Study Project at C-DOT, Bangalore

On

Network Management

Prepared by:

Jyothsna Deshpande,
NIE, Mysore

Date : 21 Jun 2018

Network Management

What is a Network ?

- It’s a collection of computers, servers, mainframes, network devices, peripherals etc., connected to one another
- Basic elements of a computer network include hardware, software, and protocols
- The interrelationship of these basic elements constitutes the infrastructure of the network
- Hardware components of a network involve cable, hub, switch, NIC (network interface card), modem, router, bridge etc.,
- Types of computer networks: LAN, MAN, WAN etc

Prepared by:
Jyothsna Deshpande,
NIE, Mysore

Date : 21 Jun 2018

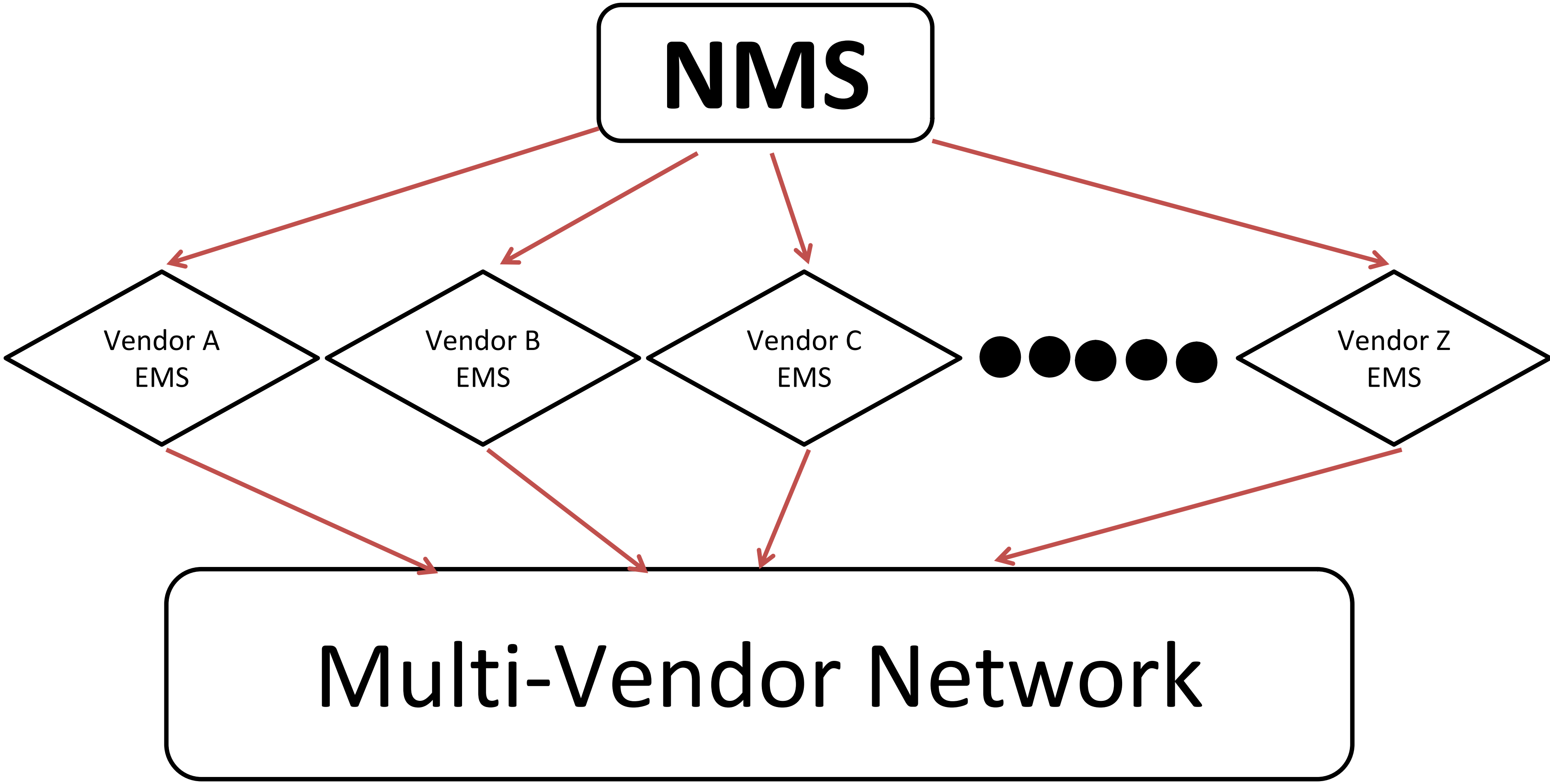
Network Management

Monitoring and Management

- Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator in case of outages or other trouble. Network monitoring is part of network management
- Network management is the process of administering and managing computer networks. Software that enables network administrators to perform their functions is called network management software

Network Management

Typical Network Management System



Prepared by:
Jyothsna Deshpande,
NIE, Mysore

Date : 21 Jun 2018

Network Management

NMS

A network management system (NMS) is an application or set of applications that lets network administrators manage a network's independent components inside a bigger network management framework.

Applications

- Network device discovery
- Network device monitoring
