Chapter 12: Network Management

Jian Ren and Tongtong Li, *Michigan State University*

Abstract: The continuous growth in scale and diversity of computer networks and network components has made network management one of the most challenging issues facing network administrators. It has become impossible to carry out network management functions without the support of automated tools and applications. In this chapter, the major network management issues, including network management requirements, functions, techniques, security, some well-known network management protocols and tools, will be discussed. Location management for the wireless cellular networks will also be briefly described. Finally, policy-based network management, which is a promising direction for the next generation of network management, will be briefly described.

Keywords: network management, Simple Network Management Protocol (SNMP), Structure of Management Information (SMI), Management Information Base (MIB), Remote Network Monitoring (RMON), network monitor, network scanner, packet filter, policy-based network management (PBNM)

1 Introduction

Network management, in general, is a service that employs a variety of protocols, tools, applications, and devices to assist human network managers in monitoring and controlling of the proper network resources, both hardware and software, to address service needs and the network objectives.

When transmission control protocol/internet protocol (TCP/IP) was developed, little thought was given to network management. Prior to the 1980s, the practice of network management was largely proprietary because of the high development cost. The rapid development in the 1980s towards larger and more complex networks caused a significant diffusion of network management technologies. The starting point in providing specific network management tools was in November 1987, when Simple Gateway Monitoring Protocol (SGMP) was issued. In early 1988, the Internet Architecture Board (IAB) approved Simple Network Management Protocol (SNMP) as a short-term solution for network management. Standards like SNMP and Common Management Information Protocol (CMIP) paved the way for standardized network management and development of innovative network management tools and applications.

A network management system (NMS) refers to a collection of applications that enable network components to be monitored and controlled. In general, network management systems have the same basic architecture, as shown in Figure 12.1. The architecture consists of two key elements: a managing device, called a *management station*, or a *manager* and the managed devices, called *management agents* or simply an *agent*. A management station serves as the interface between the human network manager and the network management system. It is also the platform for management applications to perform management functions through interactions with the management agents. The management agent responds to the requests from the management station and also provides the management station with unsolicited information.

Given the diversity of managed elements, such as routers, bridges, switches, hubs and so on, and the wide variety of operating systems and programming interfaces, a management protocol is critical for the management station to communicate with the management agents effectively. SNMP and CMIP are two well-known network management protocols. A network management system is generally described using the Open System Interconnection (OSI) network management model. As an OSI network management protocol, CMIP was proposed as a replacement for the

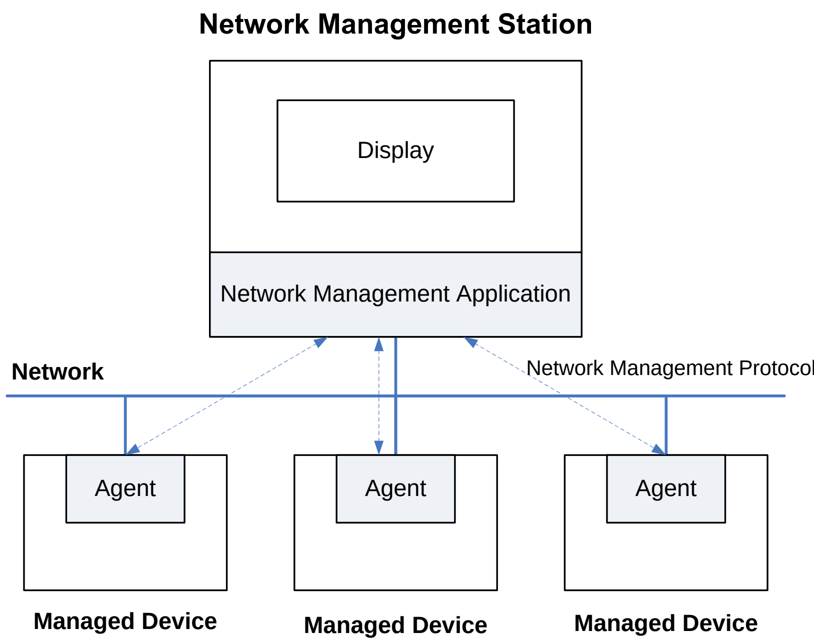

Figure 12.1: Typical Network Management Architecture [1]

simple but less sophisticated SNMP; however, it has not been widely adopted. For this reason, we will focus on SNMP in this chapter.

1.1 OSI Network Management Model

The OSI network management comprises four major models [2]:

- **Organization Model** defines the manager, agent, and managed object. It describes the components of a network management system, the components' functions and infrastructure.
- **Information Model** is concerned with the information structure and storage. It specifies the information base used to describe the managed objects and their relationships. The Structure of Management Information (SMI) defines the syntax and semantics of management information stored in the Management Information Base (MIB). The MIB is used by both the agent process and the manager process for management information exchange and storage.
- **Communication Model** deals with the way that information is exchanged between the agent and the manager and between the managers. There are three key elements in the communication model: transport protocol, application protocol and the actual message to be communicated.

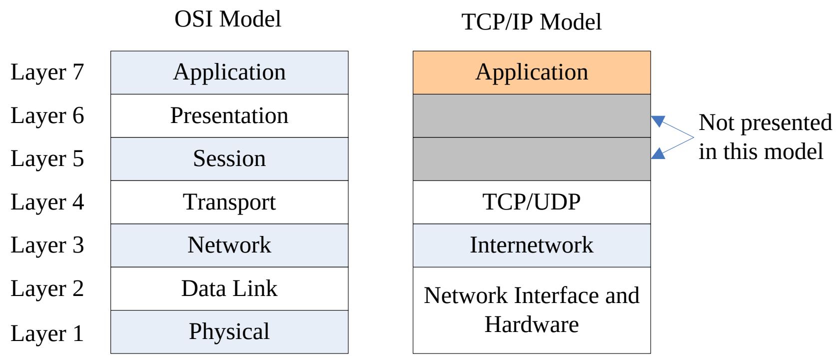

Figure 12.2: The OSI and TCP/IP Reference Models

- **Functional Model** comprises five functional areas of network management, which are discussed in more detail in the next section.

1.2 Network Management Layers

Two protocol architectures have served as the basis for the development of interoperable communications standards: the International Organization for Standardization (ISO) OSI reference model and the TCP/IP reference model, which are compared in Figure 12.2 [3]. The OSI reference model was developed based on the promise that different layers of the protocol provide different services and functions. It provides a conceptual framework for communications among different network elements. The OSI model has seven layers. Network communication occurs at different layers, from the application layer to the physical layer; however, each layer can only communicate with its adjacent layers. The primary functions and services of the OSI layers are described in Table 12.1.

The OSI and TCP/IP reference models have much in common. Both are based on the concept of a stack of independent protocols. Also, the functionality of the corresponding layers is roughly similar.

However, the difference does exist between the two reference models. The concepts that are central to the OSI model include service, interface, and protocol. The OSI reference model makes the distinction among these three concepts explicit. The TCP/IP model, however, does not clearly distinguish among these three concepts. As a consequence, the protocols in the OSI model are better hidden than in the TCP/IP model and can be replaced relatively easily as the technology changes. The OSI model was devised before the corresponding protocols were invented. Therefore,

Table 12.1: OSI Layers and Functions

Layer	Functions
Application	• Provides the user application process with access to OSI facilities
Presentation	• Responsible for data representation, data compression, data encryption and decryption • Ensures communication between systems with different data representation • Allows the application layer to access the session layer services
Session	• Allows users on different machines to establish sessions between them • Establishes and maintains connections between processes, and data transfer services
Transport	• Establishes, maintains and terminates connections between end systems • Provides reliable, transparent data transfer between end systems, or hosts • Provides end-to-end error recovery and flow control • Multiplexes and de-multiplexes messages from applications
Network	• Builds end-to-end route through the network • Datagram encapsulation, fragmentation and reassembly • Error handling and diagnostics
Data Link	• Composed of two sublayers: logical link control (LLC) and and media access control (MAC) • Provides a well-defined service interface to the network layer • Deals with transmission errors • Regulates data flow
Physical	• Handles the interface to the communication medium • Deals with various medium characteristics

it is not biased toward one particular set of protocols, which makes it quite general. With TCP/IP, the reverse is true: the protocols came first, and the model was really just a description of the existing protocols. Consequently, this model does not fit any other protocol stacks [3].

The rest of the chapter is organized as follows. In the section on ISO Network Management Functions, ISO network management functions are briefly described. Network management protocols are discussed in the Section on Network Management Protocols. In the next section, network management tools are briefly described. Wireless network management is discussed next. Policy-based network management is introduced in the following section. The final section draws general conclusions.

