NETWORK MANAGEMENT

Habib Youssef, Ph.D

youssef@ccse.kfupm.edu.sa
Department of Computer Engineering
King Fahd University of Petroleum & Minerals
Dhahran, Saudi Arabia

Computer Networks, February 19 - 23, 2000

Introduction

- Once you have a network, you must see that you have the right combination of People, Tools, Systems, and Procedures to be able to
  - » **operate the network**, and
  - » **plan and implement needed upgrades**

Why?

- Computer networks have become mission critical.
- Cost of a network downtime has become prohibitive.
- To minimize network management overhead.

Goals of Network Management

- To ensure a uniform and standard ways of information manipulation
- To share resources, hardware and software (data and programs)
- To maximize the network reliability, security, accessibility, and serviceability to the end users.

Rationale for Network Management

- Network management
  - » is goal oriented
  - » covers personnel, procedures, programs, and technical systems
  - » concerns operations and planning
  - » equipment configuration
  - » transmission media

Rationale for Network Management (contd.)

- Determine operational status of equipment and transmission facilities.
- Obtain visual/audible notification of the occurrence of threshold conditions.
- Better manage large and complex networks.
- Cope with network device sophistication.
- Facilitate configuration changes.
- Make more efficient use of personnel resources.
- Balance network performance and capacity.
- Contain operating costs.

Network Assessment

- Configuration ==> It works.
- Fault ==> It works consistently.
- Performance ==> It works well.
- Security ==> It works securely.
- Accounting ==> It works optimally.

Quality of Service Parameters

- Quantitative
  - » Availability
  - » Response time
  - » Throughput
  - » Utilization
  - » Etc.

Quality of Service Parameters (contd.)

- Qualitative
  - » Flexibility in the face of change
  - » Security
  - » User friendliness

Network Management

- It is the process of using hardware and software by trained personnel to
  - monitor the status of network equipment and transmission facilities;
  - question end users, vendors, and communication carrier personnel;
  - implement / recommend actions to alleviate outages and/or improve communication performance;
  - conduct administrative tasks associated with the operation of a network.

Minimum skills required

- Workstation hardware knowledge
- Network operating system
- Device drivers
- Equipment configuration
- Transmission media

ramework for Network Management

- Configuration/Change Management
- Fault/Problem Management
- Performance/Growth Management
- Security/Access Management
- Accounting/Cost Management

Configuration/Change Management

- This is the process of keeping track of the various parameters of devices and facilities that make up a network.
- Parameters can be
  - » set
  - » reset or
  - » read and displayed.

Configuration Management (contd.)

- Configuration management includes
  - » Address and name assignment to network devices (bridges, switches, routers, etc.)
  - » Hardware / Software updates to network devices
  - » Setting parameters of network devices e.g.,
    - Ð filtering of certain traffic (by type or address)
    - Ð Enable selected protocols for multiprotocol routers

Configuration Management (contd.)

- Some network devices need more effort to configure than others
  - » Transparent Bridges are plug-and-play
  - » Source Routing Bridges require some configuration
    - Bridges may need to be numbered
    - MAC addresses may be locally assigned

Configuration Management (contd.)

- Routers require much more effort to configure
  - Network addresses have to be assigned to each interface
  - Some protocols must be enabled (e.g. RIP)
  - A number of other parameters must be set by network administrator (defaults are available)
- Workstations and servers may also need configuration

Configuration Management (contd.)

- Configuration may be done by several means
  - » a console directly attached to the device
  - » remote login across the network
  - » network management system

Fault/Problem Management

- This is the process by which the detection, logging and ticketing, isolation, tracking and eventual restoration of abnormal conditions is accomplished.
  - » Detect the fault (via threshold settings, users calling etc.)

Fault/Problem Management (contd.)

- Once a problem is detected, many installations will have a predefined operating procedure whereby
  - the situation is recorded in a log
  - if determined to be a legitimate problem assigned a Trouble Ticket
- Problem isolation may require
  - simple discussion with a user
  - diagnostic testing of equipment or
  - extensive research

Fault/Problem Management (contd.)

- It is important also to track progress of both internal and external personnel in their efforts toward correcting faults.
  - It is important to track problems, including the status of trouble tickets.

Performance/Growth Management

- Involves tasks required to evaluate network resources utilization and adjust them as required.
- Another term used to refer to this discipline is Capacity Planning

erformance/Growth Management(contd.)

- One interesting aspect of capacity planning concerns the reaction of end users to capacity problems.
  - » **Insufficient capacity**
    - Dtriggers end-user complaints
  - » But **excess capacity** detection
    - Dis incumbent upon management personnel.

Performance/Growth Management(contd.)

