Introduction of Network Management

Definition of Network Management

The definition of network management has different description, based on different points of view. Normally, network management is defined as the execution of the set of functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a telecommunications network or a computer network, including performing functions such as initial network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, and accounting management.

Generally, network management does not include user terminal equipment. Hegering [HAN99] defines network management as all measures ensuring the effective and efficient operations of a system within its resources in accordance with corporate goals. To achieve this, network management is tasked with controlling network resources, coordinating net work services, monitoring network states, and reporting network status and anomalies. The objectives of network management are:

- **Managing system resources and services**: this includes control, monitor, update, and report of system states, device configurations, and network services.
- **Simplifying systems management complexity**: is the task of management systems that extrapolates systems management information into a humanly manageable form. Conversely, management systems should also have the ability to interpret high-level management objectives.
- **Providing reliable services**: means to provide networks with a high quality of service and to minimize system downtime. Distributed management systems should detect and fix network faults and errors. Network management must safeguard against all security threats.
- **Maintaining cost consciousness**: requires keeping track of system resources and network users. All network resource and service usage should be tracked and reported. Another acceptable definition identifies network management as the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems [Cle06].
- **Operation** deals with keeping the network (and the services that the network provides) up and running

smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.

- **Administration** deals with keeping track of resources in the network and how they are assigned. It includes all the "housekeeping" that is necessary to keep the network under control.
- **Maintenance** is concerned with performing repairs and upgrades – for example, when equipment must be replaced, when a router needs a patch for an operating system image, when a new switch is added to a network. Maintenance also involves corrective and preventive measures to make the managed network run "better," such as adjusting device configuration parameters.
- **Provisioning** is concerned with configuring resources in the network to support a given service. For example, this might include setting up the network so that a new customer can receive voice service.

In short, network management involves the planning, organizing, monitoring, accounting, and controlling of activities and resources and to keep the network service available and correct.

Basic Components of Network Management System

Network management has three main components: a managing center, a managed device, and a network management protocol. The managing center consists of the network administrator and his or her facilities. A managed device is the network equipment, including its software that is controlled by the managing center. Any hub, bridge, router, server, printer, or modem can be a managed device. The network management protocol is a policy between the managing center and the managed devices. The protocol in this context allows the managing center to obtain the status of managed devices. Network management system contains two primary elements: a manager and agents.

The manager is the console through which the network administrator performs network management functions. A manager can be a network administrative device, as a management host. Agents are the entities that interface to the actual device being managed. An agent can use the network management protocol to inform the managing center of an unexpected event. Bridges, hubs, routers or network servers are examples of managed devices that contain managed objects. These managed objects might be hardware, configuration parameters, performance statistics, and so on, that directly relate to the current operation of the device in question. These objects are arranged in what is known as a virtual information database, called a management information base, also called MIB. Network management protocols (such as SNMP, CMIP) allow managers and agents to communicate for the purpose of accessing these objects. As specified in Internet RFCs and other documents, a typical distributed management system comprises:

Network elements:

Equipments which communicate with the network, according to standards defined by the ITU-T, with the purpose of being monitored or controlled, are named network elements. Sometimes they are also called managed devices [ITU96]. Network elements are hardware devices such as computers, routers, and terminal servers that are connected to networks. A network element is a network node that contains an SNMP agent, which resides on a managed network.

Manager:

A manager generates commands and receives notifications from agents. There are usually only a few managers in a system.

Agents:

Agents collect and store management information such as the number of error packets received by a network element. An agent has local knowledge of management information and transforms that information into the form compatible with SNMP. An agent responds to commands from the manager and sends notification to the manager. There are potentially many agents in a system.

Managed object:

A managed object is a vision of a feature of a network, from the point of view of the management system [ITU92]. All physical and logical resources, such as signaling terminals, routes, event logs, alarm reports and subscriber data, are regarded as managed objects. For example, in IP networks, a list of current active TCP circuits in a particular host computer is a managed object. Managed objects differ from variables, which are particular object instances. Managed objects can be scalar (defining a single object instance) or tabular (defining multiple and related instances). In literature, “managed object” is sometimes used interchangeably with “managed element.”

Network Management Stations (NMSs):

Sometimes NMSs are called consoles. These devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, mega pixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.

Management protocol:

A management protocol is used to convey management information between agents and network management stations (NMSs). Simple Network Management Protocol (SNMP) is the Internet community's de facto standard management protocol.

Structure of Management Information (SMI)

The structure of management information (SMI) language is used to define the rules for naming objects and to encode objects in a managed network center. In other words, SMI is a language by which a specific instance of the data in a managed network center is defined. SMI subdivides into three parts: module definitions, object definitions, and notification definitions.

1. Module definitions are used when describing information modules. An ASN.1 macro, MODULE-

IDENTITY, is used to concisely convey the semantics of an information module.

2. Object definitions describe managed objects. An ASN.1 macro, OBJECT-TYPE, is used to concisely convey the syntax and semantics of a managed object.
3. Notification definitions (also known as “traps”) are used when describing unsolicited transmissions of management information. An ASN.1 macro, NOTIFICATION-TYPE, concisely conveys the syntax and semantics of a notification.