2 ISO Network Management Functions

The fundamental goal of network management is to ensure that the network resources are available to the designated users. To ensure rapid and consistent progress on network management functions, ISO has grouped the management functions into five areas: (i) configuration management, (ii) fault management, (iii) accounting management, (iv) security management, and (v) performance management. The ISO classification has gained broad acceptance for both standardized and proprietary network management systems. A description of each management function is provided in the following subsections.

2.1 Configuration Management

Configuration management is concerned with initializing a network, provisioning the network resources and services, and monitoring and controlling the network. More specifically, the responsibilities of configuration management include setting, maintaining, adding, and updating the relationship among components and the status of the components during network operation.

Configuration management consists of both device configuration and network configuration. Device configuration can be performed either locally or remotely. Automated network configuration, such as Dynamic Host Configuration Protocol (DHCP) and Domain Name Services (DNS), plays a key role in network management.

2.2 Fault Management

Fault management involves detection, isolation, and correction of abnormal operations that may cause the failure of the OSI network. The major goal of fault management is to ensure that the network is always available and when a fault occurs, it can be fixed as rapidly as possible.

Faults should be distinct from errors. An error is generally a single event, whereas a fault is an abnormal condition that requires management attention to fix. For example, the physical communication line cut is a fault, while a single bit error on a communication line is an error.

2.3 Security Management

Security management protects the networks and systems from unauthorized access and security attacks. The mechanisms for security management include authentication, encryption and authorization. Security management is also concerned with generation, distribution, and storage of encryption keys as well as other security-related information. Security management may include security systems such as firewalls and intrusion detection systems that provide real-time event monitoring and event logs.

2.4 Accounting Management

Accounting management enables charge for the use of managed objects to be measured and the cost for such use to be determined. The measure may include the resources consumed, the facilities used to collect accounting data, and set billing parameters for the services used by customers, the maintenance of the databases used for billing purposes, and the preparation of resource usage and billing reports.

2.5 Performance Management

Performance management is concerned with evaluating and reporting the behavior and the effectiveness of the managed network objects. A network monitoring system can measure and display the status of the network, such as gathering the statistical information on traffic volume, network availability, response times, and throughput.

3 Network Management Protocols

In this section, different versions of SNMP and RMON will be introduced. SNMP is the most widely used data network management protocol. Most of the network components used in enterprise network systems have built-in network agents that can respond to an SNMP network management system. This enables new components to be automatically monitored. Remote network monitoring (RMON) is, on the other hand, the most important addition to the basic set of SNMP standards. It defines a remote network monitoring MIB that supplements MIB-2 and provides the network manager with vital information about the internetwork.

3.1 SNMP/SNMPv1

The objective of network management is to build a single protocol that manages both OSI and TCP/IP networks. Based on this goal, SNMP, or SNMPv1 [4–6] was first recommended as an interim set of specifications for use as the basis of common network management throughout the system, whereas the ISO CMIP over TCP/IP (CMOT) was recommended as the long term solution [7, 8].

SNMP consists of three specifications: the SMI, which describes how managed objects contained in the MIB are defined; the MIB, which describes the managed objects contained in the MIB; and the SNMP itself, which defines the protocol used to manage these objects.

3.1.1 SNMP Architecture

The model of network management that is used for TCP/IP network management includes the following key elements:

- **Management station**: hosts the network management applications.
- **Management agent**: provides information contained in the MIB to management applications and accepts control information from the management station.
- **Management information base**: defines the information that can be collected and controlled by the management application.
- **Network management protocol**: defines the protocol used to link the management station and the management agents.

The architecture of SNMP, shown in Figure 12.3, demonstrates the key elements of a network management environment. SNMP is designed to be a simple message-based application-layer protocol. The manager process achieves network management using SNMP, which is implemented over the User Datagram Protocol (UDP) [9, 10]. SNMP agent must also implement SNMP and UDP protocols. SNMP is a connectionless protocol, which means that each exchange between a management station and an agent is a separate transaction. This design minimizes the complexity of the management agents.

Figure 12.3 also shows that SNMP supports five types of protocol data units (PDUs). The manager can issue three types of PDUs on behalf of a management application: `GetRequest`,

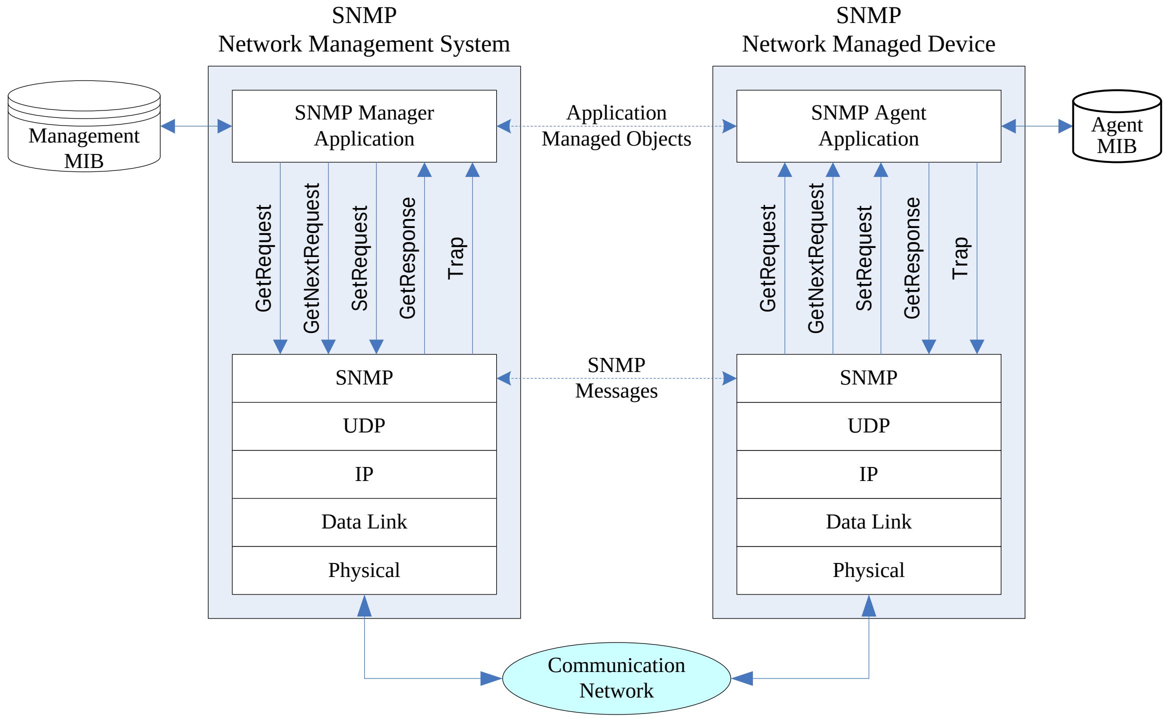

Figure 12.3: SNMP Network Management Architecture

`GetNextRequest`, and `SetRequest`. The first two are variations of the `get` function. All three messages are acknowledged by the agent in the form of a `GetResponse` message, which is passed up to the management application. Another message that the agent generates is `trap`. A `trap` is an unsolicited message and is generated when an event that affects the normal operations of the MIB and the underlying managed resources occurs.

3.1.2 SNMP Protocol Specifications

SNMP message package communicated between a management station and an agent consists of a version identifier indicating the version of the SNMP protocol, an SNMP community name to be used for this message package, and an SNMP PDU. The message structure is shown in Figure 12.4 and each field is explained in Table 12.2.

3.1.3 Structure of Management Information

Figure 12.3 shows the information exchange between a single manager and agent pair. In a real network environment, there are many managers and agents. The foundation of a network man-

Version	Community Name	SNMP PDU

(a) SNMP message

PDU Type	RequestID	ErrorStatus	ErrorIndex	VariableBindings				
				Name 1	Value 1	...	Name N	Value N

(b) `Get/Set` Type of PDUs

PDU Type	Enterprise	Agent-Address	Generic-Trap	Specific-Trap	Timestamp	VariableBindings				
						Name 1	Value 1	...	Name N	Value N

(c) `Trap` PDUs

Figure 12.4: SNMP Message Formats

agement system is a management information base (MIB) containing a set of network objects to be managed. Each managed resource is represented as an object. The MIB is in fact a database structure of such objects in the form of a tree [11]. Each system in a network environment maintains a MIB that keeps the status of the resources to be managed at that system. The information can be used by the network management entity for resource monitoring and controlling. SMI defines the syntax and semantics used to describe the SNMP management information [12].

MIB Structure. For simplicity and extensibility, SMI avoids complex data types. Each type of objects in a MIB has a name, syntax, and an encoding scheme. An object is uniquely identified by an `OBJECT IDENTIFIER`. The identifier is also used to identify the structure of object types. The term `OBJECT DESCRIPTOR` may also be used to refer to the object type [5]. The syntax of an object type is defined using Abstract Syntax Notation One (ASN.1) [13]. Basic encoding rules (BER) have been adopted as the encoding scheme for data type transfer between network entities.