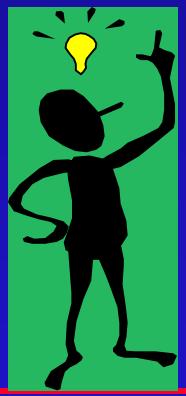
- Variety of tools for this activity :
  - » Communications carrier bills
  - » Network management systems
  - » Protocol analyzers
  - » Traffic generators
  - » Test equipment

Performance/Growth Management(contd.)

- Statistics and Event collection
  - » Current status of links (up/down)
  - » Errors on each incoming link
  - » Retransmissions on each outgoing link
  - » Packets sent and received on each link
  - » Traffic volume per source/destination
  - » Etc.

Performance/Growth Management(contd.)

- Statistics collected can help determine the nature of the problem.
- Example:



The problem must be due to improper setting of retransmission timers rather than a bad link

Security/Access Management

- It is that set of tasks that ensure that only authorized personnel can use the network.
- Security management includes:
  - Confidentiality
  - Integrity
  - Authentication
  - Access control
  - Nonrepudiation

Security/Access Management(contd.)

- Vulnerabilities include:
  - Wiretaps placed on cables
  - Outsiders dialing into the system
  - Remote login attempts
  - Introduction of a virus
- Security protection mechanisms include:
  - Encryption
  - Physical protection
  - Access control lists
  - Dial-back modems
  - Audit data collection

Security/Access Management(contd.)

- Security management tasks include:
  - authentication of users
  - encryption of data links
  - management and distribution of encryption keys Maintenance and examination of security logs.
  - Performance of audits and traces to ensure that only authorized users use network facilities & resources.
  - Virus protection.
  - Disaster recovery methods.

Accounting/cost Management

- Accounting/cost Management
  - » May be for billing for network usage.
- Accounting parameters include:
  - » The number of connections made
  - » The duration of each connection
  - » The number of email messages sent and received
  - » Traffic volumes sent and received
  - » The resources accessed across the network
- Accounting management may also place limits on the use of network resources

mary of Network Management Functional Areas and Tasks

Configu-ration/ Change Mana-gement

- Network status monitoring
- Network routing
- Parameter database
- Configurat-ion control
- Facility control

Fault/ Problem Manag-ment

- Event Notification
- Logging
- Ticketing
- Tracking
- Isolation
- Resolution

Perfor-mance/ Growth Manag-ement

- Monitoring
- Statistical analysis
- Database generation and analysis
- Reporting
- Tuning

Security /Access Manag-ement

- Authenticat-ion of users
- Maintaining security
- Encryption
- Key Distribution
- Audits
- Traces

Account -ing Cost Manag-ement

- Issue orders
- Recording
- Reconciliatio n of invoices
- Developmen t of cost algorithms
- Assignment of costs

Asset Manag-ement

- Equipment records
- Facility records
- Personnel records
- Training

Plann-ing Support Manag-ement

- Data collection
- Requirements analysis
- Trend analysis
- Modeling
- Design
- Optimization
- Implementation

active vs. Reactive Management

- **Reactive management** is similar to **Fire Fighting**.
- **Proactive management** is the process of **network monitoring to anticipate and resolve problems before they turn into a fire**.
  - » This is where a network administrator should spend most of his time.

Why ?!!

- Proactive management
  - » prepares you well for the fire.
  - » Enables you to plan your network
  - » Gives you time to breathe
- Some fire fighting is inevitable.
  - » Goal is to minimize the flames and keep you sane and better able to provide consistent quality for network users.

Proactive Management

- **Monitor state** of the network by using network management tools.
- **Keep statistics** over time and generate reports that give you idea as to how the network is doing and when it is time to upgrade and what to upgrade.
- **Maintain configuration records** and scripts that make it easy to recover when problems arise, enabling rollback to a known state, or setting up a replacement network device quickly.

Network Management

O r

- The operation of a large network requires the creation of an organization structure. Namely, the following points must be controlled
  - » Authority to recommend
  - » Arbitration
    - Dto mediate differences of opinion which affect network operation
  - » Preparation of information
  - » Contact persons/address

Organizational Aspects

- In general, the overall organization of network/ system administration tasks can be subdivided by
  - » department
  - » functional areas
  - » geographic areas
- A network primary goal is to distribute resources to various work areas.

Organizational Aspects (contd.)

- It is possible to construct a matrix of resource types and their associated tasks:
  - Hardware
    - Planning, selection, procurement, operation
    - Upkeep and adaptation to local needs and developments
    - Measurement of operational characteristics and evaluation
  - System Software (idem as above)
  - Application Software (idem as above)

Organizational Aspects (contd.)

- Operations Unit:
  - Application and system management
  - Configuration management
  - Fault management
  - User administration
  - Documentation
  - Monitoring and control

Organizational Aspects (contd.)

