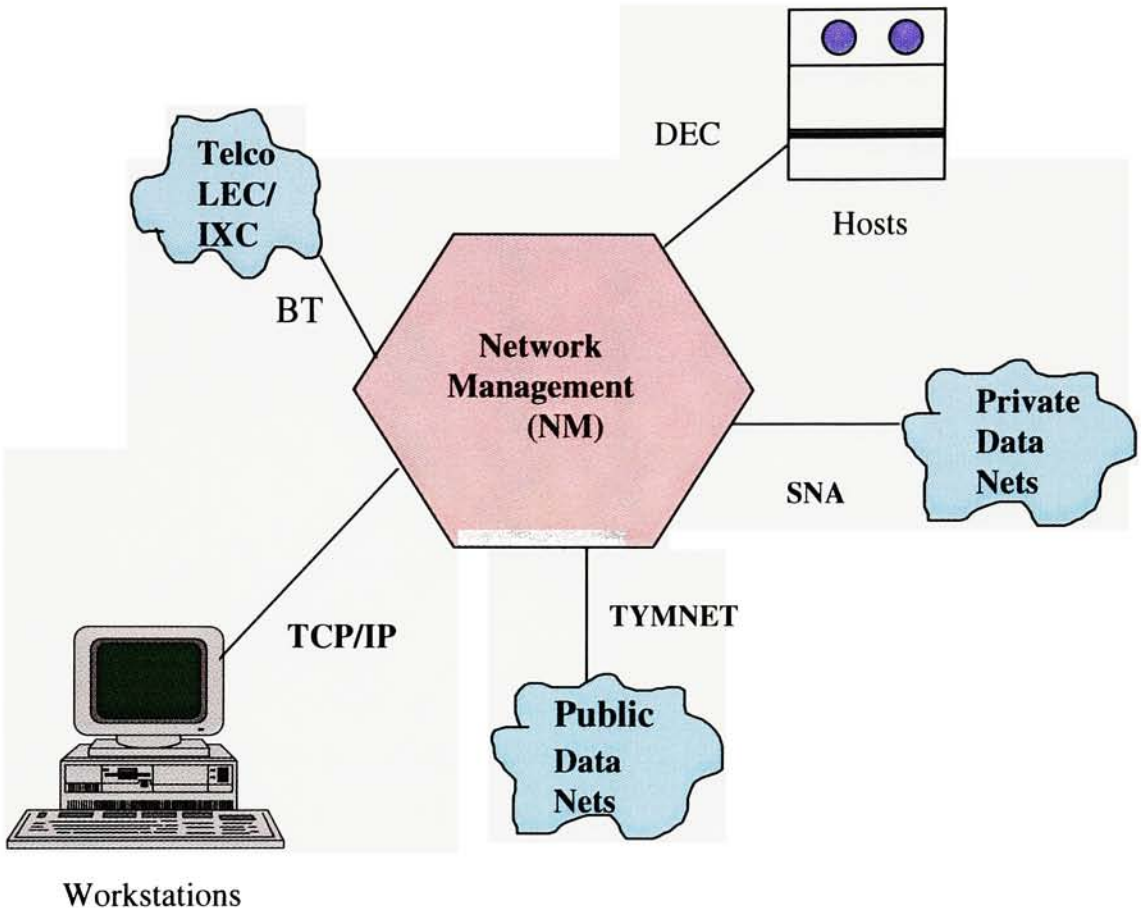


Figure 1: Network Management Scheme [14]

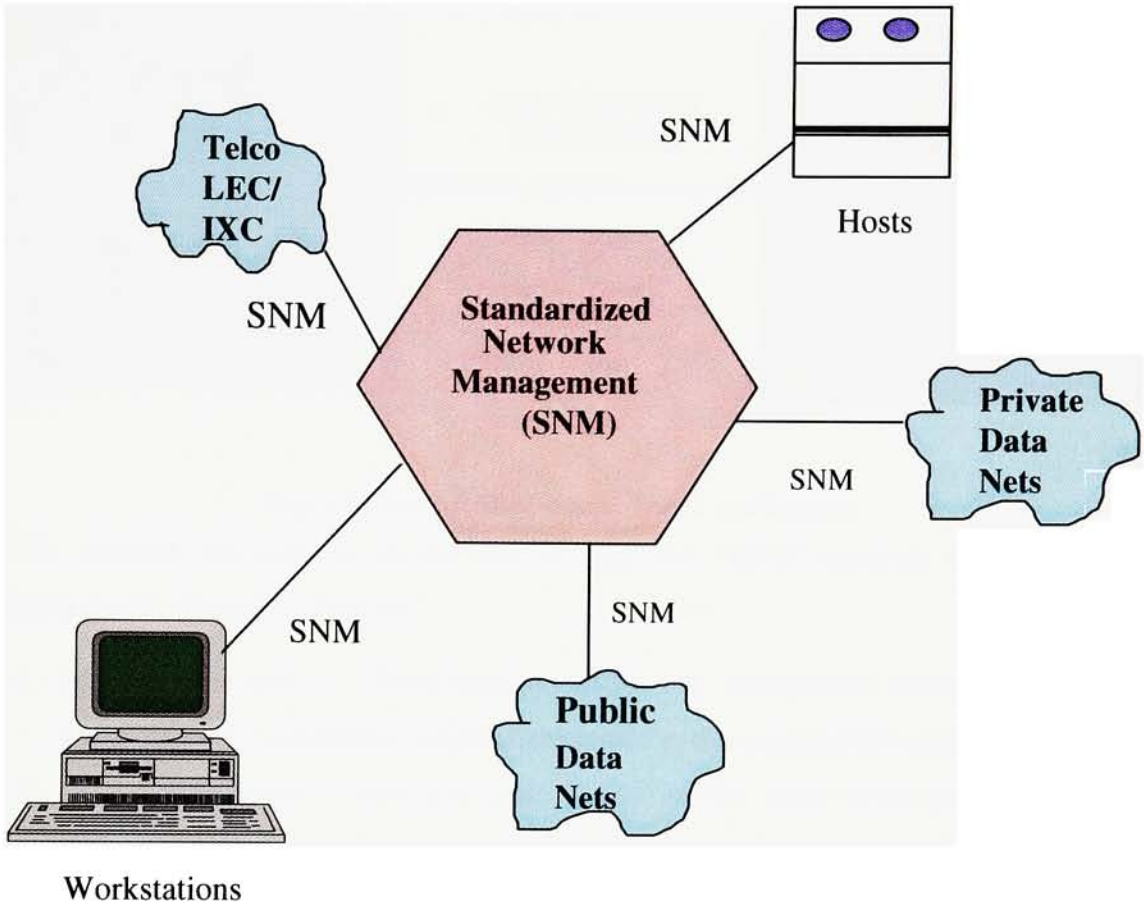


Figure 2: Standard Network Management Scheme[14]

2.3 Architecture of Network Management System

The concepts and architecture of the network management is clearly defined by the Figure 3. As seen from the figure the resources that are supervised and controlled by network management are called managed objects. The agent process stands between the managed objects and the network control system (or managing process). The Management Functional Domain (MFD) can be considered to be like a Network Control System. Detailed explanation of the all the components of a general network management system is given after the figure.

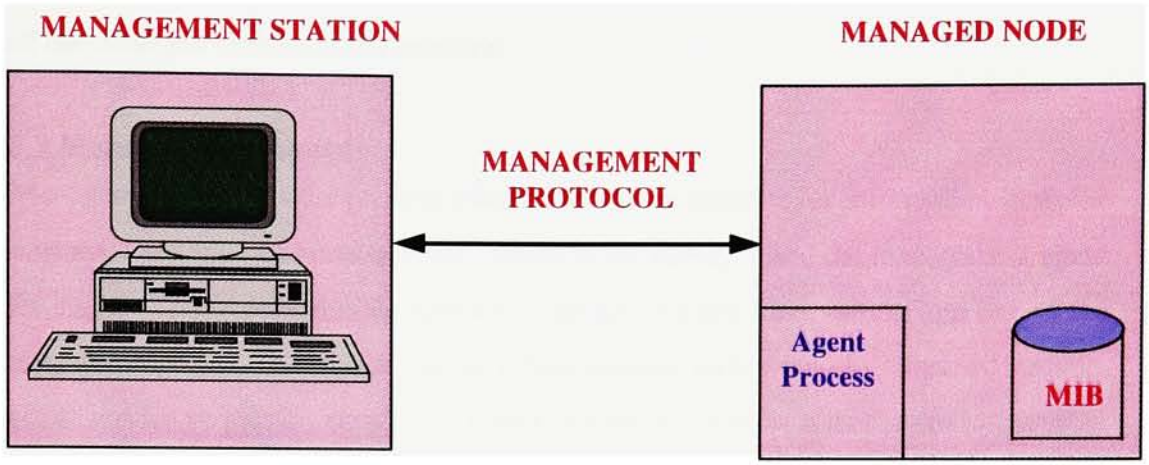


Figure 3: Network Management System Architecture

The network management model that is used for TCP/IP network management includes 4 main elements. They are :

1. *Management station* : There must be atleast one management station. One or more network management applications reside in the management station.
2. *Management agent or managed nodes*: These are the server which processes the requests sent in by the management station.
3. *Management Information Base* (MIB) : The MIB is a data structure that contains a collection of related managed objects.
4. *Network Management Protocol* : This protocol is used by the management station and the agents to exchange management information.