The set of defined objects has a tree structure. Beginning with the root of the object identifier tree, each object identifier component value identifies an arc in the tree. The root has three nodes: `itu (0), iso (1)`, and `joint-iso-itu (2)`. Some of the nodes in the SMI object tree, starting from the root, are shown in Figure 12.5. The identifier is constructed by the set of numbers, separated by a dot that defines the path to the object from the root. Thus, the `internet` node, for example, has its `OBJECT IDENTIFIER` value of `1.3.6.1`. It can also be defined as follows:

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

Table 12.2: SNMP Message Fields

Field	Functions
Version	SNMP version (RFC 1157 is version 1)
Community Name	A pairing of an SNMP agent with some arbitrary set of SNMP application entities (Community name serves as the password to authenticate the SNMP message)
PDU Type	The PDU type for the five messages is application data type, which is defined in RFC 1157 as `GetRequest` (0), `GetNextRequest` (1), `SetRequest` (2), `GetResponse` (3), `trap` (4)
`RequestID`	Used to distinguish among outstanding requests by a unique ID
`ErrorStatus`	A non-zero `ErrorStatus` is used to indicate that an exception occurred while processing a request
`ErrorIndex`	Used to provide additional information on the error status
`VariableBindings`	A list of variable names and corresponding values
`Enterprise`	Type of object generating trap
`AgentAddress`	Address of object generating trap
`GenericTrap`	Generic trap type; values are `coldStart` (0), `warmStart` (1), `linkDown` (2), `linkUp` (3), `authenticationFailure` (4), `egpNeighborLoss` (5), `enterpriseSpecific` (6)
`SpecificTrap`	Specific trap code not covered by the `enterpriseSpecific` type
`Timestamp`	Time elapsed since last re-initialization

Any object in the `internet` node will start with the prefix `1.3.6.1` or simply `internet`.

SMI defines four nodes under `internet`: `directory, mgmt, experimental`, and `private`. The `mgmt` subtree contains the definitions of MIBs that have been approved by the IAB. Two versions of the MIB with the same object identifier have been developed, `mib-1` and its extension `mib-2`. Additional objects can be defined in one of the following three mechanisms [4, 11]:

1. The `mib-2` subtree can be expanded or replaced by a completely new revision.
2. An experimental MIB can be constructed for a particular application. Such objects may subsequently be moved to the `mgmt` subtree.
3. Private extensions can be added to the `private` subtree.

Object Syntax. The syntax of an object type defines the abstract data structure corresponding to that object type. ASN.1 is used to define each individual object and the entire MIB structure. The definition of an object in SNMP contains the data type, its allowable forms and value ranges, and its relationship with other objects within the MIB.

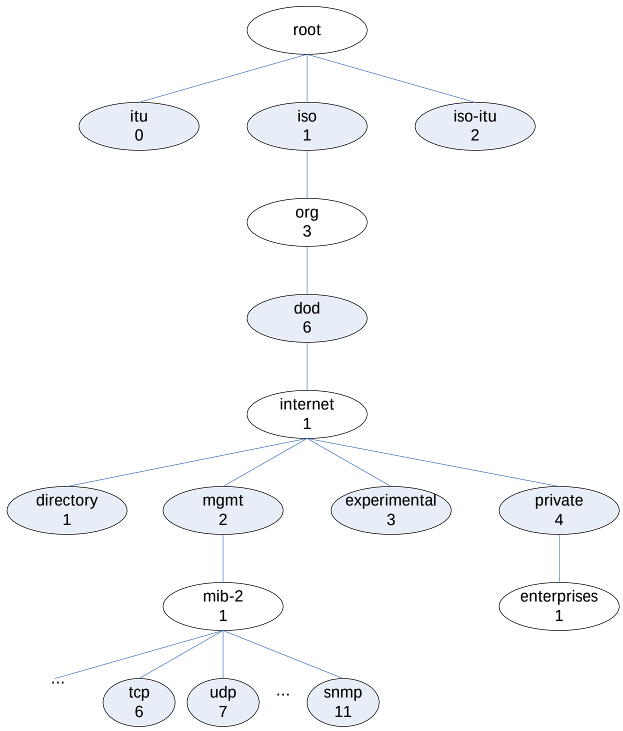

Figure 12.5: Management Information Tree

Encoding. Objects in the MIB are encoded using the BER associated with ASN.1. While not the most compact or efficient form of encoding, BER is a widely used, standardized encoding scheme. BER specifies a method for encoding values of each ASN.1 type as a string of octets for transmitting to another system.

3.1.4 Management Information Base

Two versions of MIBs have been defined: MIB-1 and MIB-2. MIB-2 is a superset of MIB-1, with some additional objects and groups. MIB-2 contains only essential elements; none of the objects is optional. The objects are arranged into groups in Table 12.3.

3.1.5 Security Weaknesses

The only security feature that SNMP offers is through the Community Name contained in the SNMP message as shown in Figure 12.4. Community Name serves as the password to authenticate the SNMP message. Without encryption, this feature essentially offers no security at all since the Community Name can be readily eavesdropped as it passes from the managed system to

Table 12.3: Objects Contained in MIB-2

Groups	Description
system	Contains system description and administrative information
interfaces	Contains information about each of the interfaces from the system to a subnet
at	Contains address translation table for Internet-to-subnet address mapping. This group is deprecated in MIB-2 and is included solely for compatibility with MIB-1 nodes
ip	Contains information relevant to the implementation and operation of IP at a node
icmp	Contains information relevant to the implementation and operation of ICMP at a node
tcp	Contains information relevant to the implementation and operation of TCP at a node
udp	Contains information relevant to the implementation and operation of UDP at a node
egp	Contains information relevant to the implementation and operation of EGP at a node
transmission	Contains information about the transmission schemes and access protocols at each system interface
snmp	Contains information relevant to the implementation and operation of SNMP on this system

the management system. Furthermore, SNMP cannot authenticate the source of a management message. Therefore, it is possible for unauthorized users to exercise SNMP network management functions and to eavesdrop on management information as it passes from the managed systems to the management system. Because of these deficiencies, many SNMP implementations have chosen not to implement the `Set` command. This reduces their utility to that of a network monitor and no network control applications can be supported.

3.2 SNMPv2

SNMP was originally developed as an interim management protocol and CMIP over TCP/IP (CMOT), which essentially enables the OSI system management protocols to operate on top of the TCP protocol, as the ultimate network management protocol. However, the later never came about in reality. At the same time, SNMP has been incorporated widely and enhancement was expected. SNMPv2 was developed when it was obvious that the OSI network management standards were not going to be implemented in the foreseeable future.

PDU Type	RequestID	ErrorStatus	ErrorIndex	VariableBindings				
				Name 1	Value 1	...	Name N	Value N

(a) All but Bulk Type of PDUs

PDU Type	RequestID	NonRepeaters	MaxRepetitions	VariableBindings				
				Name 1	Value 1	...	Name N	Value N

(b) `GetBulkRequest` PDU

Figure 12.6: SNMPv2 PDU Formats

3.2.1 Major Changes in SNMPv2

The SNMPv2 system architecture is essentially the same as that of SNMP. The key enhancement in SNMPv2 can be summarized as follows:

- **Bulk data transfer capability**: The most noticeable change in SNMPv2 is the inclusion of two new PDUs. The first PDU is the `GetBulkRequest` PDU, which enables the manager to retrieve large blocks of data efficiently, and therefore, speeds up the `GetNextRequest` process.
- **Manager-to-manager capability**: The second PDU is the `InformRequest` PDU, which enables one manager to send trap type of information to another, and thus makes network management systems interoperable.
- **Structure of management information**: The SMI defined in SNMP has been consolidated and rewritten.

3.2.2 SNMPv2 Protocol Specifications

To improve the efficiency and performance of message exchange between systems, the PDU data structure in SNMPv2 has been standardized to a common format for all messages given in Figure 12.6. In the `GetBulkRequest` PDU, `NonRepeaters` field indicates the number of non-repetitive field values requested and the `MaxRepetitions` field designates the maximum number of table rows requested.

3.2.3 SNMPv2 Structure of Management Information

The SMI for SNMPv2 is based on the SMI for SNMP. It is nearly a proper superset of the SNMP SMI. The SNMPv2 SMI is divided into three parts: module definitions, object definitions, and notification definitions.