- Planning Unit:
  - Monitor current network activities
  - Understand / Consider environmental constraints
  - Forecast future needs and technology
  - Evaluate technical opportunities
  - Create most appropriate, consistent, and coordinated plans on long, medium, and short term basis
  - Adjust plans based on results of actual implementations

Organizational Aspects (contd.)

- Adequate network operation and planning require that you have the right combination of
  - People
  - Tools and Systems
  - Procedures

People

- People
  - They are the hardest thing to find. There are not that many trained network management personnel.
  - Most organizations adopt the approach of training their own network managers. They take from within the company those people who have aptitude for the technicalities of the job and feed them through training courses, both public courses and those run be their network suppliers.

People (contd.)

- They also provide on-the-job training and expose the people selected to network management centers in other organizations.

Tools and Systems

- The equipment required in a network management center includes :
  - » Testing equipment used for diagnosing faults
  - » Reconfiguration equipment such as patching facilities and switching facilities so that the network can be reconfigured in the event of faults.

Tools and Systems (contd.)

- Diagnostic tools to detect problems with the media
  - » Time Domain Reflectometers (TDRs)
  - » Breakout Boxes
  - » Pattern generation
  - » Bit error rate testers
  - » Generate alarm on the occurrence of an event ==> This is another type of diagnostic tool.

Tools and Systems (contd.)

- Monitoring tools
  - » Used to observe & measure operation/ performance of the network.
    - Examples :
      - RMON probes
      - Protocol Analyzers
      - Equipment indicators
      - Breakout boxes
  - » Most monitoring tools can also be used as diagnostic tools.

Tools and Systems (contd.)

- Computer-Based Management Systems
  - » Store operational information about the network in database so that it can be queried and manipulated.
  - » Store information about past problems, trouble tickets
  - » Tools for project planning, network design

Tools and Systems (contd.)

- General observations concerning computer based management systems:
  - » We can segregate their general use into
    - Ð operational functions
      - They are internal for the organization using them with respect to operational aspects
    - Ð planning functions
      - In contrast, many organizations use the services of third party vendors to access computer-based management systems to use network planning software.

Procedures

- Procedures
  - » A philosophy comprised of **Rules and Regulations** to control the acquisition, installation, inventory, and monitoring of data transfer hardware and software components.

Network Management Team

- Goals
  - To ensure that the network is functioning at its best.
  - To protect the network resources from loss or misuse.
  - To ensure that the network users follow the guideline set by management.

Tasks of Management Team

- Configure the network in terms of hardware and software.
- Establish and implement work procedures.
- Add/Remove users and applications.
- Monitor the network operations and security.

Tasks of Management Team (contd.)

- Plan network growth.
- Perform data backup.
- Keep as much as possible up-to-date documentation about the network
  - **Physical topology**
  - **Configuration records**
  - a log of the problems encountered and their solutions.
  - Etc.

Network Control Hierarchy

Members of Management Team

- Administrator:
  - » Assign groups and group managers.
  - » Define/Plan/Schedule various management tasks (configuration, documentation, fault, performance, etc.).
  - » Develop and implement management procedures
- Assistant Administrator
  - » Deals with end user problems.

Members of Management Team (contd.)

- Group Managers:
  - » Add/Remove users and maintain the disk area for their respective groups
  - » Perform various management tasks to ensure adequate services to the group.
- Operators:
  - » Cater to end-users requests.
  - » Assist group managers in carrying various network management tasks.

Network Management Protocol (SNMP)

- To insure inter-operability of network management systems vendors are committing themselves to support network management standards
- SNMP (Simple Network Management Protocol) is the de facto standard for managing multi-vendor equipped Enterprise networks

SNMP (contd.)

- SNMP dates back to 1988.
- SNMP parallels the evolution of the TCP/IP protocol suite.
- A desire to monitor the performance of protocol gateways linking individual networks to the Internet resulted in the development of the Simple Gateway Monitoring Protocol (SGMP), which can be viewed as the predecessor of SNMP.

SNMP (contd.)

RFC 1065 Structure and Identification of Management Information for TCP/IP based internets.

RFC 1066 Management Information Base for Network Management of TCP/IP-based internets.