2.3.1. Management Station

The management station is the main interface for the human network manager into the network management system. The management station has a set of management applications for data analysis, fault recovery and so on. This also includes an interface by which the network manager may monitor and control the network. It has two other important features. The first one is the translation of network manager requests into actual monitoring and control of the remote elements in the network. The second feature

is that the station should also contain a database of information extracted from the MIBs of all the managed entities in the network.

2.3.2 Management Agent

Management Agent is the process which responds to requests for information from the management station. The management system is *the manager* and the management agent is *the agent.* The Managed node refers to a device of some kind, falling into one of the following categories: The device can be a host system, such as workstation, mainframe, terminal service or printer, could be a router system or could be a media device, such as bridge, repeater, hub or analyzer. All these devices have some sort of network capability.

2.3.3 Management Information Base

The unit of management information is called a managed object. A collection of related managed objects is called the Management Information Base (MIB). The MIB is a database that represents all the elements to be managed. Each resource to be managed is represented by one or more objects and MIB is a structured collection of such objects. Each managed node in the system, (the server) has an MIB that contains the status of the managed resources at that node. The management station performs the monitoring function by retrieving the value of MIB objects. A management station can cause an action to take place at an agent or can change an agent's configuration settings by modifying the value of specific variables.

2.3.4 Network Management Protocol

The management station and agents are linked by a network-management protocol. The protocol used for the management of TCP/IP networks is the simple network-management protocol, which includes the key capabilities which include Get, Set and Trap.

2.4 Enterprise Network Management Environment

Network management is frequently viewed as only a technical problem. The ultimate responsibility for management resides with people, not machines. Many people within an enterprise are often involved with network management, which includes users, managers

and the actual network administrator. Thus the integrated management environment within which network management resides is a combination of human, social, organizational and technological resources.

2.4.1 Enterprise Network Management Goals and Requirements

An important goal of network management is to support an integrated approach to the management of a network (or networks) which contains multivendor computers, software packages and carriers. Discussion of how this goal can be met is in the next paragraph.

In today's enterprise environment, the "network" to be managed is typically a combination of many interfacility and intrafacility networks. The network is a complex entity, which encompasses a wide mix of communications resources and services. The enterprise networks cannot use a single protocol suite because many networks have subnets that use different protocol suites to support wide range of services for an entire enterprise. The following lists the general capabilities required for managing enterprise networks : 1) The ability to manage all the subnetworks in the network regardless of the protocol suite used. 2) The ability to manage a combination of interfacility and intrafacility (local) networks. 3) The ability to manage a wide range of network resources from low-level devices (e.g. repeaters, modems) to intermediate systems (e.g. bridges, routers, gateways) to end systems (e.g. systems with full protocol stacks). 4) The ability to provide a set of basic management functions. The above mentioned requirements describe the technical capabilities needed for managing communications resources. However technical capabilities are not the only solution in an enterprise environment. Human elements cannot be ignored in the network management. Information on the network may need to be reported to managers, network administrators must have considerable expertise to manage complex networks. Unfortunately such expertise is difficult and expensive to acquire. Thus automated network tools become necessary so that they share some burden and the skills needed for management can be reduced. Thus necessitates additional requirements such as :

- The network management tools must generate reports that are easily understandable.
- The network management tools must be easy to learn and easy to use, so that less human skill is needed.

- The network management tools should decrease the network administrator's work load, providing a single set of tools for all networks to be managed. The tools should have functions, displays, and vocabulary that should be consistent regardless of the network to being managed.
- The tools should manifest the expertise of a skilled network administrator so that less skill is required of the human staff for jobs that are monotonous and frequent.

One of the approaches that can be used to meet the requirements of the enterprise network management is what is called *'Integrated Network Management'*.

2.4.2 Integrated Network Management

This provides a single set of tools for managing all of the network resources within a network. Given below in figure 4 is the architecture for the Integrated Network Management.

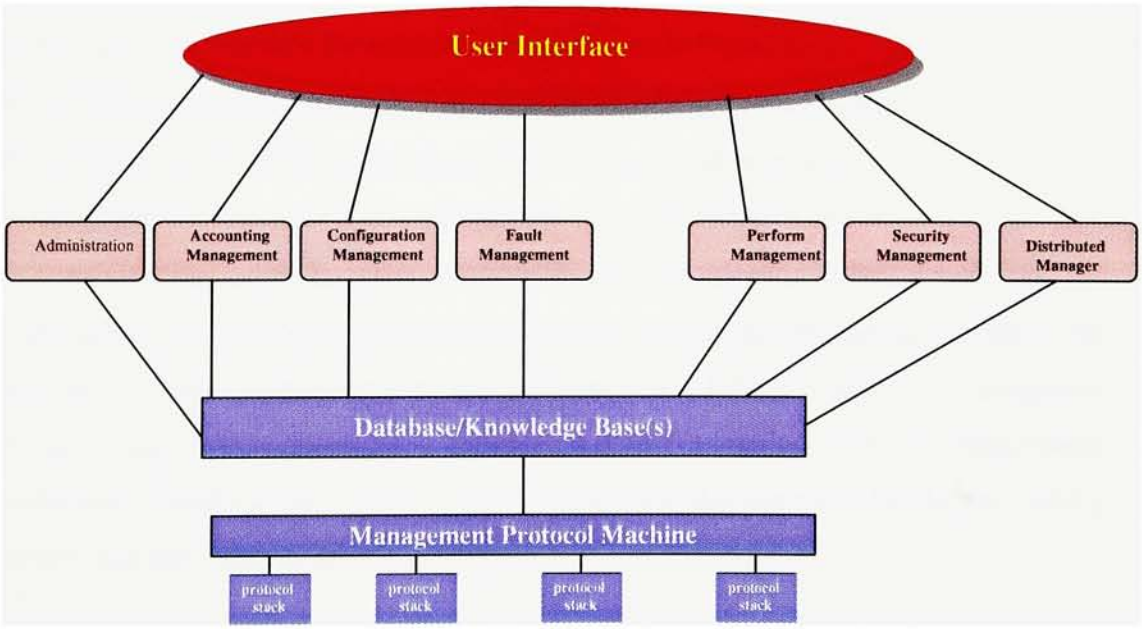


Figure 4: Architecture of Integrated Network Management[8]

The architecture's main components are the user interface, network management applications, a database, a management protocol machine, and one or more protocol stacks. The user interface includes human-computer interfaces, and graphical display of

topology and statistical outputs. Network management applications include administrative, configuration management, fault management, performance management, security management and accounting management functions. A database management system provides central storage of the management information needed for the profiles and protocol suites used. The system must provide an efficient data management mechanism, possibly based on distributed database concepts. One or more knowledge base is also required if expert system capabilities are used. The management protocol includes the management protocol used in the protocol suites, plus mechanisms for management data acquisition. This architecture permits great flexibility in the actual structure used to implement network management. The following figure shows possible integrated network management implementations.

Integrated network management can solve many of the management problems experienced in today's enterprise networks. It provides the following features and reduces the expertise needed for network administrators.

- A single user interface for network administrators to learn.
- A solitary management vocabulary for network administrators to learn
- A solitary set of common management functions for all networks.
- Automatic maintenance of the relationship between managed objects.
- Automatic translation between managed objects definitions in different networks.

Currently many computer and communications vendors are beginning to realize the lack of integration in current network management tools. Efforts to achieve an integrated network management architecture is included in AT&T's Unified Network Management Architecture (UNMA), DEC's Enterprise Management Architecture (EMA) and IBM's NetView, and HP's OpenView.

3.0 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Data networks are getting more and more complex everyday. Contemporary data networks contain bridges, routers, gateways, printers, servers, personal computers and

workstations from multiple vendors. As these networks are growing in size so are the demands on the network management. The network managers are looking for automated tools which they can use to manage various devices on the network. This tremendous growth in data networks and growing demands for the interoperable network management tools has created a very strong need for a standard network management protocol. Currently there are two competing standards in the industry, simple network management protocol (SNMP), based on the popular TCP/IP protocol suite and Common Management Information Protocol (CMIP), based on OSI's systems management framework. SNMP refers to a collection of specifications for network management that includes the protocol itself, the definition of a database, and associated concepts.

The protocol used for the management of TCP/IP networks is the simple network management protocol, which includes the following key capabilities:

Get : Enables the management station to retrieve the value of objects at the agent.

Set : Enables the management station to set the value of objects at the agent.

Trap : Enables an agent to notify the management station of significant events.

Let us look more in detail about SNMP in the following section.