Module definitions are used to describe information modules. An ASN.1 macro, `MODULE-IDENTITY`, is used to concisely convey the semantics of an information module. *Object definitions* are used to describe managed objects. `Object-Type` is used to concisely convey both syntax and semantics of a managed object. *Notification definitions* are used to describe unsolicited transmissions of management information. Notification in SNMPv2 is equivalent to trap in SNMP SMI. `NOTIFICATION-TYPE` conveys both syntax and semantics.

3.2.4 SNMPv2 Management Information Base

The SNMPv2 MIB defines objects that describe the behavior of an SNMPv2 entity. It consists of three groups:

- **System group**: An expansion of the original MIB-2 `system` group. It includes a collection of objects which allow an SNMPv2 entity to act in an agent role to describe its dynamic configurable object resources.
- **SNMP group**: A refinement to the original MIB-2 `snmp` group. It consists of objects which provide the basic instrumentation of the protocol activity.
- **MIB Objects group**: A collection of objects that deal with `SNMPv2Trap` PDUs and that allow several cooperating SNMPv2 entities, each acts in a manager role, to coordinate their use of the SNMPv2 set operations.

3.2.5 Security Weaknesses

Similar to SNMP, SNMPv2 fails in providing any security services. The security of SNMPv2 remains the same as the SNMP. Therefore, it is still vulnerable to security attacks such as masquerade, information modification, and information disclosure.

3.3 SNMPv3

The security deficiency in SNMP and SNMPv2 significantly limits their utility. To remedy this problem, SNMPv3 was developed [14–19]. The SNMPv3 configuration can be set remotely with secure communication links. SNMPv3 also provides a framework for all three versions of SNMP

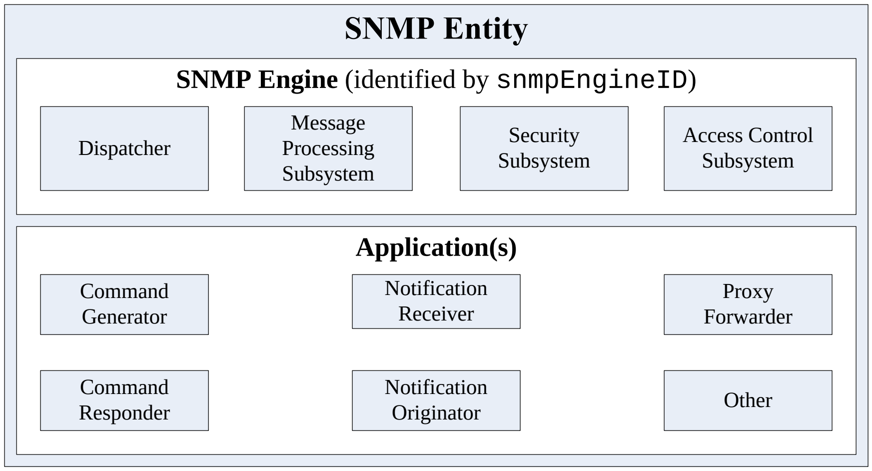

Figure 12.7: SNMP Entity

and future development in SNMP with minimum impacts on existing operations.

3.3.1 SNMPv3 Architecture

An SNMP management network consists of a distributed, interacting collection of SNMP entities. Each entity consists of a collection of modules that interact with each other to provide services. The architecture of an entity is defined as the elements of that entity and the names associated with them. There are three kinds of naming: naming of entities, naming of identities, and naming of management information.

SNMP Entities. The elements of the architecture associated with an SNMP entity, shown in Figure 12.7, consist of an SNMP engine, named `snmpEngineID`, and a set of applications which use the services provided by the SNMP engine. A brief definition of each of the modules is described below.

- **Dispatcher**: Allows for concurrent support of multiple versions of SNMP messages in the SNMP engine. It performs three sets of functions. First, it sends and receives SNMP messages from the network. Secondly, it determines the version of the message and interacts with the corresponding message processing model. Thirdly, it provides an abstract interface to SNMP applications to deliver an incoming PDU to the local application, and to send a PDU from the local application to a remote entity.
- **Message Processing Subsystem**: Responsible for preparing messages for sending, and

Table 12.4: List of Primitives

Component	Primitive	Service Provided
Dispatcher	`sendPdu`	Sends an SNMP request or notification to another SNMP entity
	`processPdu`	Passes an incoming SNMP PDU to an application
	`returnResponsePdu`	Returns an SNMP response PDU to the PDU dispatcher
	`processResponsePdu`	Passes an incoming SNMP response PDU to an application
	`registerContextEngineID`	Registers responsibility for a specific `contextEngineID`, for specific `pduTypes`
	`unregisterContextEngineID`	Unregisters responsibility for a specific `contextEngineID`, for specific `pduTypes`
Message Process Subsystem	`prepareOutgoingMessage`	Prepares an outgoing SNMP request or notification message
	`prepareResponseMessage`	Prepares an outgoing SNMP response message
	`prepareDataElements`	Prepares the abstract data elements from an incoming SNMP message
Access Control Subsystem	`isAccessAllowed`	Checks if access is allowed
Security Subsystem	`generateRequestMsg`	Generates a request or notification message
	`processIncomingMsg`	Processes an incoming message
	`generateResponseMsg`	Generates a response message
User-based Security Model	`authenticateOutgoingMsg`	Authenticates an outgoing message
	`authenticateIncomingMsg`	Authenticates an incoming message
	`encryptData`	Encrypts data
	`decryptData`	Decrypts data

extracting data from received messages.

- **Security Subsystem**: Provides security services such as authentication and privacy of messages. It potentially contains multiple Security Models.
- **Access Control Subsystem**: Provides authorization services by means of one or more Access Control Models.

SNMP Names. The names associated with the identities include principal, `securityName` and a model-dependent security ID. A principal indicates to "whom" services are provided. A principal can either be a person or an application. A `securityName` is a human readable string which represents a principal. A model-dependent security ID is the model-specific representation of a securityName within a particular Security Model.

A management entity can be responsible for more than one managed object. Each object is called a context and has a contextEngineID and a contextName. A scopePDU is a block of data containing a contextEngineID, a contextName, and a PDU.

Abstract Service Interfaces. Abstract service interfaces describe the conceptual interfaces between the various subsystems within an SNMP entity and are defined by a set of primitives and the abstract data elements. A primitive specifies the function to be performed, and the parameters to be used to pass data and control information. Table 12.4 lists the primitives that have been defined for the various subsystems.

3.3.2 SNMPv3 Applications

SNMPv3 formally defines five types of applications. These applications make use of the services provided by the SNMP engine. SNMPv3 defines the procedures followed by each type of application when generating PDUs for transmission or processing incoming PDUs. The procedures are defined in terms of interaction with the dispatcher by means of the dispatcher primitives.

Command Generator. The command generator application makes use of the sendPdu and processResponsePdu dispatcher primitive to generate GetRequest, GetNextRequest, GetBulk, and SetRequest messages. It also processes the response to the command sent. The sendPdu provides the dispatcher with information about the intended destination, security parameters, and the actual PDU to be sent. The dispatcher then invokes the Message Processing Model, which in turn invokes the Security Model, to prepare the message. The dispatcher delivers each incoming response PDU to the correct command generator application, using the processResponsePdu primitive.

Command Responder. A command responder application makes use of four dispatcher primitives (registerContextEngineID, unregisterContextEngineID, processPdu, and returnResponsePdu) and one Access Control Subsystem primitive (isAccessAllowed) to receive and process SNMP Get and Set requests. It also sends response messages. The dispatcher delivers each incoming request PDU to the correct command responder application, using the processPDU primitive.

The command generator uses `returnResponsePdu` to deliver the message back to the dispatcher.

Notification Originators. A notification originator application follows the same general procedures used for a command generator application to generate either a `trap` or an `Inform`. If an `Inform` PDU is to be sent, both the `sendPDU` and `processResponse` primitives are used. If a `trap` PDU is to be sent, only the `sendPDU` primitive is used.

Notification Receiver. A notification receiver application follows a subset of the general procedures as for a command responder application to receive SNMP notification messages. Both types of PDUs are received by means of a `processPdu` primitive. For an `Inform` PDU, a `returnResponsePdu` primitive is used to respond.

Proxy Forwarder. A proxy forwarder application makes use of dispatcher primitives to forward SNMP messages. The proxy forwarder application handles four types of messages: messages containing PDU types generated by a command generator application, messages containing PDU types generated by a command responder application, messages containing PDU types generated by a notification originator application, and messages containing a `report` indicator.

3.3.3 SNMPv3 Management Information Base

Three separate MIB modules have been defined in [17] to support SNMPv3 applications: the management target MIB, the notification MIB, and the proxy MIB.

The `SNMP-TARGET-MIB` module contains objects for defining management targets. It consists of two tables. The first table, the `snmpTargetAddrTable`, contains information about transport domains and addresses. The second table, the `snmpTargetParamsTable`, contains information about SNMP version and security information to be used when sending messages to particular transport domains and addresses.