- Network performance analysis
- Network device management
- Intelligent notifications, or customizable alerts

Prepared by:
Jyothsna Deshpande,
NIE, Mysore

Date : 21 Jun 2018

Network Management

Features of a quality network management system

- Cost Reduction: Only one system admin is required at a single location to monitor and manage the entire network
- Time Management : IT provider gets direct access to any data when required. All team members can simply enter or retrieve data using their own workstations. At the same time, their access may be controlled by the network manager.
- Increases productivity: Helps manage every aspect of the office network, which includes software, hardware and other peripherals. The NMS identifies an issue as soon as it occurs it to ensure that there is no productivity slowdown or data loss.
- A large number of protocols exist to support network and network device management. Common protocols are SNMP, TL1 and JMX etc.,

Network Management

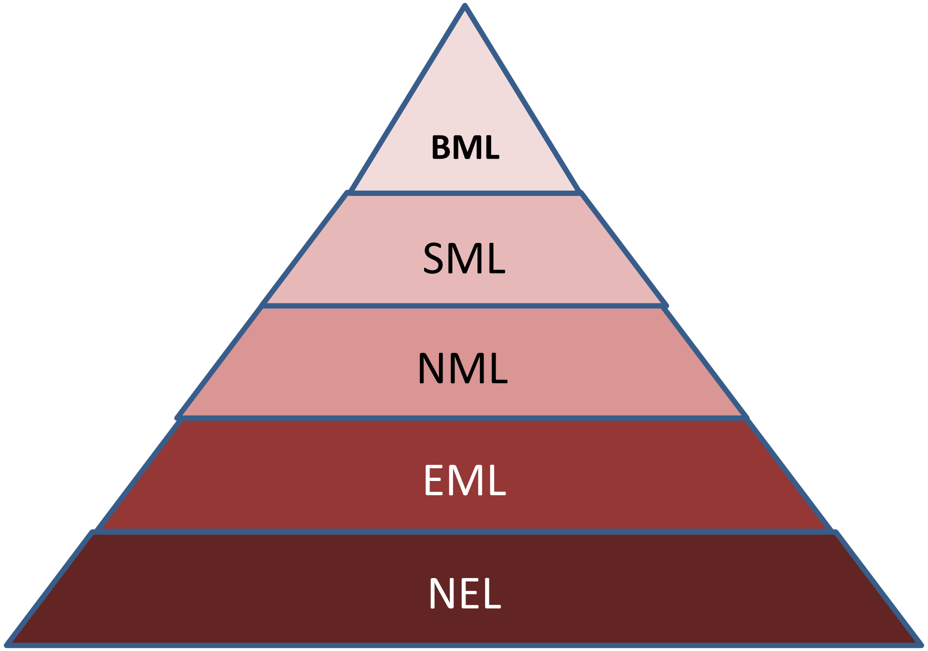
FCAPS

FCAPS is the ISO Telecommunications Management Network model and framework for network management. FCAPS is an acronym for fault, configuration, accounting, performance, security, the management categories into which the ISO model defines network management tasks

Abbreviation	Meaning
F	Fault Detection and Correction
C	Configuration and Operation
A	Accounting and Billing
P	Performance Assessment and Optimization
S	Security Assurance and Protection

Network Management

FCAPS Continued ….