3.1 Background of SNMP

Simple network management protocol (SNMP) is based on the TCP/IP suite of protocols. TCP/IP was developed in the early 1970's when U.S department of defense (DoD) funded Advanced Research Project Agency (ARPA) to develop one of the first packet switching network, ARPANET. At the time of TCP/IP development not much thought was given to the network management. As the popularity of TCP/IP increased and ARPANET evolved into Internet, a collection of LANs and WANs with ARPANET as the core, the need for a network management became apparent very quickly.

To meet this growing requirement of network management, various efforts were started to develop TCP/IP based network management protocol. SNMP evolved from the simple gateway monitoring protocol (SGMP) which was a part of the original TCP/IP suite. Internet activity board reviewed the initial proposals and approved the

development of SNMP in the early 1988. Finally, the RFCs for SNMP standard (1155, 1157 & 1213) were submitted in the 1990 - 1991 time frame. The growing success of the SNMP protocol led to increasing demands for changes. One major set of changes included extensions to strengthen management capabilities, beyond monitoring. The language was generalized beyond gateways to include end systems and other network elements. Some more changes were made to ease the transition to OSI-style network management. These changes included the definition and adoption of an OSI-style Structure of Management Information (SMI) and Management Information Base (MIB). Biggest criticism against the early SNMP was the lack of built in security features. This was addressed in SNMP version2 or SNMPv2. A set of documents which define SNMPv2 have recently been submitted as proposed standard by the Internet Engineering Task Force (IETF). Even though, these standards are not final yet, no major changes are expected.

3.2 SNMP Architecture

SNMP is an application layer protocol which runs on top of User Datagram Protocol (UDP/IP). The SNMP commands are encoded according to basic encoding rules (BER) associated with ISO Abstract Syntax Notation one (ASN.1) and are sent over services provided by UDP/IP. Refer to Figure 5 below for the architecture block diagram.

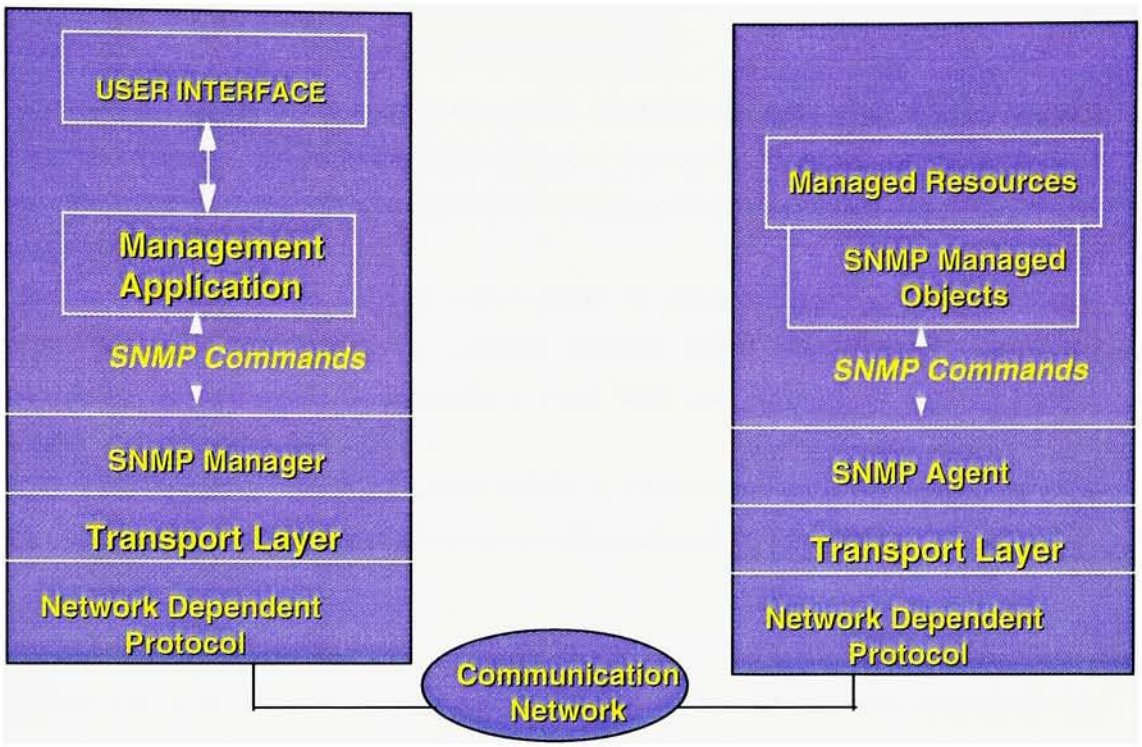


Figure 5: SNMP Architecture[6]

As detailed earlier about the components of network management systems, SNMP has 3 main elements. They are Managers, Agents and MIB.

Managers: In any configuration there is at least one network node which acts as a management station. There can be more than one managers. Manager can either read or change the value of variables contained in the management information base of a remote managed device.

Agents: Devices on the network which are to be managed, such as bridges, routers, printers, gateways, etc., contain a software module called SNMP agent. It is the responsibility of this agent to maintain a local MIB and respond to queries from a manager.

MIB: Management information base (MIB) is a local data base maintained by each agent. MIB contains objects which represent information to be managed.

3.3 SNMP Design Process

SNMP was built via the correct design process. First, SNMP was shaped by the collaborative effort of university researchers, users and managers of networks, and communications vendors. The principle designers of SNMP were involved in the management and research of internets. The short time in which the SNMP was designed, implemented, and deployed was possible because of this shared focus. Secondly, design ideas were gathered from parallel efforts of other researchers. The SGMP principles were used to refine many design ideas. Finally, all design proposals were prototyped and tested by the implementation experiences of multiple independent implementations. The SNMP design is based on three principles:

3.3.1 Designed For Predominance

In the present times network management demands the use of a single management scheme, including a single management protocol to facilitate end-to-end management. This means that management system must be implemented on a wide range of platforms. SNMP-based network management has been implemented on a wide range of platforms, from PC's to supercomputers.

3.3.2 Engineered Economy

Economy was given the most consideration when SNMP was designed. Memory and Computational requirements were placed on the Network Operations Centers rather than on the management agents. There were two reasons to do this. Firstly, there were many more agents than NOCs. Secondly, this design allows the network elements to focus their resources on their principal functions rather than on network management overhead.

3.3.3 Planned Extensibility

SNMP design included many extensibility hooks for network management. The most important is the mechanism for extending the management information base. This process allows the generation of new versions of the Internet standard MIB. New versions may declare old objects out-of-date, add to the definition of existing objects, or define entirely new objects. Mechanisms for vendor or enterprise specific extensions to the MIB are also defined.

3.4 SNMP Applications

SNMP provides two types of applications, Network Operations Center and Agent applications.

3.4.1 Network Operations Center (NOC) Applications

A Network Operations Center (NOC), is where the management stations reside. The following features are associated with NOC

- There can be many managed elements per NOC station.
- There can be one or many NOC stations for a given managed element.

Many SNMP based tools for controlling and monitoring the network are available. Some of these tools use the powerful X-Windows system on modern workstations. Some execute on entry level MSDOS systems. Several of these applications are quite mature, having been ported from the SGMP environment. These applications address either one

or more than one of the five OSI functional management facilities such as fault management, performance management, configuration management, accounting management and security management.

3.4.2 Agent Applications :

The SNMP is used on many types of platforms. The platforms include hosts, workstations, terminal servers, and network connected printers. SNMP is also used to communicate network management information among physical layer devices such as fiber optic hubs, and other devices such as bridges, gateways and routers.

3.5 SNMP: Merits and Demerits

SNMP is the most desirable protocol today because of its many advantages. But SNMP also has its share of undesirable features. In this section we look at both the advantages and disadvantages of SNMP[9].

3.5.1 Extensibility

SNMP has provisions for extending the MIB by the individual vendors. Vendors that make networking hardware can obtain their own "enterprise " designation under the private branch of the ISO name space. Since there is a well defined syntax for defining MIBs, console vendors can convert the standard notation of the MIB definition into a form usable by their particular network management console software. This makes SNMP an easily extended environment.

3.5.2 Simplicity

What makes SNMP simple are the limited data types supported and the limited set of operations that can be performed on that data. Data can be structured only in two-dimensional tables. This makes fetching tables simple since only one set of rows and columns exists in each table. SNMP is a protocol in which the operations are very simple. There are only 4 operations viz., get, get-next, set, and trap. Because of the simplicity of the protocol, developing application programs becomes easy. SNMP does not require large computations or memory resources from the machines that

accommodate it. This issue is very important in case of bridges and routers because these devices normally have just enough memory to handle their own workloads.

3.5.3 Peer-to-Peer topology

SNMP is configured as a peer to peer topology. Hence the flow of data is not hierarchical in SNMP. In a hierarchical topology, systems cannot speak until spoken to by higher order elements in the network. In SNMP the manager talks to the agent directly and vice versa and therefore the response to error conditions is quicker. Thus SNMP systems are robust.

3.5.4 Centralized Management

A typical SNMP topology has a single management station with several managed nodes. This architecture gives a convenient observation point for the network administrator. He can issue commands conveniently from this central station to alter the behavior of the network.

3.5.5 Minimal Resources

Since SNMP protocol does not need any specialized hardware, SNMP applications need minimal resources. SNMP manager and the server run like any other application program using the underlying physical connections and protocols.