Management Information Base (MIB)

A management information base (MIB) stems from the OSI/ISO Network management model and is a type of database used to manage the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network. Objects in the MIB are defined using a subset of Abstract Syntax Notation One (ASN.1) called “Structure of Management Information Version 2 (SMIv2)” RFC 2578. The software that performs the parsing is a MIB compiler. The database is hierarchical (tree-structured) and entries are addressed through object identifiers.

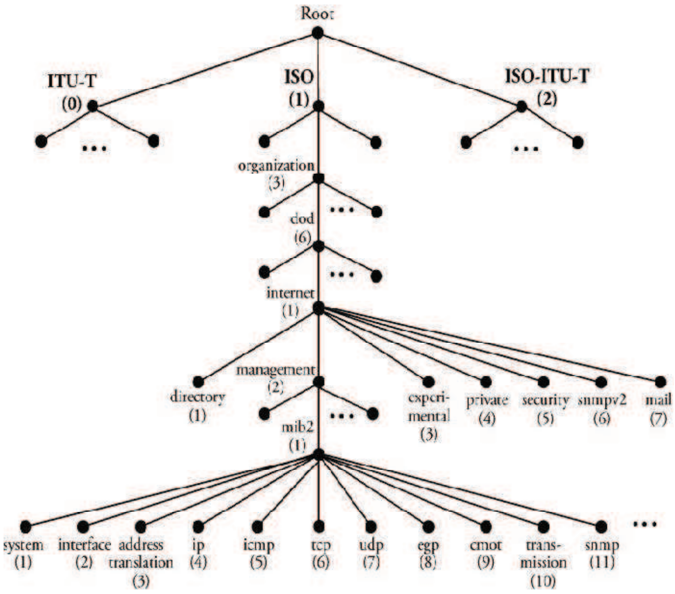

Figure 1: ASN.1 Object Identifier Organized Hierarchically

At the root of the object identifier hierarchy are three entries: ISO (International Standardization Organization), ITU-T (International Telecommunication Union – Telecommunication) standardization sector, and ISO-ITU-T, the joint branch of these two organizations. Figure 3.1 shows only part of the hierarchy. Under the ISO entry are other branches. For example, the organization (3) branch is labeled sequentially from the root as 1.3. If we continue to follow the entries on this branch, we see a path over dod (6), Internet (1), management (2), mib- 2 (1), and ip (4). This path is identified by (1.3.6.1.2.1.4) to indicate all the labeled numbers from the root to the ip (4) entry. Besides that entry, MIB module represents a number of network interfaces and well known Internet protocols at the bottom of this tree. This path clearly shows all the standards of “IP” associated with the “MIB-2” computer networking “management.” Internet documentation RFCs discuss MIBs, notably RFC 1155, “Structure and Identification of Management Information for TCP/IP based internets,” and its two companions, RFC 1213, “Management Information Base for Network Management of TCP/IP-based internets,” and RFC 1157, “A Simple Network Management Protocol.” The most basic elements of a network management model are graphically represented within the basic architecture of network management in Figure 2.

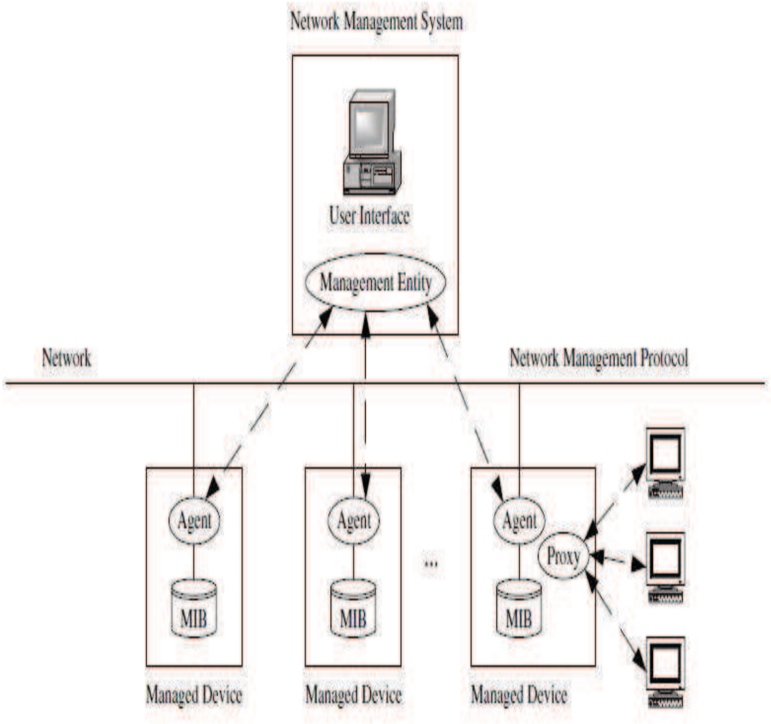

Figure 2: The Typical Network Management Architecture

Interactions between NMSs and managed devices can be any of four different types of commands: *read*, *write*, *traverse*, and *trap*.

• **Read**: To monitor managed devices, NMSs read variables maintained by the devices.

• **Write**: To control managed devices, NMSs write variables stored within the managed devices.

- **Traverse**: NMSs use these operations to determine which variables a managed device supports and to sequentially gather information from variable tables (such as IP routing tables) in managed devices.
- **Trap**: Managed devices use traps to asynchronously report certain events to NMSs.