The `SNMP-NOTIFICATION-MIB` module contains objects for remote configuration of the parameters used by an SNMP entity for the generation of notifications. It consists of three tables. The first table, the `snmpNotifyTable`, selects one or more entries in `snmpTargetAddrTable` to be used for notifications generation. The second table, the `snmpNotifyFilterProfileTable`, sparsely augments the `snmpTargetParamsTable` so as to associate a set of filters with a particular management

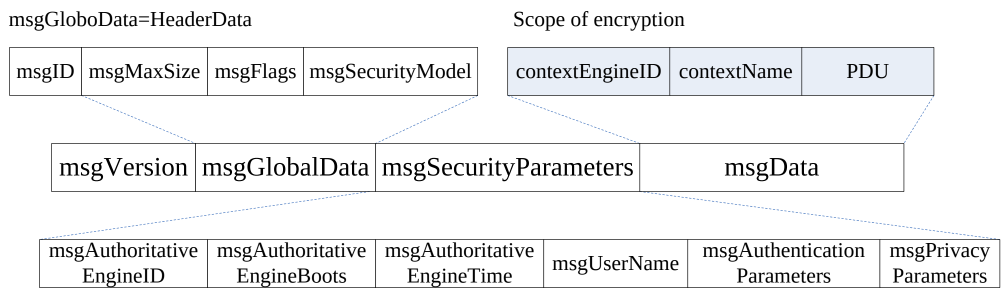

Figure 12.8: SNMPv3 Message Format

target. The third table, the `snmpNotifyFilterTable`, defines filters used to limit the number of notifications generated for a particular management target.

The `SNMP-PROXY-MIB` contains objects for the remote configuration of the parameters used by an SNMP entity for proxy forwarding operations. It contains a single table, `snmpProxyTable`, which is used to define the translations between management targets for forwarding messages.

3.3.4 SNMPv3 Message Format

Each SNMPv3 message includes four data groups: `msgVersion`, `msgGlobaGata`, `msgSecurityParameters`, and `msgPDU`, as shown in Figure 12.8.

The `msgVersion` field is set to `snmpv3 (3)` and identifies the message as an SNMP version 3 Message. The `msgGlobaGata` field contains the header information. The `msgSecurityParameters` field is used exclusively by the Security Model. The contents and format of the data are defined by the Security Model. The `msgData` is the scoped PDU field containing information to identify an administratively unique context and a PDU.

3.3.5 Security Enhancement

One of the main objectives in developing SNMPv3 is the addition of security services for network management. SNMPv3 is intended to address four types of security threats: modification of information, masquerade, disclosure, and message stream modification. The first two are identified as principal threats, while the last two are identified as secondary threats. A User-based Security Model (USM) is proposed in SNMPv3. This model reflects the traditional concept of a user identified by a `userName` [18].

User-Based Security Model (USM). The USM encompasses three different security modules: the *authentication module*, the *timeliness module*, and the *privacy module*.

In order to protect against message replay, delay and redirection, when two management entities communicate, one of the SNMP engines is designated to be the *authoritative SNMP engine*. Particularly, when an SNMP message contains a payload which expects a response, then the receiver of such messages is authoritative. When an SNMP message contains a payload which does not expect a response, then the sender of such a message is authoritative.

The message process model invokes the USM in the security subsystem. Based on the security level set in the message, the USM in turn invokes the authentication modules, privacy modules, and timeliness module. The USM allows for different protocols to be used instead of, or concurrent with the protocols described in [18] and [19].

Authentication. USM uses one of two alternative authentication protocols to achieve data integrity and data origin authentication: HMAC-MD5-96 and HMAC-SHA-96. HMAC uses a secure hash function and a secret key to produce a message authentication code [11, 20]. In this case, the secret key is the localized user's private authentication key `authKey`. The value of `authKey` is not accessible via SNMP. For HMAC-MD5-96, MD5 is used as the underlying hash function. The `authKey` is 16 octets in length. The algorithm produces a 128-bit output, which is truncated to 12 octets (96 bits). For HMAC-SHA-96, the underling hash function is SHA-1. The `authKey` is 20 octets in length. The algorithm produces a 20-octet output, which is again truncated to 12 octets.

Encryption. USM uses CBC-DES Symmetric Encryption Protocol to protect against disclosure of the message payload [11,20]. A 16-octet `privKey` is provided as the input to the encryption protocol. The first eight octets (64 bits) of this `privKey` are used as a DES key. Since DES uses only 56 bits, the least significant bit in each octet is disregarded. For CBC mode, a 64-bit initialization vector (IV) is required. The last eight octets of the `privKey` contain a value that is used to generate this IV.

In order to ensure that the IVs for two different packets encrypted by the same key are not identical, an 8-octet string called "salt" is XOR-ed with the pre-IV to obtain the IV.

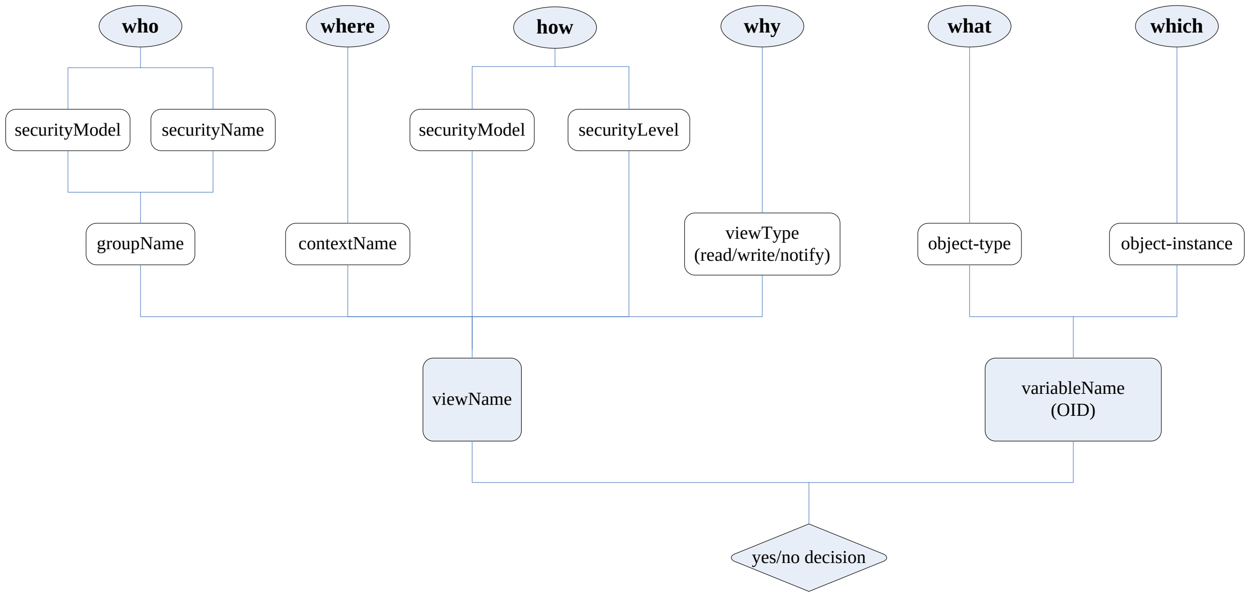

Figure 12.9: VACM Access Control Logic

View-Based Access Control Model (VACM). The access control subsystem of an SNMP engine has the responsibility for checking whether a specific type of access (read, write, notify) to a particular object (instance) is allowed.

Access control occurs in an SNMP entity when processing SNMP retrieval or modification request messages from an SNMP entity and when an SNMP notification message is generated.

The VACM defines a set of services that an application can use for checking access rights. It is the responsibility of the application to make the proper service calls for access checking.

Elements of the VACM Model. VACM defined in [19] comprises five elements: groups, security levels, contexts, MIB views, and access policy.

- **Groups**: A group is a set of zeros or more < `securityModel, securityName` > tuples on whose behalf SNMP management objects can be accessed. A group defines the access rights afforded to all `securityNames` which belong to that group. The combination of a `securityModel` and a `securityName` maps to at most one group identified by a `groupName`.
- **securityLevel**: The access rights for the members of a group may vary depending on the security levels. The level of security is set by the `msgFlags` given in Figure 12.8.
- **Contexts**: An SNMP context is a collection of management information accessible by an

SNMP entity. An SNMP entity potentially has access to many contexts.

- **MIB Views**: For security reasons, it is often desirable to restrict the access rights of a particular group to only a subset of the MIB. To provide this capability, access to a context is via a MIB view, which details the specific set of managed object types as a set of view subtrees, with each view subtree being included in or excluded from the view.
- **Access Policy**: The VACM determines the access rights of a group (identified by `groupName`) for a particular context (identified by `contextName`) based on `securityModel` and `securityLevel`. The access rights include a read-view, a write-view and a notify-view.

