

Overview of Network Management

By R VIJAYAN, Assistant Professor(Sr), SITE, VIT University

Network Management

- Network management is the process of controlling a complex data network to maximize its efficiency and productivity.
- The overall goal of network management
 - help with the complexity of a data network
 - to ensure that data can go across it with maximum efficiency and transparency to the users.

Network Management Requirements

- Ease of use
- Security features
- Restoral capability
- Ability to delete/add
- Ability to monitor network availability
- Traffic rerouting
- Improved automation
- User registration
- Improved reporting
- Ability to monitor response time
- Control corporate strategic assets
- Control complexity
- Improve service
- Balance various needs
- Reduce downtime
- Control cost

Network Management

- The ISO Network Management Forum divided network management into five functional areas:
 - Fault Management
 - Configuration Management
 - Accounting Management.
 - Performance Management
 - Security Management.

Fault Management

- The facilities that enable the **detection, isolation, and correction of abnormal operation** of the OSI environment
- What is “a fault”?
 - an abnormal condition that requires management attention (or action) to repair
 - indicated by failure to operate correctly or by excessive errors
 - Communication line is cut
 - A crimp in the cable
 - Certain errors may occur occasionally and are not normally considered to be faults
- When a fault occurs
 - Determine “exactly” where the fault is
 - Isolate the rest of the network from the failure
 - Reconfigure or modify the network to minimize the impact of operation
 - Repair or replace the failed components

User requirements for Fault Management

- Fast and reliable problem resolution
 - Receive notification and correct the problem immediately
 - Requires rapid and reliable fault detection and diagnostic management
 - Provides fault tolerance
 - Redundant components and alternate communication routes
 - Fault management capability itself should be redundant
- Keep informed of the network status
 - Reassurance of correct network operation through mechanisms that use tests or analyze dumps, logs, alerts, or statistics
- Problem tracking and control
 - Ensure the problem is truly resolved and no new problems are introduced
- Fault management should have minimal effect on network performance

Configuration Management

- The configuration of certain network devices controls the behavior of the data network.
- Configuration management is concerned with
 - Initializing a network
 - Gracefully shutting down part or all of the network
 - Maintaining, adding, and updating the relationships among components and the status of components themselves during network operation

Requirements for Configuration Management

- The network manager needs the capability to
 - Identify initially the components that comprise the network
 - Define and change the connectivity of components
 - Define and modify default attributes, and load the predefined sets of attributes into the specified network components
 - Reconfigure a network for performance evaluation, network upgrade, fault recovery or security checks
 - End users want to inquire about the upcoming status of resources and their attributes before reconfiguration
 - Generate configuration reports
 - Periodic basis
 - Response for a request
 - Only authorized end users can manage and control network operation (software distribution and updating)

Accounting Management

- Involves tracking individual's utilization and grouping of network resources to ensure that users have sufficient resources.
- Involves granting or removing permission for access to the network.
- The facilities that enable
 - charges to be established for the use of managed objects
 - costs to be identified for the use of those managed objects
- Network managers track the use of network resources by end user or end-user class
 - An end user or group of end users may be abusing its access privileges and burdening the network at the expense of other users
 - End users may be making inefficient use of the network, and network manager can assist in changing procedures to improve performance
 - The network manager is easier to plan for network growth if end user activity is known in sufficient detail

By R VIJAYAN, Assistant Professor(Sr), SITE, VIT University

Requirements for Accounting Management

- The network manager can specify
 - the kinds of accounting information to be recorded at various nodes
 - the desired interval between sending the recorded information to higher-level management nodes
 - the algorithms to be used in calculating the charging
- Generate accounting reports
- Provide the capability to verify end users' authorization to access and manipulate the information

Performance Management

- Involves measuring the performance of the network hardware, software and media.
- The facilities needed to evaluate
 - the behavior of managed objects
 - the effectiveness of communication activities
- Functions of performance management
 - Monitoring
 - Tracks activities on the network
 - Controlling
 - Enables performance management to make adjustments to improve network performance
- Examples of measured activities are:
 - Overall throughput.
 - Percentage utilization.
 - Error rates.
 - Response time.