Date : 21 Jun 2018

Prepared by:
Jyothsna Deshpande,
NIE, Mysore

Network Management

FAULT MANAGEMENT

- A fault is an event that has a negative significance. The goal of fault management is to recognize, isolate, correct and log faults that occur in the network

- When a fault or event occurs, a network component will often send a notification to the network operator using either a proprietary or open protocol such as SNMP to collect information about network devices or at least write a message to its console for a console server to catch and log/page. allowing appropriate action to be taken

- This notification is supposed to trigger manual or automatic activities. For example, the gathering of more data to identify the nature and severity of the problem or to bring backup equipment on-line

- Fault logs are one input used to compile statistics to determine the provided service level of individual network elements, as well as sub-networks or the whole network. They are also used to determine apparently fragile network components that require further attention. Errors primarily occur in the areas of fault management and configuration management

Network Management

CONFIGURATION MANAGEMENT

- At this level, network operation is monitored and controlled. Hardware and programming changes, including the addition of new equipment and programs, modification of existing systems, and removal of obsolete systems and programs, are coordinated. At the C level, inventory of equipment and programs is kept and updated regularly
- Streamline the processes of maintenance, repair, expansion and upgrading
- Minimize configuration errors as part of change management
- Optimize network security
- Ensure that changes made to a device or system do not adversely affect other devices or systems
- Roll back changes to a previous configuration if system updating or replacement efforts are unsatisfactory
- Archive the details of all network configuration changes

ACCOUNTING MANAGEMENT

- The goal is to gather usage statistics for users
- Accounting management is concerned with tracking network utilization information, such that individual users, departments, or business units can be appropriately billed or charged for accounting purposes
- For non-billed networks, "administration" replaces "accounting". The goals of administration are to administer the set of authorized users by establishing users, passwords, and permissions, and to administer the operations of the equipment such as by performing software backup and synchronization
- Accounting is often referred to as billing management. Using the statistics, the users can be billed and usage quotas can be enforced. These can be disk usage, link utilization, CPU time, etc.,
- RADIUS, TACACS, and Diameter are examples of protocols commonly used for accounting.(MENTION WHAT IS A PROTOCOL)

Network Management

PERFORMANCE MANAGEMENT

- The performance management level is involved with managing the overall performance of the network. Throughput is maximized, network bottlenecks are avoided, and potential problems are identified. A major part of the effort is to identify which improvements will yield the greatest overall performance enhancement.
- It enables the manager to prepare the network for the future, as well as to determine the efficiency of the current network

Network Management

SECURITY MANAGEMENT

- Security management is the process of controlling access to assets in the network. Data security can be achieved mainly with authentication and encryption
- also that gathered security-related information is analyzed regularly. Security management functions include managing network authentication, authorization, and auditing, such that both internal and external users only have access to appropriate network resources
- configuration and management of network firewalls, intrusion detection systems, and security policies

Network Management

EMS

- An **element management system (EMS) consists of systems and applications for managing network elements on the NEL of Telecom Management Network model**
- EMS manages the functions and capabilities within each NE but does not manage the traffic between different NEs in the network. To support management of the traffic between itself and other NEs, the EMS communicates upward to higher-level NMS.
- The EMS key functionality is divided into FCAPS.
- NORTHBOUND- Interfaces to NMS
- SOUTHBOUND-talks to the devices on the network
- EMS helps Telecom companies to meet stringent QUALITY OF SERVICE.
- EMS to NMS interface provides foundation for implementation of architectures like CORBA(Common Object Request Broker Architecture)

Network Management

WHY NMS ?