3.5.6 Interoperability

The SNMP improves the interoperability among the products from different vendors. This means that the manager software and each of the agent softwares can be from different vendors. Eventhough the manager and the agent can be from different vendors they can communicate as long as the protocol (SNMP) is obeyed. Thus vendors have the freedom to supply their own management software for their network devices.

3.5.7 Extensive MIB variables

MIB variables support a large variety of network devices and operations. For example, if the network administrator finds that a particular route causes longer delays, he can issue commands to change the routing table entries and the route accordingly.

SNMP still being the most sought after protocol has its disadvantages too. The disadvantages of SNMP are listed below[5]:

- The first and foremost drawback of SNMP is the lack of security. At present, SNMP authentication facilities are only superficial. Community names can be defined for monitoring, setting and trap information. If the proper community name is given, requests to set values are honored. In SNMP, No attempt is made to encrypt community names. Anyone monitoring the network can capture the community names contained in SNMP packets .
- SNMP does not have any application programs or user interfaces in terms of plots, visual displays etc., In SNMP the applications with the associated user interfaces have to be developed separately. On the other hand, CMIS/CMIP offers a library of useful application programs.
- SNMP is unreliable. The protocol uses the underlying UDP protocol for transferring the protocol data units. Hence the SNMP packets themselves may be lost, duplicated, or delayed.
- SNMP does not support complex data structures. OSI supports complex data structures like arrays and complex data transfers like transferring bulk data (routing tables, visual information, etc.). Because of this OSI takes less time to transfer bulk data. Since SNMP supports only simple data structures and transfers, SNMP can be inefficient for transferring bulk data in a short time.
- Each of the SNMP implementations might have proprietary MIBs. In order for a manager to access the proprietary MIB of a different vendor, he should have a knowledge of the other MIB. This might complicate the SNMP implementation and attaining true interoperability might become difficult.
- SNMP traps are unacknowledged. In the typical case where UDP/IP is used to deliver trap messages, the agent cannot be sure that a critical message has reached the management station.
- The basic SNMP standard provides only trivial authentication. Thus, basic SNMP is better suited for monitoring than for control.

- In SNMP the only way to trigger an event at an agent is indirectly, by setting an object value. This is less-flexible and less-powerful scheme than one that would allow some sort of remote procedure call, with parameters, conditions and status and results to be reported.
- The SNMP does not support communications between managers. There is no mechanism that allows a management system to learn about the devices and networks managed by another management system.

Many of these limitations are addressed by the OSI network management. But again OSI network management is very large in size and complex so vendors and customers may still prefer the simple SNMP network management. Improvements to SNMP in the area of security are in progress and it remains to be seen if these improvements will have vendor support of SNMP without having them jump to OSI network management.

3.6 Management Information of SNMP

The SNMP protocol itself is actually one aspect of the total network management structure, and the other two aspects are the Management Information Base (MIB) and the Structure of Management Information (SMI). Section 3.6.1 talks about ASN.1 notation including the syntax, data types and values. Section 3.6.2 talks about Object Identifiers.

The MIB is a database that has the collection of all the attributes that reflect the status of the physical link (Number of packets received, transmission rate, maximum packet size etc.,), the details of routing (destination address, next hop address etc.), the status of the devices or the details of the underlying protocols (TCP, IP etc.). The MIB also has an extensive collection of network variables that are essential for management functions like monitoring, control etc.

The SMI is a standard that defines the general framework within which an MIB can be defined and constructed. This standard dictates the format of the network variables used. The exact data types that have to be used for each variable, their lengths, and their access control modes are defined in SMI. The representation and naming of the MIB resources is also governed by SMI.

3.6.1 Abstract Syntax Notation One (ASN.1)

SNMP uses a language known as Abstract Syntax Notation, One (ASN.1) which defines object information independent of computer architectures and operating systems. Objects within a SNMP MIB and the entire MIB structure are defined using ASN.1. This structure provides a method for uniquely identifying each object (in this case objects are pieces of management information) within a tree structure. A collection of ASN.1 descriptions, relating to a common theme is termed a ***module***. The high-level syntax for the module is simple[12] :

<< module >> DEFINITIONS ::= BEGIN

<< linkage >>

<< declarations>>

END

The <<module>> term names the module, both informally and uniquely. These modules can EXPORT definitions by other modules, which in turn import them. The <<declarations>> term contains the actual ASN.1 definitions. ASN.1 defines three kinds of objects namely *Types, Values and Macros.*

3.6.1.1 TYPES

These define new data structures[11]). The ASN.1 word for *types* start with an uppercase letter (e.g., Gauge). The ASN.1 type has the following syntax **:**

NameOf Type ::= TYPE

The simple ASN.1 types, also called the UNIVERSAL types , are used to define MIB objects. The following are the UNIVERSAL types.

INTEGER:

This is a data type that takes number as its value and the number can also be negative.

OCTETSTRING: :

This data type takes zero or more octets as its value. Each byte in an octet string may take any value from 0 to 255.

OBJECT IDENTIFIER:

This topic is discussed in a more detailed way in section 3.6.2

SEQUENCE:

SEQUENCE data type is similar to a structure in other programming languages.

SEQUENCE OF

This is analogous to dynamic array in many programming languages where the number of elements are not known until the array is created.

Apart from the above mentioned data types SMI defines five or six APPLICATION data types [11]:

NetworkAddress : This data type uses the CHOICE construct to select and address from one of the possibly several protocol families.

```
NetworkAddress : : =
    CHOICE {
        internet
         IpAddress
    }
```

IpAddress : a 32-bit address using the format specified in IP.

```
IpAddress : :=
  [APPLICATION 0]
      IMPLICIT OCTET string (SIZE (4))
```

Counter : This data type represents a non-negative integer, which monotonically increases until it reaches a maximum value, when it wraps back to zero. The maximum value is

```
Counter : : =
  [APPLICATION 1]
      IMPLICIT INTEGER (0..4,294,967,295)
```

Gauge : This is a non-negative integer that may increase or decrease, with a maximum value of 2^{32-1} . If the maximum is reached, the gauge remains latched at that value until reset.

Gauge : : =

[APPLICATION 2]

IMPLICIT INTEGER (0..4294967295)

The maximum value is 2^{32-1}

TimeTicks : a non-negative integer that counts the time in hundredths of a second since some epoch.

TimeTicks : : =

[APPLICATION 3]

IMPLICIT INTEGER (0..4294967295)

Opaque : supports the capability to pass arbitrary data .

Opaque : : =

[APPLICATION 4]

IMPLICIT OCTET STRING (0..4294967295)

3.6.1.2 VALUES

These are instances of a type. The word starts with a lowercase letter (e.g., internet)

3.6.1.3 MACROS

These change the actual grammar of the ASN.1 language. The word consists of uppercase characters. (e.g., OBJECT-TYPE). The formalism used to precisely capture the management definition of a managed object is given below:

OBJECT-TYPE MACRO : : =

BEGIN

TYPE NOTATION : : = "SYNTAX" type (TYPE ObjectSyntax)

"ACCESS" Access

"STATUS" Status

VALUE NOTATION : : = Value (VALUE ObjectName)

Access : : = "read-only"

|"read-write"|"write-only"|"not-accessible"

Status : : = "mandatory"|"optional"|"obsolete"

END

A simple example of managed object described using the above formalism is given below. It describes a managed object called numberOfFontsSupported.

numberOfFontsSupported OBJECT_TYPE

SYNTAX INTEGER

ACCESS read-only

STATUS current

Now let us define the terms used in the description:

SYNTAX : This defines the abstract syntax for the object type. The syntax must be constructed using the UNIVERSAL types and Applicationwide types allowed in the SMI.

ACCESS : This defines the way in which an instance of the object may be accessed, via SNMP or some other protocol. The options are *read-only, read-write, write-only and not-accessible*. The last option says instances of the object may not be accessed via SNMP.

STATUS : This indicates implementation support required for this object. The options are *current, deprecated* and *obsolete*. The *current* indicates that the definition is current. The *deprecated* means that the definition will soon be made obsolete and need no longer be implemented. The *obsolete* indicates managed nodes should not implement this object.

NAME (value):

The value of the object "numberOfFontsSupported" is, according to the macro, of the type ObjectName. The SMI defines this type as :

ObjectName : : =

OBJECT IDENTIFIER

So, managed objects are named by OBJECT IDENTIFIERs

3.6.2 Object Identifier

The Object Identifier is a unique identifier of an object, consisting of a sequence of integers, known as subidentifiers. The sequence, read from left to right, defines the location of the object in the MIB tree structure. The most concise textual format is to list the integer values found by traversing the tree, starting at the root and proceeding to the object in question. The integer values are separated with a dot. Thus **1.0.8571.5.1** identifies the object found by starting at the root, moving to the node with label 1, then moving to the node with label 0 and so on. The node found after traversing this list is the one being identified. Let us explain this in detail with an example as given by the figure.