The VACM Process. An SNMP application invokes VACM via the `isAccessAllowed` primitive with the input parameters, including `securityModel, securityName, securityLevel, viewType, contextName`, and `variableName`. The VACM decision for access control is shown in Figure 12.9.

3.4 Remote Network Monitoring (RMON)

Remote network monitoring devices, often called *monitors* or *probes*, are instruments that exist for the purpose of managing a network. The RMON can produce summary information of the managed objects, including error statistics, performance statistics, and traffic statistics. Based on the statistics information, the status of the managed objects can be observed and analyzed.

3.4.1 RMON1 Groups

The RMON1 specification is primarily a definition of a MIB defined in [21] and [22]. RMON1 delivers management information in nine groups of monitoring elements, each provides specific sets of data to meet common network-monitoring requirements. Some RMON1 groups require support of other RMON1 groups to function properly. Table 12.5 summarizes the nine monitoring groups specified in [23].

3.4.2 RMON2

RMON2 defined in [23] enables network statistics and analysis be provided from the network layer up to the application layer. The most visible and most beneficial capability in RMON2 is

Table 12.5: RMON1 MIBs

RMON Group	**Function**
Statistics	Contains statistics measured by the probe for each monitored interface on this device
History	Records periodic statistical samples from a network and stores them for later retrieval
Alarm	Takes statistical samples periodically from variables in the probe and compares them with previously configured thresholds. If the monitored variable crosses a threshold, an event is generated
Host	Contains statistics associated with each host discovered on the network
HostTopN	Prepares statistics about the top N hosts on a subnetwork based on the available parameters
Matrix	Stores statistics for conversations between sets of two addresses. As the device detects a new conversation, it creates a new entry in its table
Filters	Enables packets to be matched by a filter equation. These matched packets form a data stream that may be captured or may generate events
Packet Capture	Enables packets to be captured after they flow through a channel
Events	Controls the generation and notification of events from a device
Token Ring Extensions	Contains four groups to define some additional monitoring functions specified for Token Ring. They are the Ring Station Group, the Ring Station Order Group, the Ring Station Configuration Group, and the Source Routing Statistics Group

monitoring above the MAC layer which supports protocol distribution and provides a view of the whole network rather than a single local area network (LAN) segment. RMON2 also enables host traffic for particular applications to be recorded. The managed objects in RMON2 are arranged into groups as shown in Table 12.6.

4 Network Management Tools

The tremendous growth in scale and diversity of computer networks has made network management a complex and challenging task for network administrators. To manage computer networks tangibly and efficiently, specific management tools must be used to monitor the network activities and to preemptively determine the network behavior.

Network management tools are usually based upon particular network management protocols. Most systems use open protocols. However, some network management tools are based upon vendor specific proprietary protocols. The network management capabilities provided with the tools are usually based upon the functionality supported by the network management protocols.

Table 12.6: RMON2 MIBs

RMON2 MIB Group	Functions
Protocol directory	Presents an inventory of protocol types capable of monitoring
Protocol distribution	Collects the relative amounts of octets and packets
Address mapping	Provides address translation between MAC addresses and network addresses on the interface
Network layer host	Provides network host traffic statistics
Network layer matrix	Provides traffic analysis between each pair of network hosts
Application layer host	Reports on protocol usage at the network layer or higher
Application layer matrix	Provides protocol traffic analysis between pairs of network hosts
User history collection	Provides user-specified history collection on alarm and configuration history
Probe configuration	Controls the configuration of probe parameters
RMON conformance	Describes the conformance requirements to RMON2 MIB

4.1 Network Monitors

One of the fundamental responsibilities of a network administrator is network monitoring. Network monitors should have the ability to collect and analyze network traffic. A good system will allow you to generate log files and performance charts that detail your system's capabilities and responses. With this data, you can optimize your network configuration and be better prepared for faults. Some network monitors are designed with SNMP management capability to offer full view of the fundamental network issues. To minimize the network down-time, effective networking monitoring will alert network anomaly immediately.

4.2 Network Scanners

Network security vulnerabilities are being detected on a daily basis – over 10,000 in the last two years alone [24]. Network scanner is one of the key element for network security. It checks network system, operating system and applications running on your network to identify vulnerabilities and possible security flaws that could expose your network to security compromise. To protect online assets and eliminate the risk to your business, some network scanners can also automate vulnerability assessment.

4.3 Packet Filters

Packet filters control access of data packets to a network by scanning the contents of the packet headers. A packet filter determines whether a packet should be allowed to go through a given point based on certain access control policies.

Packet filtering is most commonly used as a first line of defense against attacks from machines outside your network. It has become a common and inexpensive method of security protection mechanism. However, packet filtering does guarantee the security of your network and internal data.

Dynamic packet filtering, also referred to as stateful inspection, is a firewall architecture that works at the network layer. Stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid. A stateful firewall may examine the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Because of this, filtering decisions are based not only on administrator-defined rules but also on context that has been established by prior packets that have passed through the firewall.

5 Wireless Network Management

Wireless communications have had a significant impact on the world as far back as World War II. Since then wireless communications have experienced an explosive grown due to the development of cellular concept to reuse the radio frequency [25]. People use cellular phones daily to communicate with one another and share data quickly in a small office building and across the world. Emergency services such as the police department utilize wireless networks to communicate important information quickly. Wireless network is also an inexpensive and rapid way to be connected to the Internet in countries and regions that lack of resources as is the case in most developing countries.

A wireless network is a radio network of individual cells employed with base stations (BSs). Each BS covers a small and uniquely identified geographical area. For identification purposes, each user must subscribe to a regional subnetwork, called the *subscriber's home network*, for communications services. The subscriber's identity is a permanent address that resides in the subscriber's home

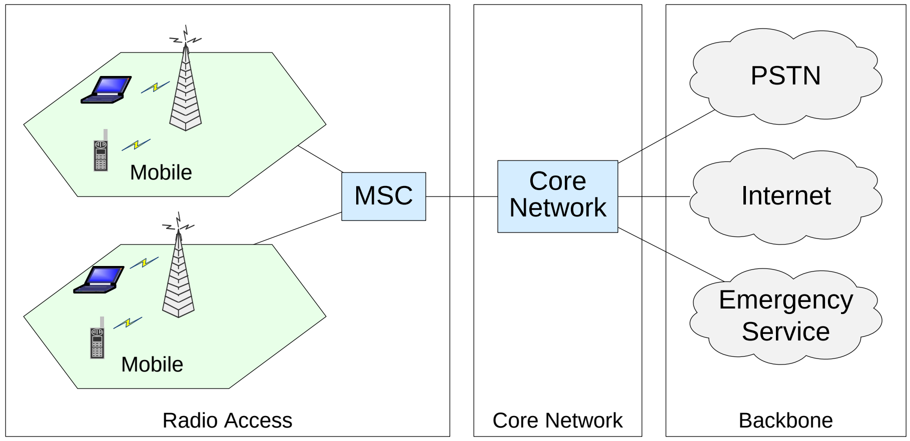

Figure 12.10: A Typical Cellular Network

location register (HLR). When the subscriber moves away from its home network, the new network it enters is a foreign or visitor network. It must update its registration with the home location register through its visitor location register (VLR) in order to facilitate message delivery to the mobile in its new location. The procedure of maintaining an association between the mobile and its HLR when it is away from its home network is referred to as *location management*.

Location management is one of the major functions in cellular networks. The aim of location management is to track where the subscribers are, so that calls, short message service (SMS) and other mobile phone services can be delivered to them.

5.1 Cellular Networks

In a cellular network, a service coverage area is divided into smaller areas of hexagonal shape, referred to as a *cell*. Each cell is served by a fixed BS. The BS is able to communicate with mobile stations such as cellular phones using its radio transceiver. The BS is connected to the mobile switching center (MSC) which is, in turn, connected to the backbone network. Figure 12.10 illustrates a typical cellular network.

One of the central concept of the cellular networks is frequency reuse without increasing the interface. The ability to reuse frequencies expands the total system capacity without the need to employ high power transmitters.

5.2 Location Management for Cellular Networks

Location management allows the system to keep the user's location knowledge in order to be able to find him in case of an incoming call. The location management consists of a *location updating* scheme and a *paging* scheme.

The paging operation is performed by the cellular network. When an incoming call arrives for a mobile station, the cellular network will page the mobile station in all possible cells to find out the cell in which the mobile device is actually located so that incoming call can be routed to the corresponding BS. The paging process consists of polling the cells in the location area until the target mobile device replies to the paging message. The location area can be divided in cell subsets that are called paging areas, which will be polled sequentially [26]. Paging must be performed within the maximum paging delay. Each polling cycle should be limited by a timeout period. The paging cost is proportional not only to the number of polling cycles but also to the number of cells polled in each cycle. The paging area can be either set statically or dynamically determined by a prediction on available profile information provided by the location update function.