It is capable of scaling as the network grows, maintaining high performance levels as the number of network events increase, and providing simplified integration with third-party systems. It meets the service provider's expectations for integrated operational support systems.

Simple Network Management Protocol

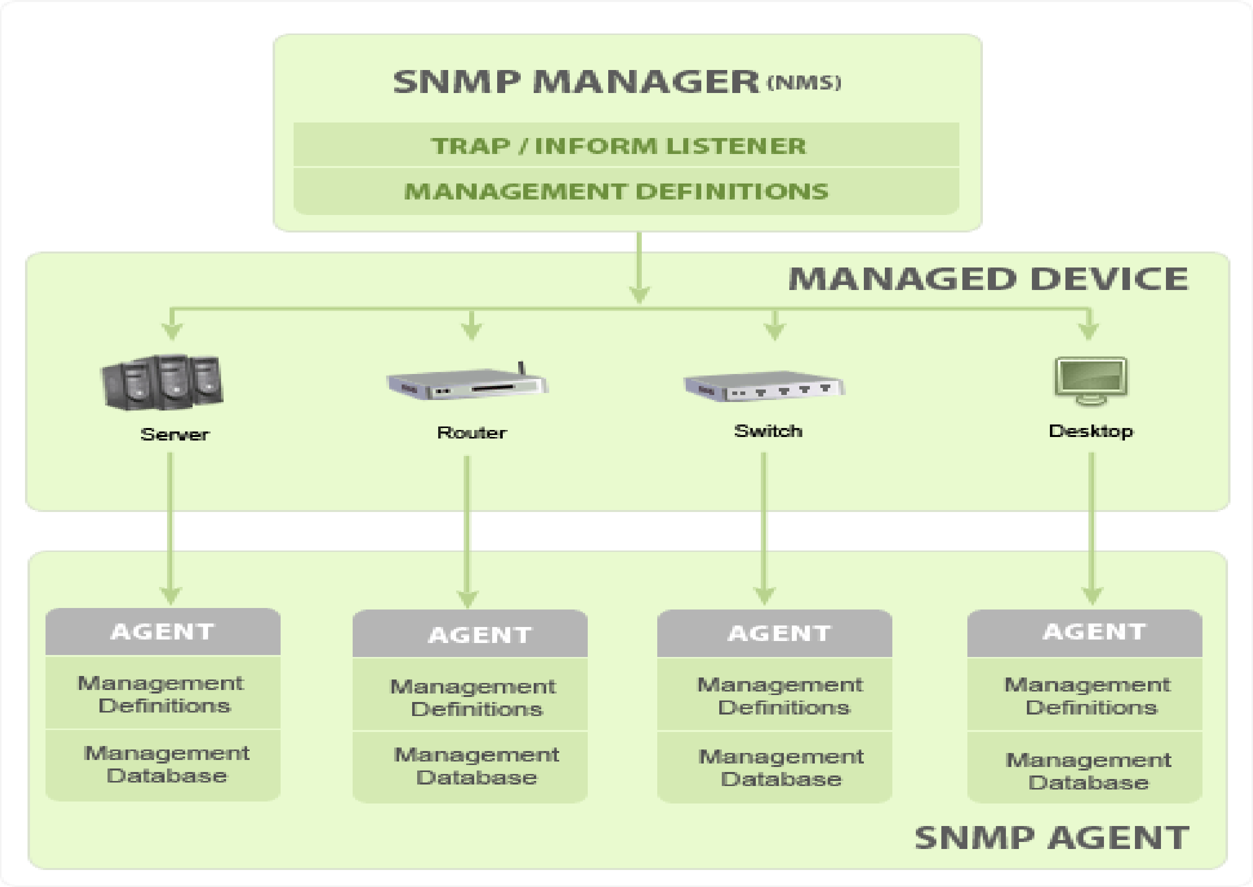
Protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers

Widely used in network management and monitoring.