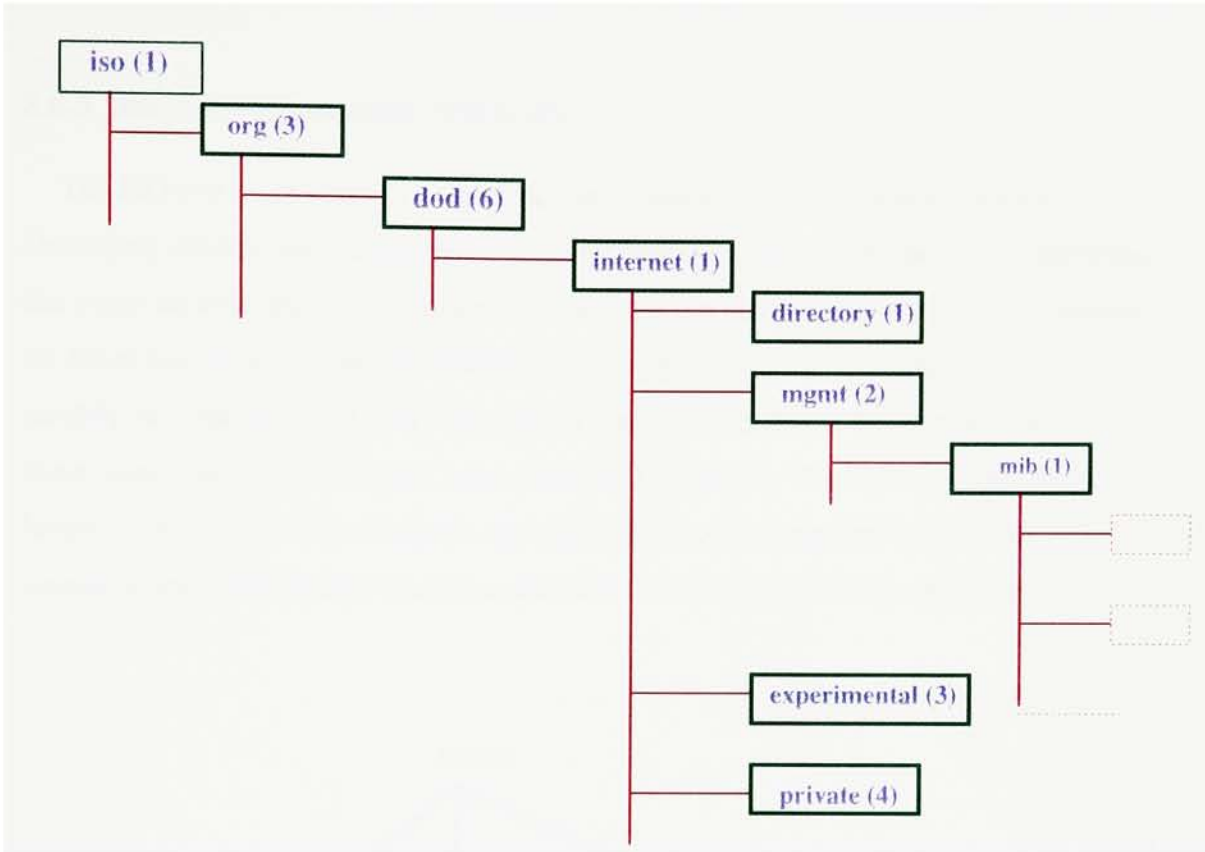


Figure 6: MIBII Object Groups[6]

Looking at Figure 6 the object identifier for the object *MIB* is derived as follows:

iso	**org**	**dod**	**internet**	**mgmt**	**mib**
1	**3**	**6**	**1**	**2**	**1**

Thus the object identifier is **1.3.6.1.2.1.**

As for the internet the prefix used is

internet OBJECT IDENTIFIER :: = {iso org (3) dod (6) 1 }

3.6.3 Internet Registration Hierarchy

The ISO and CCITT have jointly developed a scheme for naming and uniquely identifying objects, such as standards, member bodies, organizations, protocols- anything that needs an unambiguous identifier. The scheme is a hierarchical tree structure wherein the lower leaves on the tree are subordinate to the leaves above. The upper branches identify the authorities as CCITT (0), ISO (1), or an object that is developed jointly by these organizations. The Figure 7 shows the ISO approach. The ISO uses four nodes below the root to identify standards, registration authorities, member-bodies and organizations. This figure 7 is used as the base for internet registration hierarchy.

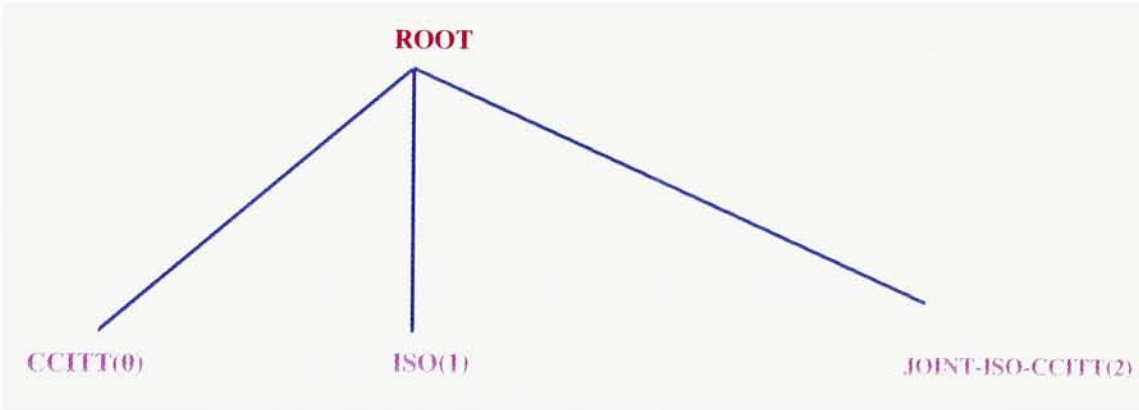


Figure 7: The ISO registration hierarchy

Figure 8 shows the ISO and Internet registration tree for the Internet MIB. At the root level, three branches identify the registration hierarchy as either ccitt(0), iso(1), or joint ccitt/iso. Within internet hierarchy there are 4 nodes. One is labeled management (Mgmt). The next entry of this branch is labeled mib (1). This is the internet MIB.

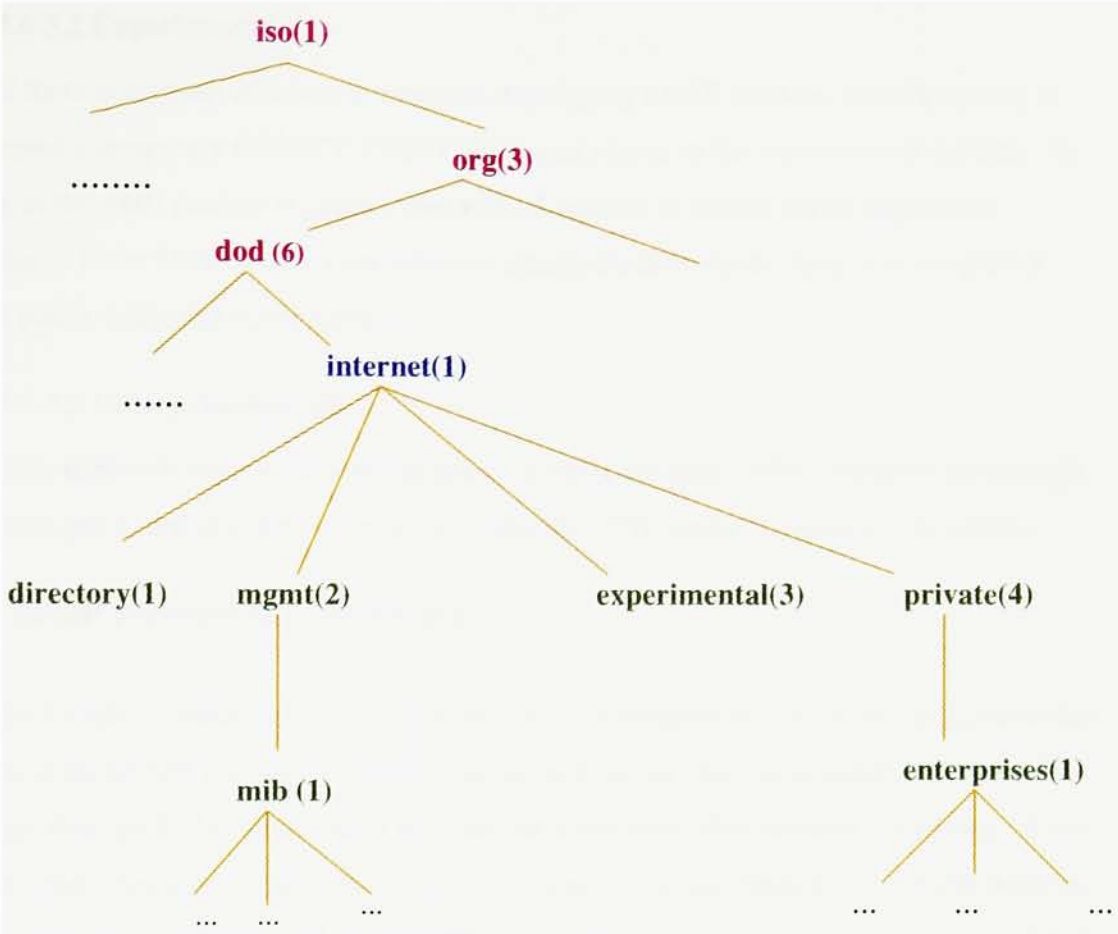


Figure 8: Object Identifier Prefix for Internet[11]

There are three kinds of MIB modules as given below :

3.6.3.1 Standard

These MIB modules are developed by a working group of the Internet Engineering Task Force (IETF) and then declared standard by the Internet Engineering Steering Group (IESG). The prefix for the OBJECT IDENTIFIER assignments for these MIBs is under the *mgmt* subtree. There is a standard MIB for the printer called the RFC 1759 (Request For Comments) in the public domain of the internet.