Issues of Performance Management

- What is the level of capacity utilization?
- Is there excessive traffic?
- Has throughput been reduced to unacceptable levels?
- Are there bottlenecks?
- Is response time increasing?

To deal the issues of PM

- The network manager focus on some initial set of resources to be monitored in order to assess performance levels
 - Appropriate metrics and values with relevant network resources as indicators of different levels of performance
 - The count of retransmission on a transport connection
 - Monitor many resources to provide information in determining network operating level
 - Collect and analyze information, and then using the resultant analysis as feedback to the prescribed set of values

User Requirements for Performance Management

- End users want to know
 - the average and worst case response times
 - the reliability of network services
- Performance statistics can help managers
 - Plan, manage and maintain large networks
 - Recognize potential bottlenecks in advance
 - balance or redistribute traffic load by changing routing tables

Security Management

- It is the process of controlling access to information on the data network.
- The facilities that address those aspects of OSI security essential to
 - Operate OSI network management correctly
 - Protect managed objects
 - network resources
 - end user information
- End users want to know
 - the proper security policies are in force and effective
 - the management of security facilities is itself secure
- Provides a way to monitor access points and records information on a periodic basis.
- Provides audit trails and sounds alarms for security breaches.

Issues of Security Management

- Managing information protection, and access control facilities
 - Generating, distributing and storing **encryption keys**
 - Passwords, authorization or access control information must be maintained and distributed
- Monitoring and controlling access to computer networks and to all or part of the network management information
 - SM involves with the collection, storage, and examination of **audit records and security logs**
 - the enabling and disabling of these logging facilities