It consists of an application layer protocol, a database schema and a set of data objects

Simple Network Management Protocol



Prepared by:

Jyothsna Deshpande,
NIE, Mysore

Date : 21 Jun 2018

Simple Network Management Protocol

OVERVIEW

An SNMP-managed network consists of three key components:

- Managed devices
- Agent- A software that runs on the managed device
- Manager with a network management software

Simple Network Management Protocol

MANAGED DEVICES

A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMS. the managed devices can be any type of device I . e routers , access servers , switches , cable modems, bridges, hubs etc.,

Simple Network Management Protocol

AGENTS

Network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP-specific form.

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.

Simple Network Management Protocol

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

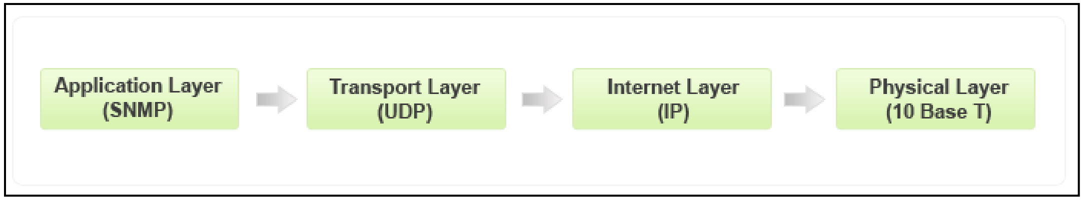
Prepared by:
Jyothsna Deshpande,
NIE, Mysore

Date : 21 Jun 2018

Simple Network Management Protocol

Typical SNMP communication

Being the part of TCP⁄ IP protocol suite, the SNMP messages are wrapped as User Datagram Protocol (UDP) and intern wrapped and transmitted in the Internet Protocol. The following diagram will illustrate the four–layer model developed by Department of Defense (DoD).



Prepared by:
Jyothsna Deshpande,
NIE, Mysore

Date : 21 Jun 2018

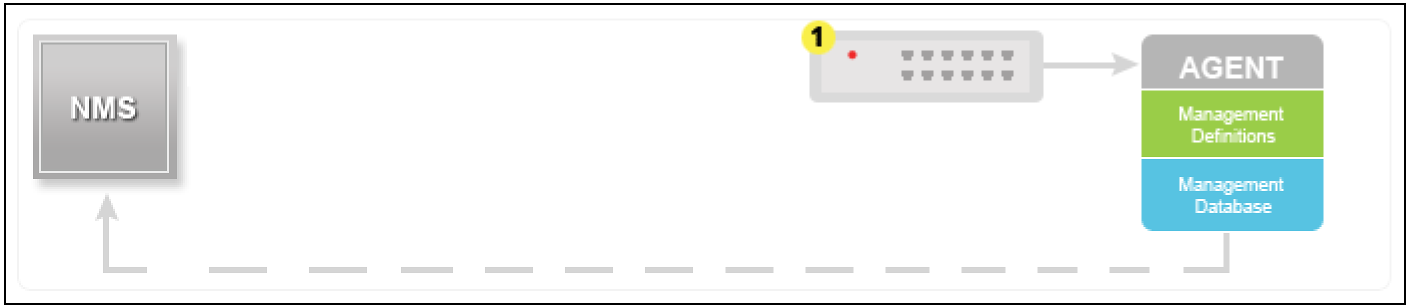
Simple Network Management Protocol

Basic commands of SNMP

- 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

Simple Network Management Protocol

Communication in SNMP



Prepared by:

Jyothsna Deshpande,
NIE, Mysore

Date : 21 Jun 2018

Simple Network Management Protocol

VERSIONS

- SNMP v1
- SNMP v2
- SNMP v3

Prepared by:
Jyothsna Deshpande,
NIE, Mysore

Date : 21 Jun 2018

Simple Network Management Protocol

SNMP version 1

The oldest. Easy to set up - only requires a plaintext community. The biggest downsides are that it does not support 64 bit counters, only 32 bit counters, and that it has little security.

Three simple data types are defined in the SNMPv1 :

- The integer data type is a signed integer in the range of -2^{31} to $2^{31}-1$.
- Octet strings are ordered sequences of 0 to 65,535 octets.
- Object IDs come from the set of all object identifiers allocated according to the rules specified in ASN.1.