Location update is the process for the mobile terminals to report their locations to the network. All mobiles are actively sending location update messages to the BSs to keep the network informed of their locations. The location management implemented in cellular systems makes use of location areas and are performed automatically. Location areas allow the system to track the mobiles during their roaming in the network(s): subscriber location is known if the system knows the location area in which the subscriber is located. When the system must establish a communication with the mobile, the paging only occurs in the current user location area. Thus, resource consumption is limited to this location area since paging messages are only transmitted in the cells of this particular location area. A location update scheme is either *static* or *dynamic* [27–29]. A scheme is called static if the location area is static and is the same for all users. The location updates must be generated by a mobile station regardless of its mobility patterns. A scheme is called dynamic if the location update is based on the mobile station in any cell and its mobility patterns. The structure of the location update is user specific and changes whenever the user changes his mobility and call patterns.

A location update scheme can also be classified as either *global* or *local* [27, 28]. A location update scheme is global if all subscribes update their locations at the same set of cells. A global scheme is based on aggregate statistics and traffic patterns. A scheme is called local if an individual subscriber is allowed to decide when and where to perform location update. A local scheme is also called individualized or per-user based. A per-user based scheme is based on the statistics and/or mobility patterns of an individual subscriber, and it is usually dynamic. An individualized scheme is not necessarily dynamic.

Location update involves reverse control channels while paging involves forward control channels. The total location management cost is the sum of the location update cost and the paging cost. There is a tradeoff between the location update cost and the paging cost. If a mobile station updates its location more frequently, the network knows the location of the mobile station more accurately. Then the paging cost will be lower when an incoming call arrives for the mobile station. Therefore location update and paging costs cannot be minimized at the same time.

There is also a tradeoff between the paging cost and the paging delay. If there is no delay constraint, the cells can page sequentially to minimize paging cost. While for highly delay constraint paging, all cells can be paged simultaneously, which will result in maximum paging cost. The research on minimizing location update cost under paging cost constraints and on minimizing the paging cost under delay constraints have been intensively studied in the current literature [27, 30].

6 Policy-based Network Management - *Solutions for the Next Generation*

Policy-based network management (PBNM) [31] is a way to manage the configuration and behavior of one or more entities based on the business needs and policies. PBNM systems enable business rules and procedures to be translated into policies that configure and control the network and its services. PBNM can also be defined as a condition-action response mechanism. The general form is:

```
ON <event>
IF <conditions>
THEN <actions>
```

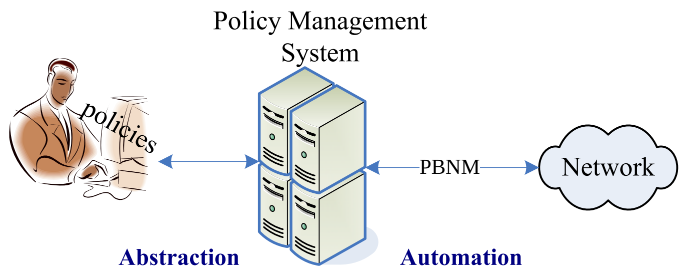

Figure 12.11: The Basic Model Of Police-Based Management

Business Management Layer • Goal setting, planning • Policy setting
Service Management Layer • QoS • Service interface
Network Management Layer • connectivity • Network control, statistics

Figure 12.12: Network Management Layered View

PBNM enables an automatic response to conditions in the network according to pre-defined policies. By automating the network management, the entire network can be managed as an entity itself. The essence of PBNM can be portrayed in Figure 12.11.

6.1 What Is a Policy?

Policy is typically defined as a set of operating rules that manage and control access to network resources. It allows a network to be managed through a descriptive language. Policy can be represented at different levels, ranging from business goals to device-specific configuration parameters.

Policy management is the usage of operating rules to accomplish decisions. It forms a bridge between service level agreement (SLA) and the network entities. Business goals and policies can be defined as a separate business management layer on top of the service management layer that provides service such as Quality of Service (QoS) as shown in Figure 12.12 [32].

With the growth in scale and complexity of computer networks, QoS and security are becoming very challenging management issues. PBNM is emerging as a promising solution in simplifying the management of QoS and security.

6.2 Benefits of PBNM

The appealing part of PBNM is that through abstractions, the network management QoS and security mechanisms can be simplified so that the majority of network management tasks are simple in nature. PBNM also enables system behavior to be changed without modifying implementation. More specifically, the benefit of PBNM can be summarized as follows [31, 33]:

- **Optimizes network resource intelligently**: The automation of management tasks intelligently optimizes both the use of network infrastructure and the network policies. PBNM reduces the need for adding bandwidth to congested links.

- **Simplifies network and service management**: PBNM users are no longer required to be a specialist in order to perform network management functions. Another aspect is that changes in business policies do not necessarily require any low layer development, which makes management updating painless.

- **Manages complex traffic and services intelligently**: PNBM can manage applications with competing demand for shared resources using the predicated traffic information. Unauthorized and unwanted applications can be controlled or eliminated, while mission critical applications can be assigned with special priority.

- **Performs time-critical functions efficiently**: PBNM can simplify and better implement the time-critical functions, such as changing device configurations within a specific time-window and performing scheduled provisioning functions.

- **Provides better security**: PBNM can help categorize traffic into expected and unexpected types and assign rules to deal with each type. PBNM can also be used to determine whether a particular user can access a resource or not.

6.3 Architecture of a PBNM System

The general architecture for a policy management system is shown in Figure 12.13. This architecture contains four major components [33, 34]:

- **Policy management Console**: The user interface to construct policies, deploy policies, and monitor the status of policy-managed environment.

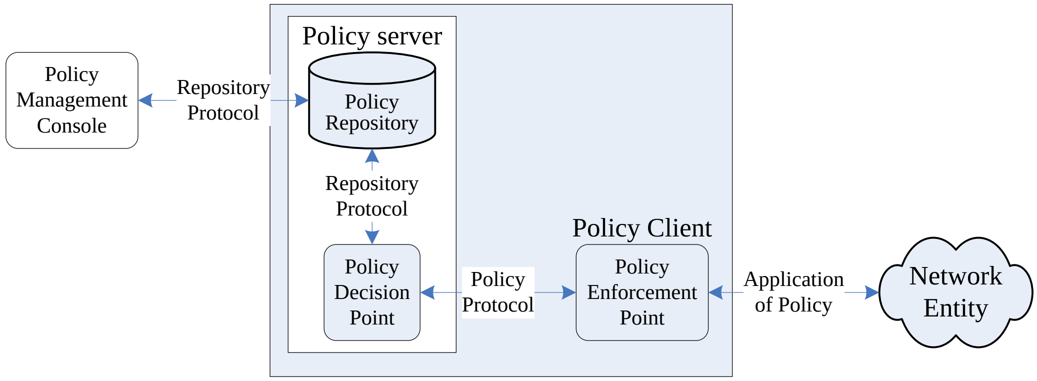

Figure 12.13: A Logic Architecture for PBNM

- **Policy Repository**: A database that stores the policy rules, their conditions and actions, and related policy data. It can also be defined as a model abstraction representing an administratively defined, logical container for reusable policy elements.
- **Policy Decision Point (PDP)**: A logical process that makes decisions based on the policy rules and the conditions under which the policy rules are applied.
- **Policy Enforcement Point (PEP)**: A logical entity that executes policy decisions and/or makes a configuration change.
- **Policy communication protocols**: Needed for data exchange between entities in the policy management system. The Common Object Policy Service Protocol (COPS) is often mentioned to support the communication between the PDP and the PEP.

7 Conclusion

In this chapter, after a brief introduction of the network management system, the evolution of two most widely used network management standards, SNMP and RMON, is reviewed along with the rapid development in computer and communication networks, including wireless networks. As a promising solution for the next generation network management, the architecture of PBNM has also been briefly discussed. The popularity of SNMP and RMON is largely due to their simplicity in architecture and implementation. However, the simplicity has its price, the versatile expertise required for the administrators and the reality that even a slight change in business policy may require complex development at lower layers, prevent these standards from further development.

To overcome these disadvantages, PBNM is proposed to ensure efficient network management and smooth network services upgrade. Although PBNM is still not fully mature yet, the promising features make it very appealing and convincing for a gloomy future.

8 Glossary

Account management One of the five OSI systems management functional areas. Consists of facilities that enable cost allocation based on the use of network resources.

Common Management Information Protocol (CMIP) An object-oriented OSI standard management protocol.