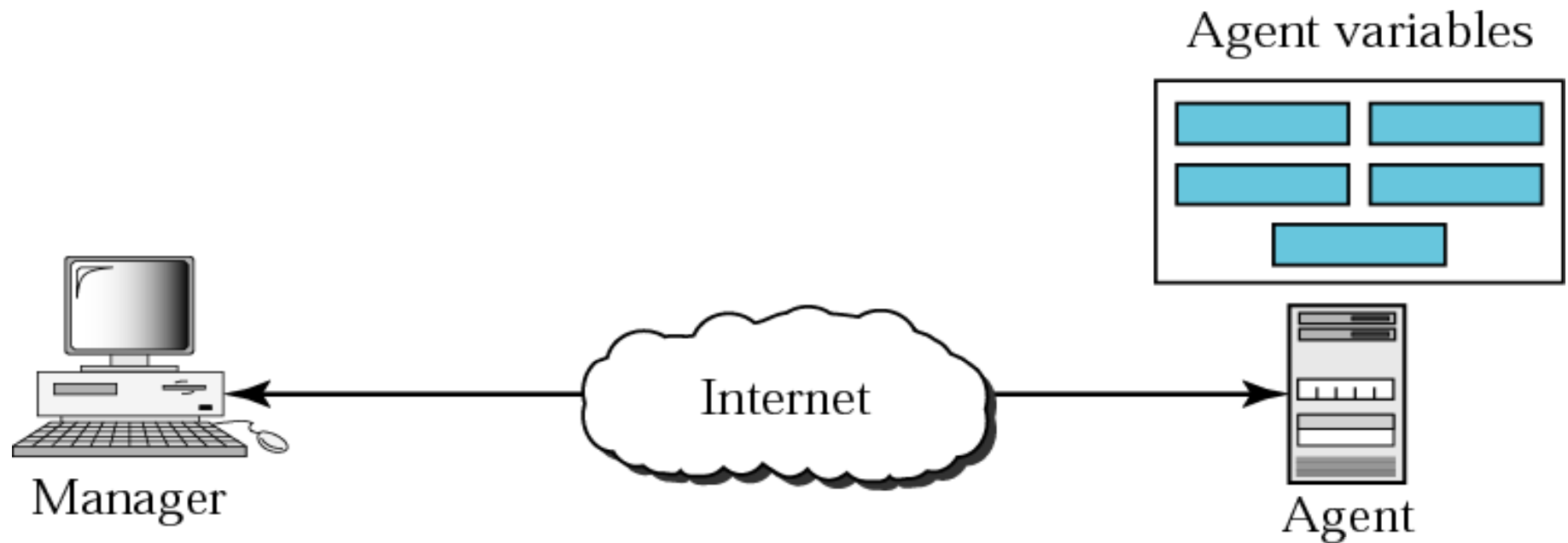
SNMP - Objectives

- A framework for managing devices in an internet using TCP/IP.
- Provides a set of fundamental operations for monitoring and maintaining an internet.
- An application-level protocol allows it to monitor devices made by different manufactures installed on different physical networks.
- Simple Network Management Protocol
 - Provides a tool
 - for multi-vender, interoperable network management
 - used across a broad spectrum of product types
 - include end systems, bridges, switches, routers and telecommunications equipment
 - TCP/IP based
- A set of standards for network management
 - a protocol
 - a data base structure specification
 - a set of data objects

SNMP Family

- SNMPv1
 - Proposed in 1989
- SNMPv2
 - Proposed in 1993
 - Revised in 1995
 - An upgrade to SNMPv1
 - Add functional enhancements to SNMP and codify the use of SNMP on OSI-based networks
- SNMPv3
 - Issued in 1998
 - Define a security capability for SNMP and an architecture for future enhancements
 - Used with the functionality provided by SNMPv2 or SNMPv1

SNMP Concept



Agent & Manager

- Agent:
 - A router or host that runs the SNMP server program.
 - Keep performance information in a database.
 - Can send a trap to the manager if something unusual occurs.
- Manager:
 - A host that runs the SNMP client program.
 - Has access to values in the agents database.

Based on three basic ideas

- A manager checks an agent by requesting information that reflects the behavior of the agent.
- An manager forces an agent to perform a task by resetting values in the agent database.
- An agent contributes to the management process by warning the manager of an unusual situation.

Management Components

- SNMP uses two other protocols
- SMI-Structure of Management Information
- MIB-Management Information Base

Role of SNMP

- SNMP defines the format of packets exchanged between a manager and an agent.
- It reads and changes the status (values) of objects (variables) in SNMP packets.