Simple Network Management Protocol

SNMP Version 1 (SNMPv1) Message Format

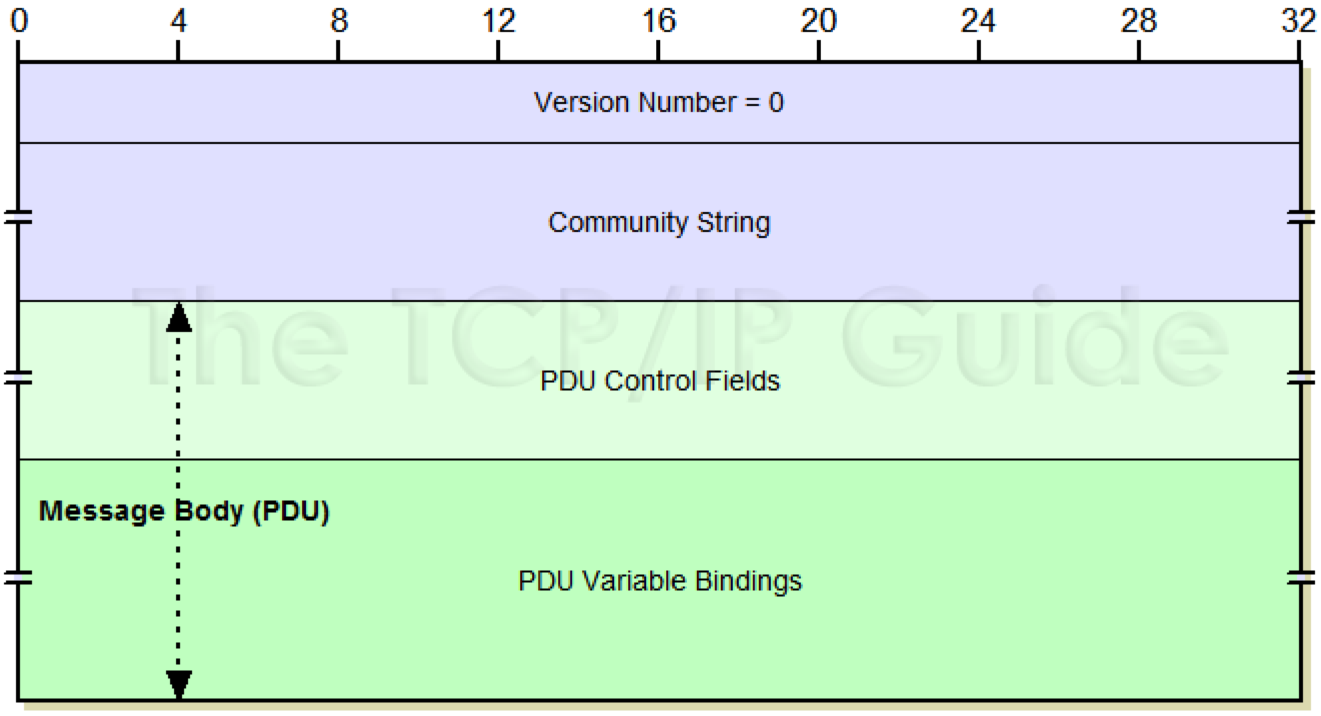
Field Name	Syntax	Size	content
Version	Integer	4	Version Number : Describes the SNMP version number of this message
Community	Octet String	Variable	Community String : Identifies the SNMP community in which the sender and recipient of this message are located
PDU	—	Variable	Protocol Data Unit : The PDU being communicated as the body of the message

Prepared by:
Jyothsna Deshpande,
NIE, Mysore

Date : 21 Jun 2018

Simple Network Management Protocol

Message format



Version Number = 0

Community String

PDU Control Fields

Message Body (PDU)