3.6.3.2 Experimental

If there is a group which is working on developing a MIB module, then that group is assigned a temporary OBJECT IDENTIFIER and placed in the *experimental* subtree. As long as the MIB module is under experimental subtree, it should not be shipped as product. If the MIB module ever achieves standardization status, then, it is assigned a new prefix under the *mgmt* subtree.

3.6.3.3 Enterprise-Specific

This subtree is where vendors can assign a prefix for their MIBs. Vendors are strongly encouraged to develop their own product-specific MIBs under the *enterprises* subtree.

3.7 SNMP Protocol Specifications

In SNMP information is exchanged between a management station and an agent in the form of an SNMP message. SNMP is an asynchronous request/response protocol. This means that an SNMP entity need not wait for a response after sending a message. It can send other messages or do other activities. Each message includes a version number, indicating the version of SNMP, a community name to be used for this exchange, and one of the five types of protocol data units (PDUs). In this section let us look at SNMP Data units and its operations to a certain detail.

3.7.1 Protocol Data Units (PDU) of SNMP

The Figure 9 gives the format of Protocol Data Units used by SNMP.

Let us explain some of the terms used in the figure :

Version:

Refers to SNMP version

Community:

This acts as password to validate the SNMP message.

request-id:

An integer value used by a manager to distinguish among outstanding requests.

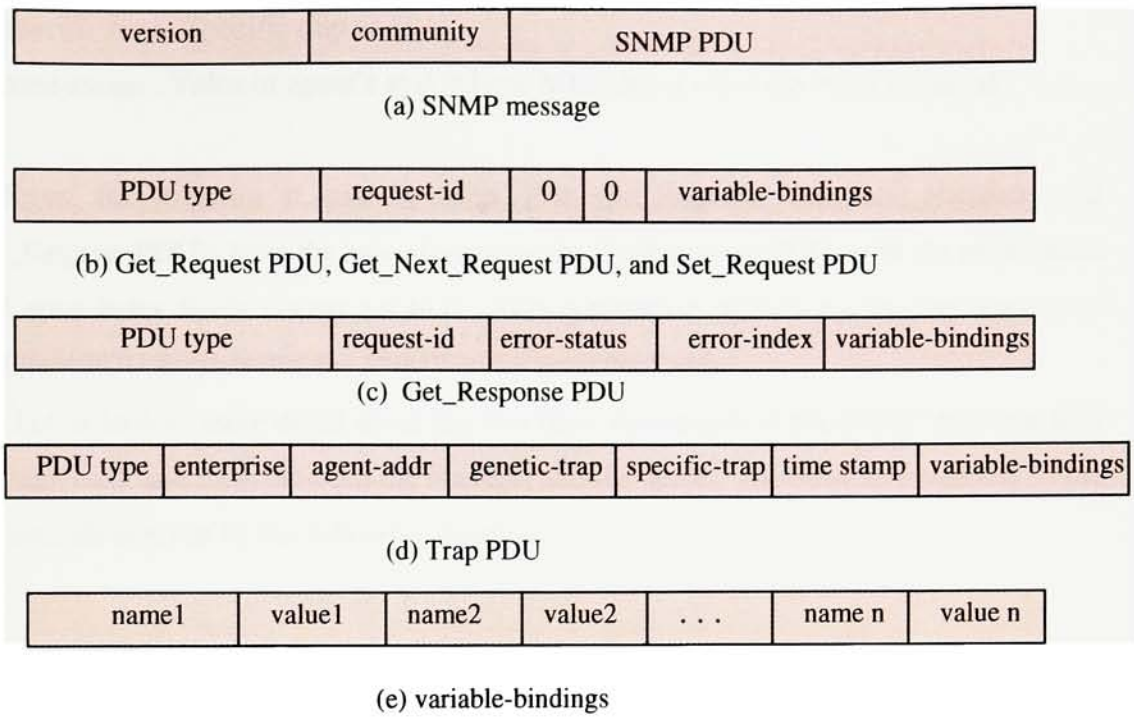


Figure 9: SNMP Formats [6]

error-status:

If non-zero this indicates an exception occurred when processing the request.

error-index:

If non-zero this indicates which variable in the request was in error.

variable-bindings:

A list of variable names and corresponding values. In Get_Request cases values are NULL.

The fields of TRAP-PDU are described :

enterprise: Type of object generating the trap

agent-addr: Address of object generating trap.

generic-trap : Generic trap type

specific trap : Specific trap code.

time-stamp : Value of agent's sysUpTime MIB object when the event occurred

From the diagram it can be seen that Get_Request, Get_Next_Request, and Set_Request PDU's have the same format as the GetResponse PDU, with the error-status and error-index fields always set to 0. This convention reduces by one the number of different PDU formats that the SNMP entity must deal with.

Let us look in more detail about the five basic commands of the SNMP and how they are sent back and forth between the manager and the agent. The basic functionality of the commands is given by the following diagram.

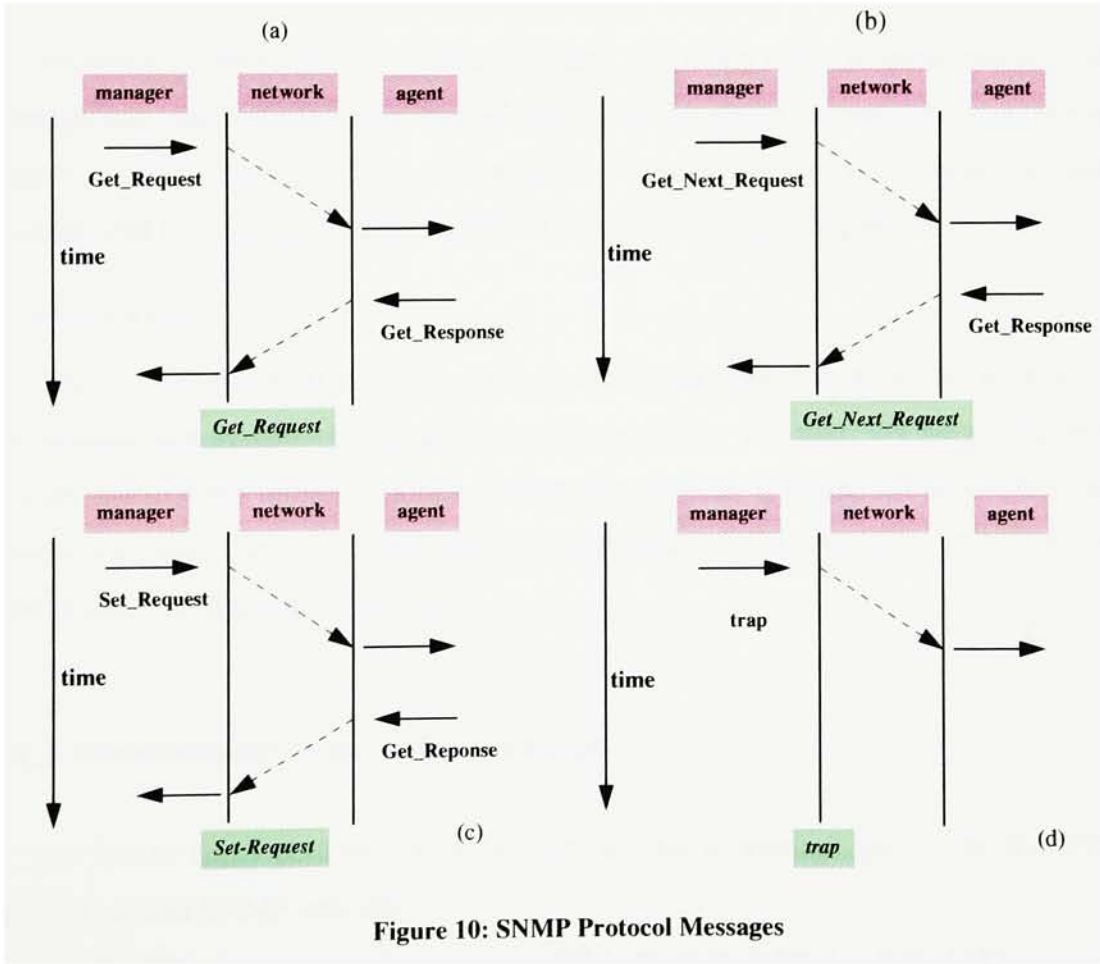


Figure 10: SNMP Protocol Messages

3.7.1.1 Get_Request

In the above figure (a) represents the Get_Request operation. By doing a Get_Request operation on a particular element of the MIB a management system can obtain raw data about the target end-system. The management system can then process the data and present it to the user.