Role of SMI

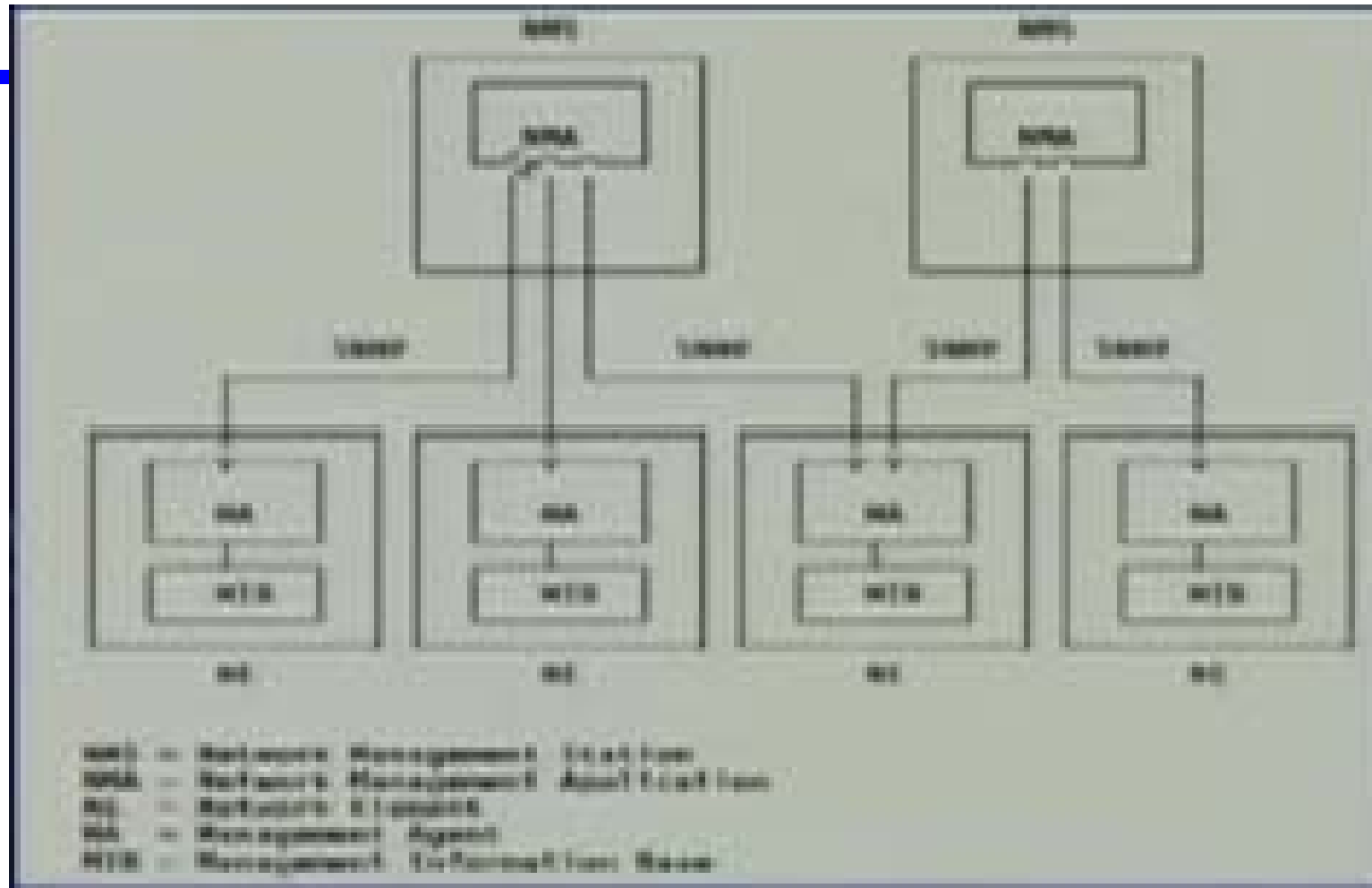
- It defines the general rules for
 - naming objects,
 - defining object types (including range and length)
 - showing how to encode objects and values.
- It does not defines
 - number of objects an entity should manage
 - names the objects to be managed
 - the association between the objects and their values.

Role of MIB

- MIB creates a collection of named objects, their types and their relationships to each other in an entity to be managed.

SNMP

- A group was formed and their efforts were complete in early 1993.
- There are 12 documents describing SNMPv2
- There are 3 basic commands that are used with SNMP;
 - GetRequest
 - SetRequest
 - Get NextRequest or notify



By R VIJAYAN, Assistant Professor(Sr), SITE, VIT University

SNMP

- There are two approaches for the management system to obtain information from SNMP
 - Traps
 - Polling

SNMP Traps

- Traps are unrequested event reports that are sent to a management system by an SNMP agent process
- A trap will contain
 - Network device name
 - Time the event happened
 - Type of event
- When a trappable event occurs, a trap message is generated by the agent and is sent to a trap destination (a specific, configured network address)
- Many events can be configured to signal a trap, like a network cable fault, failing NIC or Hard Drive, a “General Protection Fault”, or a power supply failure.

SNMP Traps

- Traps can also be throttled – you can limit the number of traps sent per second from the agent.
- Traps have a priority associated with them – Critical, Major, Minor, Warning, Marginal, Informational, Normal, Unknown.
- Resources are required on the network device to generate a trap.
- When a lot of events occur, the network bandwidth may be tied up with traps.
- Because the network device has a limited view, it is possible the management system has already received the information and the trap is redundant.

SNMP Polling

- The network management system periodically queries the network device for information.
- The advantage is the network management system is in control and knows the “big picture”.
- The disadvantage is the amount of delay from when an event occurs to when it’s noticed.
 - Short interval, network bandwidth is wasted.
 - Long interval, response to events is too slow.

SNMP Traps/Polling

- When an event occurs, the network device generates a simple trap.
- The management system then polls the network device to get the necessary information.
- The management system also does low frequency polling as a backup to the trap.