PDU Variable Bindings

Prepared by:
Jyothsna Deshpande,
NIE, Mysore

Date : 21 Jun 2018

Simple Network Management Protocol

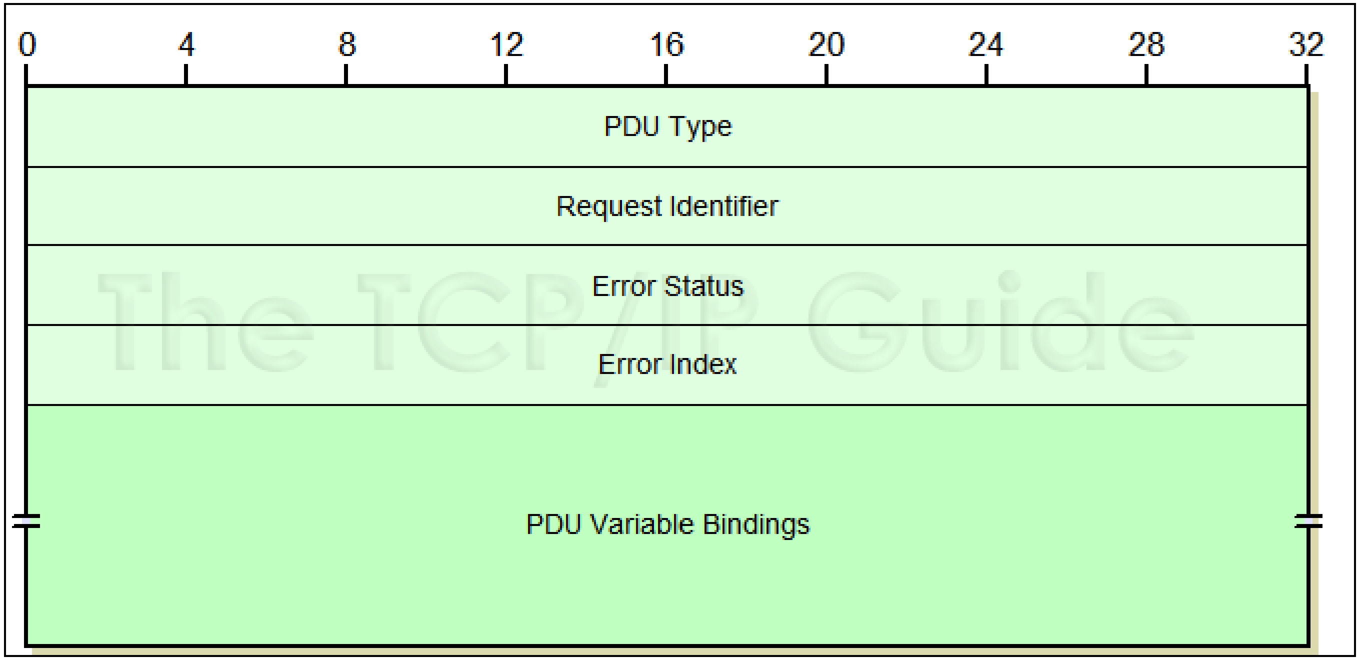
SNMP Version 2

Identical to version 1, except it adds support for 64 bit counters. This matters, especially for interfaces.

Most devices support SNMP V2c nowadays, and generally do so automatically. There are some devices that require you to explicitly enable v2c.

Simple Network Management Protocol

Message body format



PDU Type

Request Identifier

Error Status

Error Index

PDU Variable Bindings

Prepared by:
Jyothsna Deshpande,
NIE, Mysore

Date : 21 Jun 2018

Simple Network Management Protocol

SNMP v3

- Adds security to the 64 bit counters. SNMP version 3 adds both encryption and authentication, which can be used together or separately. SNMPv3 also facilitates remote configuration of the SNMP entities.
- Setup is more complex
- Message format is same as v2

Simple Network Management Protocol

MIB

- Every SNMP agent maintains an information database describing the managed device parameters. The SNMP manager uses this database to request the agent for specific information and further translates the information as needed for the Network Management System (NMS). This commonly shared database between the Agent and the Manager is called Management Information Base (MIB).
- Typically these MIB contains standard set of statistical and control values defined for hardware nodes on a network.
- In short, MIB files are the set of questions that a SNMP Manager can ask the agent. Agent collects these data locally and stores it, as defined in the MIB. So, the SNMP Manager should be aware of these standard and private questions for every type of agent.