Configuration management One of the five OSI systems management functional areas. Consists of facilities that set and change the configuration of networks and network components.

Fault management One of the five OSI systems management functional areas. Consists of facilities that detect, isolate and correct the abnormal operation of the OSI environment.

HMAC protocols Message authentication protocols used for the authentication scheme in security management. It is based on hashing algorithm, to derive the message access code (MAC). Two common algorithms used in SNMP security management are HMAC-MD5-96 and HMAC-SHA-96.

Managed object A network device that can be managed remotely by a network management system.

Management Information Base (MIB) An abstract definition of the management information available through a management interface in a system.

Network management system (NMS) The platform that houses the network manager module. It monitors and controls the network components from a centralized operation.

Network monitoring Network monitoring describes the use of a system that constantly monitors a computer network for slow or failing systems and that notifies the network administrator in case of outages via email, pager or other alarms.

Network scanner Network scanner describes the systems used to check network system, operating system and applications running on your network to identify vulnerabilities and possible security flaws that could expose your network to security compromise.

Packet filter A packet filter determines if a packet is allowed to go through a given point based on certain access control policies.

Performance management One of the five OSI systems management functional areas. Consists of facilities that evaluate the behavior of managed objects and the performance of network activities.

Policy-based network management (PBNM) Manages the configuration and behavior of networks based on business needs and policies.

Remote Network Monitoring (RMON) Remotely monitoring the network with a probe.

Security management One of the five OSI systems management functional areas. Consists of facilities that provide security services essential to operate OSI network management correctly and to protect managed objects.

Simple Network Management Protocol (SNMP) An application layer protocol that facilitates the exchange of management information between network devices.

Structure of Management Information (SMI) Defines managed objects and their characteristics, as well as the relationship between the objects.

Trap An alarm or an event generated by a management agent and sent in an unsolicited manner to a network management system.

User-based access control model (UACM) The access control scheme defined in SNMPv3. It is more secure and flexible than the simple access policy defined in SNMP.

9 Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments. This research was partially supported by the US National Science Foundation under grants CNS-0716039, CNS-0848569, CNS-0845812, and CNS-0746811.

References

[1] Cisco Systems. Network management basics. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm, February 2002.

[2] M. Subramanian. *Network Management - Principles and Practice*. Addison Wesley, 2000.

[3] A. S. Tanenbaum. *Computer Networks*. Prentice Hall, fourth edition, 2003.

[4] J. Case, M. Fedor, M. Schoffstall, and J. Davin. RFC1157: A Simple Network Management Protocol (SNMP). http://www.rfc-editor.org/rfc/rfc1157.txt, May 1990.

[5] K. McCloghrie and M. Rose. RFC1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II. http://www.rfc-editor.org/rfc/rfc1213.txt, March 1991.

[6] M. Rose and K. McCloghrie. RFC1155: Structure and Identification of Management Information for TCP/IP-based Internets. http://www.rfc-editor.org/rfc/rfc1155.txt, May 1990.

[7] V. Cerf. RFC1052: IAB Recommendations for the Development of Internet Network Management Standards. http://www.rfc-editor.org/rfc/rfc1052.txt, April 1988.

[8] V. Cerf. RFC1109: Report of the Second Ad Hoc Network Management Review Group. http://www.rfc-editor.org/rfc/rfc1109.txt, August 1989.

[9] J. Postel. RFC768: User Datagram Protocol. http://www.rfc-editor.org/rfc/rfc768.txt, November 1980.

[10] Hossein Bidgoli, editor. *The Handbook of Computer Networks*, volume 2, chapter TCP/IP Suite. John Wiley & Sons, Inc., 2006.

[11] W. Stallings. *SNMP, SNMPv2, SNMPv3 and RMON 1 and 2*. Addison Wesley, third edition, 1998.

[12] K. McCloghrie, D. Perkins, and J. Schoenwaelder. Structure of Management Information Version 2 (SMIv2). http://www.rfc-editor.org/rfc/rfc2819.txt, April 1999.

[13] International Organization for Standardization. Specification of Abstract Syntax Notation One (ASN.1). International Standard 8824, December 1987.

[14] J. Case, R. Mundy, D. Partain, and B. Stewart. RFC3410: introduction and applicability statements for Internet standard management framework. http://www.rfc-editor.org/rfc/rfc3410.txt, December 2002.

[15] D. Harrington, R. Presuhn, and B. Wijnen. RFC3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. http://www.rfc-editor.org/rfc/rfc3411.txt, December 2002.

[16] J. Case, D. Harrington, R. Presuhn, and B. Wijnen. RFC3412: Message Processing and Dispatching for the Simple Network Management Protocol (SNMP). http://www.rfc-editor.org/rfc/rfc3412.txt, December 2002.

[17] D. Levi, P. Meyer, and B. Stewart. RFC3413: Simple Network Management Protocol (SNMP) Applications. http://www.rfc-editor.org/rfc/rfc3413.txt, December 2002.

[18] U. Blumenthal and B. Wijnen. RFC3414: User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3). http://www.rfc-editor.org/rfc/rfc3414.txt, December 2002.

[19] B. Wijnen, R. Presuhn, and K. McCloghrie. RFC3415: View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). http://www.rfc-editor.org/rfc/rfc3415.txt, December 2002.

[20] H. Krawczyk, M. Bellare, and R. Canetti. RFC2104: HMAC: Keyed-Hashing for Message Authentication. http://www.rfc-editor.org/rfc/rfc2104.txt, February 1997.

[21] S. Waldbusser. RFC2819: Remote Network Monitoring Management Information Base. http://www.rfc-editor.org/rfc/rfc2819.txt, May 2000.

[22] S. Waldbusser. RFC1513: Token Ring Extensions to the Remote Network Monitoring MIB. http://www.rfc-editor.org/rfc/rfc1513.txt, September 1993.

[23] S. Waldbusser. RFC2021: Remote Network Monitoring Management Information Base Version 2 using SMIv2. `http://www.rfc-editor.org/rfc/rfc2021.txt`, January 1997.

[24] Virus Defence Bureau. eEye digital security retina security scanner. `http://www.virusdefence.com.au/eeye/eeye_retina.html`.

[25] V. H. MacDonald. The cellular concept. *Bell Systems Technical Journal*, 58(1):15–43, 1979.

[26] V. W. S. Wong and V. C. M. Leung. Location management for next-generation personal communications networks. *IEEE Communications Magazine*, 14:18–24, 2000.

[27] A. Bar-Noy, I. Kessler, and M. Sidi. Mobile users: To updae or not to update? *Wireless Networks*, 1:175–185, 1995.

[28] J. Zhang. *Handbook of Wireless Networks and Mobile Computing*, chapter: Location Management in Cellular Networks, pages 27–49. John Wiley & Sons, 2002.

[29] S. Ramanathan and M. Steenstrup. A survey of routing techniques for mobile communication networks. *Mobile Networks and Applications*, 1:89–104, 1996.

[30] C. Rose and R. Yates. Minimizing the average cost of paging under delay constraints. *Wireless Networks*, 1(2):211–219, 1995.

[31] J. C. Strassner. *Policy-Based Network Management - Solutions for the Next Generation.* Morgan Kaufmann Publishers, 2004.

[32] S. Erfani, V.B. Lawrence, M. Malek, and B. Sugla. Network Management: Emerging Trends and Challenges. *Bell Labs Technical Journal*, October-December 1999.

[33] Hewlett-Packard Company. A Primer on Policy-based Network Management. `http://www.openview.hp.com/Uploads/primer_on_policy-based_network_mgmt.pdf`, September 24 1999.

[34] A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry, and S. Waldbusser. RFC3198: Terminology for Policy-Based Management. `http://www.rfc-editor.org/rfc/rfc3198.txt`, November 2001.

10 Acronyms

ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
BS	Base Station
CBC	Cipher Block Chaining
CMIP	Common Management Information Protocol
CMOT	CMIP over TCP/IP
COPS	Common Object Policy Service Protocol
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Services
EGP	External Gateway Protocol
HLR	Home Location Register
HMAC	Hashed Message Authentication Code
IAB	Internet Architecture Board
IP	Internet Protocol
ISO	International Organization for Standardization
IV	Initialization Vector
MD	Message Digest
MAC	Media Access Control
MSC	Mobile Switching Center
MTU	Maximum Transmission Unit
MIB	Management Information Base
NMS	Network Management System
OSI	Open Systems Interconnection
PBNM	Policy-Based Network Management
PDP	Policy Decision Point
PDU	Protocol Data Unit
PEP	Policy Enforcement Point
QoS	Quality of Service
RFC	Request for Comments
RMON	Remote Network Monitoring
SGMP	Simple Gateway Monitoring Protocol
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SMI	Structure of Management Information
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLR	Visitor Location Register