3.7.1.2 Get_Next_Request

The second section (b) portray the Get_Next_Request command. This command returns the value of the next variable instance in the MIB tree rather than the one specified in the request.

3.7.1.3 Set_Request

Section (c) depicts the command set-request. By doing a Set_Request operation the manager can take input from the user and set a variable within the end-system, to re-set a statistics count variable to zero for instance. This is used by the manager to store management information with the agent and to control managed objects.

3.7.1.4 Trap

The last command (d) is a trap. This is used by the server to attract the attention of the management system. For Example to raise an alarm. The user, via the management system, has to make further inquiries, through Get_Request's, to find out about the event. Unlike the GetRequest, GetNextRequest and SetRequest PDUs the Trap PDU does not elicit a response from the other side.

3.7.2 Transmission of an SNMP message

The SNMP entity performs the following actions to transmit one of the five PDU types to another SNMP entity[6]:

1. The PDU is constructed, using the ASN.1 structure defined in RFC 1157.

2. This PDU is then passed to an authentication service, together with the source and destination transport addresses and a community name. The authentication service performs any required transformations for this exchange, such as encryption or the inclusion of an authentication code, and returns the result.
3. The protocol entity then constructs a message, consisting of a version field, the community name and the result from step 2.
4. This new ASN.1 object is then encoded, using the basic encoding rules, and passed to the transport service.

3.7.3 Receipt of an SNMP message

In principle, an SNMP entity performs the following actions upon receipt of an SNMP message:

1.It does a basic syntax check of the message and discards the message if it fails to parse.

2.It verifies the version number and discards the message if there is a mismatch.

3.The protocol entity then passes the user name, the PDU portion of the message and the source and destination transport address to an authentication service.

•If authentication fails, the authentication service signals the SNMP protocol entity, which generates a trap and discards the message.

•If authentication succeeds, the authentication service returns a PDU in the form of an ASN.1 object that conforms to the structure defined in RFC 1157.

4.The protocol entity does a basic syntax check of the PDU and discards the PDU if it fails to parse. Otherwise, using the named community, the appropriate SNMP access policy is selected and the PDU is processed accordingly.

3.8 SNMPv2

SNMPv2 provides a substantial functional enhancement to SNMPv1 and also has many security enchanments. The key areas in which the enchnacements are made to SNMPv1 falls into the following categories :

3.8.1 Strcuture of Management Information (SMI)

In SNMPv2 the macro used to define object types has been expanded to include several new data types and to enchance the documentation associated with an object.

3.8.2 Protocol Operations

SNMPv2 has two new PDU's added to its protocol operations. The *GetBulkRequest* PDU enables the manager to efficiently retrieve large blocks of data. The *InformRequest* PDU enables one manager to send trap type of information to another.

3.8.3 Manager-to-Manager capability

There are two MIBs defined as part of SNMPv2 specification. The SNMPv2 MIB contains basic traffic information about the operation of the SNMPv2 protocol. The SNMPv2 MIB also has information about SNMPv2 manager or agent. The second MIB namely, manager-to-manager MIB is specifically provided to support the distributed management architecture.

3.8.4 Security

SNMPv2 coantains a security capability that is based on that of Secure SNMP.

4.0 PRACTICAL USAGE OF SNMP

Support for network management is gaining momentum in the network printing industry. As the printers are transforming into multi-function network devices, the ability to manage them remotely is becoming a requirement. It is very inconvenient to send a long print job to a network printer, then walk all the way to the remote printer, only to find out that the job was printed with wrong font types. Ability to query the printer, in this case, for supported font types before submitting a print job can save some frustration later. Similarly, a network manager should not have to walk all the way down to the remote network printer to get status. One should be able to get printer status right in their office on a networked workstation or PC. Most network printers, currently use SNMP with a proprietary management information base (MIB). Other printer manufacturers include QMS, Lexmark and Xerox. Lexmark also uses other management protocols like

NPAP(Netowrk Printing Alliance Protocol). Now in this section we shall see to some extent about how printers are used in working environment

4.1 General Printing Architecture

Most users take printing process for granted, they are unaware that there is a large amount of work and many technologies involved in the printing process to put the image from the video display onto a piece of paper. Figure 11 gives an overview of the printer architecture :

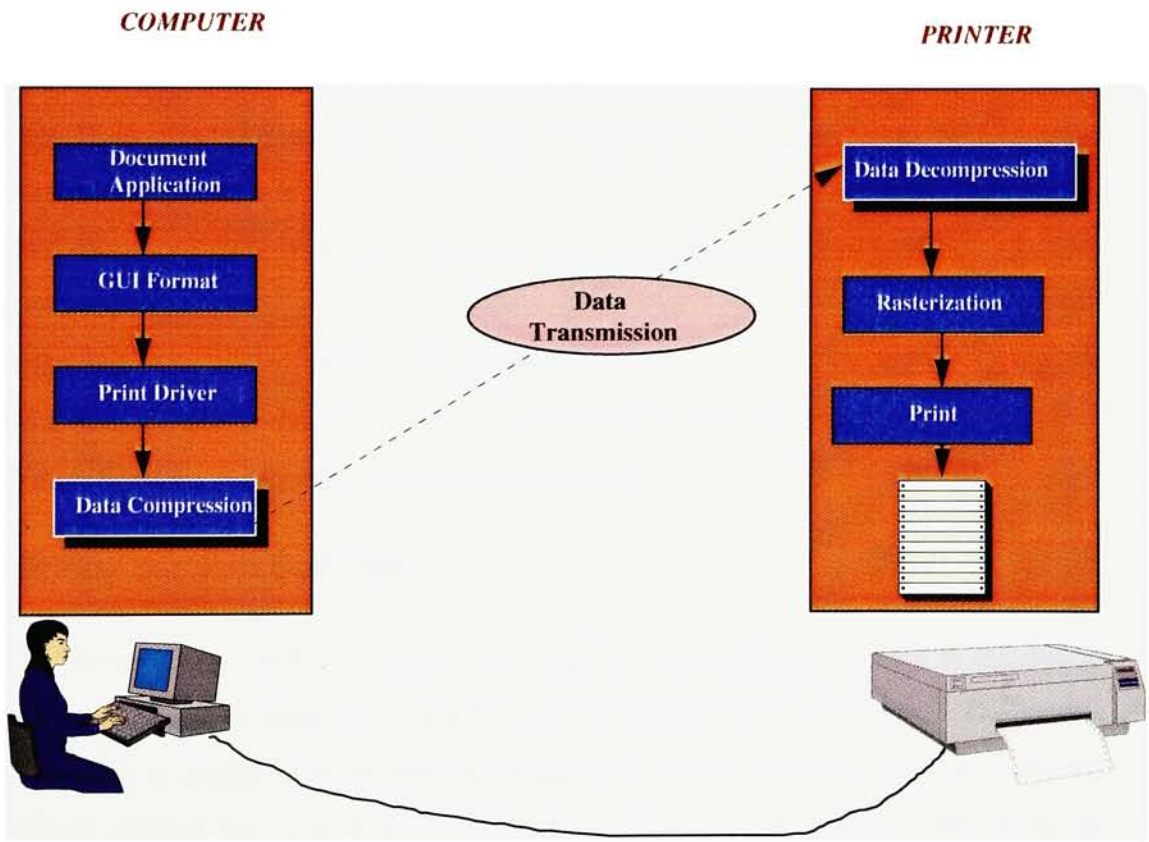


Figure 11: General Printing Architecture

The process of printing a document from a computer application has the following steps :

1. The document is prepared using some application. Examples of this application are Adobe Photoshop, Microsoft Word or Lotus Smart suite.
2. Store the document in the GUI format of that platform. In Windows, this is in GDI metafile format, In MAC this is in Quickdraw format, and on Sun Unix it would be X.
3. Perform the conversion process that translates the GUI format into the appropriate printer's language using the selected printer driver.
4. Data Compression : Reduce the size of the data during transmission between the host and the printer, the print driver has the option to perform compression on the output data file.
5. Data Transmission: Transmit the data that the printer driver generated to the printer via host-printer connection.
6. Data decompression: If the data is compressed, decompression must be done.
7. Rasterization :

- If the data is rasterized, skip to the next step.
- Else, take the data through the printer's interpreter to produce raster data.