Simple Network Management Protocol

OID (object ID)

- Management Information Base (MIB) is a collection of Information for managing network element. The MIBs comprises of managed objects identified by the name Object Identifier (Object ID or OID).
- Each Identifier is unique and denotes specific characteristics of a managed device. When queried for, the return value of each identifier could be different e.g. Text, Number, Counter, etc...
- Scalar: Device’s vendor name, the result can be only one.
- Tabular: CPU utilization of a Quad Processor, this would give me a result for each CPU separately, means there will be 4 results for that particular Object ID.

Simple Network Management Protocol

Sample structure of an OID:

Iso(1).org(3).dod(6).internet(1).private(4).transition(868).products(2).chassis(4).card(1).slotCps(2)-cpsSlotSummary(1).cpsModuleTable(1).cpsModuleEntry(1).cpsModuleModel(3).3562.3

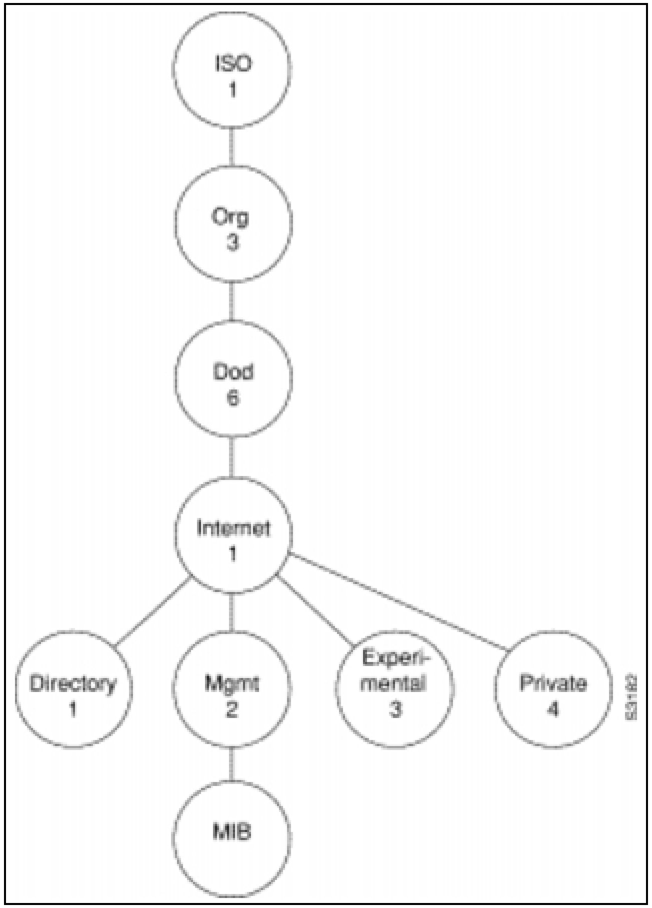
or just:

1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3

Simple Network Management Protocol

MIB HIERARCHY

- The MIB structure is logically represented by a tree hierarchy
- The structure uses branches and those that fall below each category have short text strings and integers to identify them. Text strings describe object names, while integers allow computer software to create compact, encoded representations of the names
- The SNMP MIB is conceptually a tree structure with conceptual tables



Simple Network Management Protocol

SNMP MIB Tables

- Tables are a powerful and often confusing aspect of SNMP MIBs. using or implementing them gets somewhat more complex than implementing scalars.
- Tables have a rigid structure, defined in the SMI. Tables may contain only simple objects, not other tables, although multiple indexes can represent the concept of tables in tables. An entry, or row, in a table is uniquely identified by one or more table indexes, also called auxiliary objects. The OID of an object from a table is the OID for that object's position in the MIB tree concatenated with a representation of all the table indexes for an entry in the table.