8. Print : Send the raster data to the marking engine.

4.2 Printer Services Software

The XPrint Color DS/P (Document Services for Printing) utility, which is referred to as printer services, contains user and the system administrator functions. The printer service utility is available in the Macintosh and also on the Personal Computer. The PC version is divided into two utilities : User Status/Management Services and Setup & Administrative Services. The Windows Setup & Admin Services utility provides full access to the status and configuration of the printer. This allows you to remotely control network options, communications settings, security and maintenance functions from a workstation. The user Status and Management Services application is your main access into the XPrint Color user system information. This application allows you to access and

perform all the necessary features and functions needed to interact fully with the XPrint 4915/4920/4925 as a user. A wide range of functionality is made available through the use of a Menu bar and a Button bar, as well as through standard keyboard command operations. The printer services software can display printer configuration, can attach and detach from file servers, can read maintenance and consumable displays like dry ink, oil bottle etc., displays information about queues to which the default printer is connected, can add and delete jobs from queues.

4.3 XPrint 4900 Printer Series

Xerox corporation has launched a new set of three printers called the XPrint Series. The XPrint 4920 and 4925 are based on a Hitachi 600-dpi CMYK color engine which was modified by Xerox. The other printer XPrint 4915, is an updated version of the company's first-generation model 4900 Color Laser Printer. The 4925 is identical but adds the capability to print multiple, collated copies of a job once the initial print job has been sent to the printer. All of these models are powered by a 25-MHZ AMD 29030 microprocessor and comes with PostScript Level 2 built in.

4.3.1 XPrint 4920

The XPrint 4920 is designed to support both black and white and color printing for small workgroups in a shared environment. The XPrint 4920 provides excellent text quality and superior color quality for graphics and pictorial applications. The 4920 has the following features[15]:

- The 4920 has excellent printing features. The XPrint 4920 will print upto 3 pages per minute minute (ppm) full color. It has a lot of printing options that cover the gamut from simple business graphics to scanned images.
- The 4920 product contains 16 MB of memory sufficient to print almost all images at 600 x 600 dpi in black and white and color.
- As for connectivity the 4920 can be directly connected to personal computers with Microsoft Dos 5.0, 6.0, or Microsoft Windows 3.1, or Apple Macintosh system 6.0,7.0 or 7.1, Windows NT, SUN OS and OS/2.

- A rich array of connectivity features allows multiple workstations and/or printer servers to be connected to the XPrint 4920 simultaneously.
- XPrint 4920 also has two optional Network Interface Cards (NIC). The first one is Ethernet and the second is the Token Ring. Both the cards provide automatic switching to the appropriate protocols. The principle protocols supported are Appletalk, Novell netware and TCP/IP.
- In XPrint 4920 the printer default settings are sufficient to operate your printer in most situations. XPrint 4920 allows a user to manually control printer functions at the printer if necessary by using the control panel.

4.3.2 XPrint 4900 and XPrint 4920 Printer Management Mechanism

Xerox has answered many of the complaints of the 4900 printer with its new 4920 series. The 4920 has improved print quality and better speed than the 4900. The 4900 uses postscript bi-directional printer management mechanism. They use postscript to set variables and also to request variables. SNMP was not a product feature requirement for 4900 whereas it was a requirement for 4920. The 4900 had a configuration in which all the printer variables were stored in the Postscript Language. But there was a major drawback of using postscript as bi-directional communication mechanism. There is only one Post-Script interpreter on a printer. When someone is sending a job to the printer, the printer services software cannot communicate to the printer as print job is using the Post-Script Interpreter. Printer Services has to keep checking until the print job is done and has to wait for a unknown time. If the printer is idle, then it is fine but the printer is busy then the printer service has to wait for an undetermined time.

In 4920 the above problem is overcome by using SNMP. In SNMP you send a request and you get a response immediately. In 4920 because SNMP was used for bi-directional communication between the client and the server there were lot of changes on both the client group and the server group. On the server group they had to implement an agent. The Agent is a piece of code that takes the actual SNMP requests, accesses the required variables in the MIB, formulates the response and sends back the response through the

protocol which is used for communication. The server group had to also implement an MIB specific to the 4920. On the management side a windows application was built so that when you click a box it has to translate to SNMP requests and interpret responses from agents. This windows application called printer Services can talk to both 4900 and 4920 printer. (when user chooses a 4900 it uses PS to manage and in 4920 it uses SNMP)

4.3.3 SNMP Communication Mechanism for the Xprint 4920 Printer

The SNMP communicaton mechanism in 4920 is through the printer services software. When the user clicks a button asking for information, for instance (asking for paper size on the tray1) a mapping is done to some function in the client's code. This function has certain knowledge about what it needs to get from the MIB to get the paper size. The printer services builds the list of all objects which are required, provides a community name for authentication and passes it on to the next layer with a request for getting information. The next layer (SNMP manager) is a piece of code that constructs the Get_Request PDU with the above given information and passes it on to the transport layer for transmission.

On the receiving end, the agent software does an authentication check on the input message. If authentication fails the SNMP entity generates a trap and discards the message. If authentication succeds it futher proceeds to process the message. Agent receives the PDU's, decomposes them and extracts the OID'S and understands that it has to fetch these objects from the MIB. In the MIB each object is represented as a bunch of functions. Let us say user tries to access an object say by using Get_Request command. This command in turn calls the *get* function associated with this object. This *get* function returns the value of the object. In our implementation of the agent we have 4 functions associated with every object. They are get, set, next and test. The get function returns the value of the object. The set function sets the value of the object. The next function returns the value of the next object in the MIB. The test function tests to see if it is okay to set a value for the object. Once the agent has done the required

function it builds a response PDU and hands it back to the UDP/IP layer for sending the datagram.

Once the printer services receives the response, it decomposes the response into OID's and the values that were asked for. It then takes these values (8.5 x 11) and prints a string (Letter) on the screen by referring to the standard printer MIB (RFC 1759).

5.0 CONCLUSION

In this paper we looked at Simple Network Management Protocol to some extent in detail. The future of SNMP appears very rosy, since most of the major computer manufacturers like IBM,DEC, HP, and Sun strongly support SNMP. SNMP will survive and continue to be developed strongly as long as the TCP/IP protocol suite exists.

Even though SNMP has its own disadvantages the functionality provided by SNMP outweighs its disadvantages. SNMP is very effective and is the only successful network management protocol right now. Eventhough SNMP was originally designed for TCP/IP based networks, it has successfully been used for managing other network technologies as well. This expansion beyond TCP/IP based networks is likely to accelerate. Gary Krall, director of marketing for Advanced Comuper Communications Inc. mentions in one of his papers that ***" With the support of manufactiures like DEC and IBM SNMP will continue to snowball"***. Thus in my viewpoint there is a broad support for SNMP amongst a wide range of manufactures and SNMP will continue to be a very successful network management protocol.

GLOSSARY

RFC:	*Request for Comments*
SGMP:	*Simple Gateway Monitoring Protocol*
SMI:	*Structure of Management Information*
TCP/IP:	*Transmission Control Protocol/Internet Protocol*
OSI:	*Open Systems Interconnection*
MIB:	*Management Information Base*
ASN.1:	*Abstract Syntax Notation*
ISO:	*International Organization for Standardization*
CMIS:	*Common Management Information Service*
CMIP:	*Common Management Information Protocol*
CCITT:	*International Telephone and Telegraph Consultative Committee*
IETF:	*Internet Engineering Task Force*
IESG:	*Internet Engineering Steering Group*

BIBLIOGRAPHY

1. Art Wittman : **Examining the Ins and Outs of SNMP**, Network Computing, Dec1992

2. Nair and Waldbusser : **SNMP Management Goes Down to the Wire**, Data Communications , May 1992

3. Peter Drake, **Using SNMP to manage networks**, IEEE Network Journal

4. Murata, Mansfield: **Network Management in a Large-Scale OSI-based Campus Network using SNMP**, IEE Network Magazine, 1992

5. Amirthalingam and Moorhead, **SNMP - An Overview of its Merits and Demerits,** IEEE Network Magazine**,** 1995

6. William Stallings, **SNMP, SNMPv2 and CMIP The Practical Guide to Network Management Standards**, Addison Wesley, July 1993

7. Case, Davin, Fedor and Schoffstall, **Internet Network Management Using The Simple Network Management Protocol**, IEEE Magazine

8. Joseph and Muralidhar, **Integrated Network Management in an Enterprise Environment**, IEEE Network Magazine, July 1990

9. Garry Krall, **SNMP Opens New Lines of Sight**, Data Communications, March 21, 1990

10. Xerox Internal Report, **Color Printer Product Specification,** 1995

11. Marshall T. Rose, **THE SIMPLE BOOK, An Introduction to Management of TCP/IP based internets**, Prentice Hall Series

12. Marshall T. Rose, **THE SIMPLE BOOK, An Introduction to Internet Management,** Prentice Hall Series

13. Ulyless Black, **Network Management Standards, The OSI, SNMP and CMOL Protocols**, McGraw-Hill Inc

14. Marshall T. Rose and Keith Mccloghrie, **Manage Your Network using SNMP,** Prentice Hall Inc

15. Xerox Internal Report, **Xprint Color Laser Printers User's Guide and System Administration Guide**.

16. Lu Ta, **Page Description Languages: The Ups, The Downs and The Potentials**

17. Franz-Joachim, **Network Management, Problems, Standards and Strategies.**