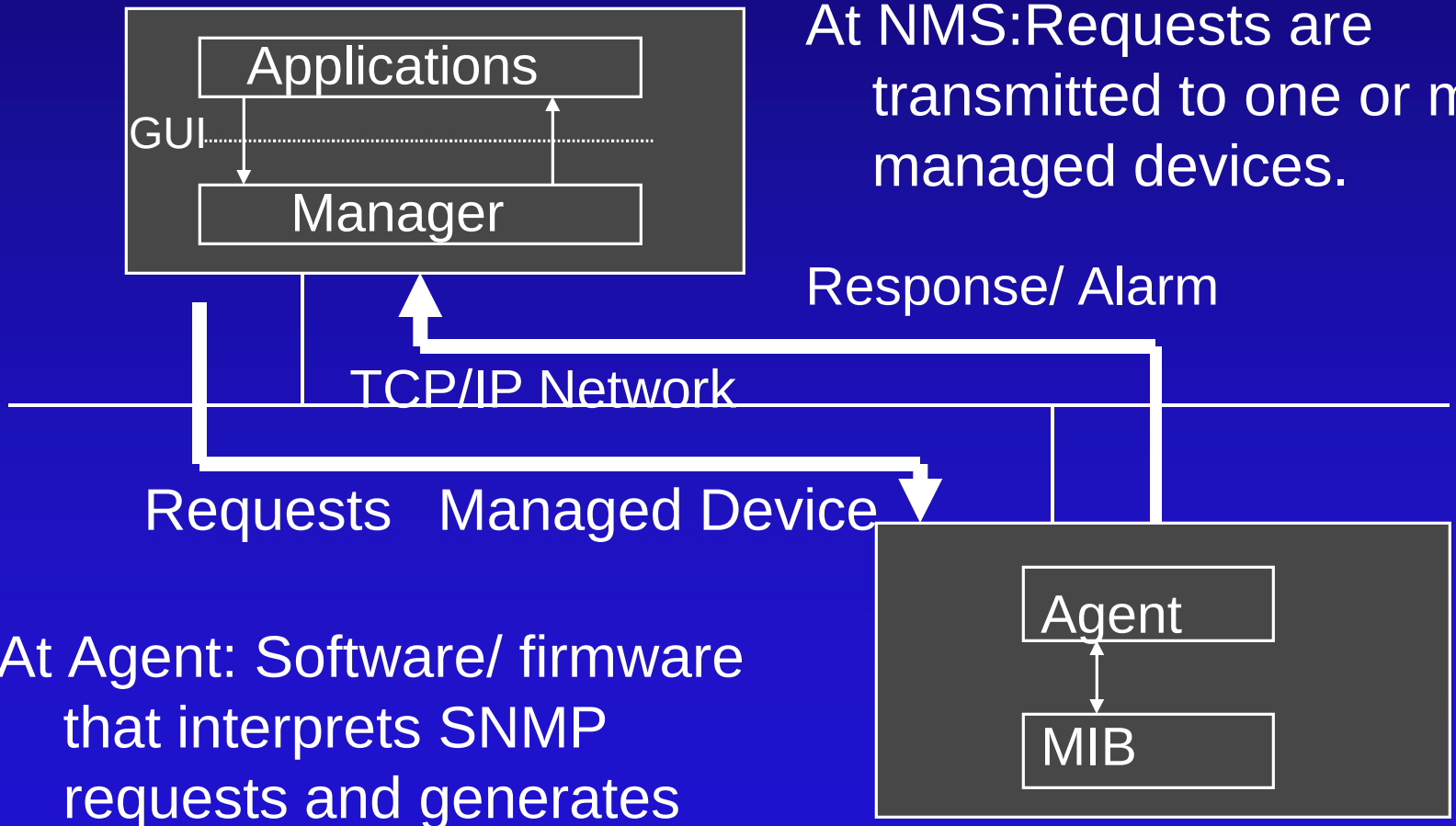
RFC 1067 A Simple Network Management Protocol.

SNMP (contd.)

- SNMP uses a simple protocol stack (SNMP over UDP over IP)
- It uses a simple set of commands and responses
  - » get to read device variable
  - » set to write a device variable
  - » trap -- an unsolicited notification of an even
- It is simple for the managed device to support
- Supported by most network management platforms

SNMP (contd.)

Network Management Station (NMS)



At NMS:Requests are transmitted to one or more managed devices.

Response/ Alarm

At Agent: Software/ firmware that interprets SNMP requests and generates responses

SNMP : Basic Architecture

- Manager : Client Program
- Agent : Sever running on remotely controlled device
- Database : Management Information Base (MIB)
- SNMP : Protocol which governs the information transfer for among the three components.

SNMP (contd.)

- Although SNMP is primarily a POLL-RESPONSE protocol
  - » Requests generated by the manager
  - » Responses sent by agents

  The agent has also the ability to initiate unsolicited response which is an alarm condition resulting from the agent monitoring a predefined activity which has crossed a pre-specified threshold.

  In SNMP terminology => ALARM => TRAP

MIB

- Each managed device has a variety of
  - » configuration,
  - » states and
  - » statistical information

  which define its functionality and operational capability.
- Collectively, these data elements constitute the MIB of the managed device

MIB (contd.)

- Each variable data element is a managed object and consists of :
  - » name
  - » one or more attributes and
  - » a set of operations that can be performed on the object.

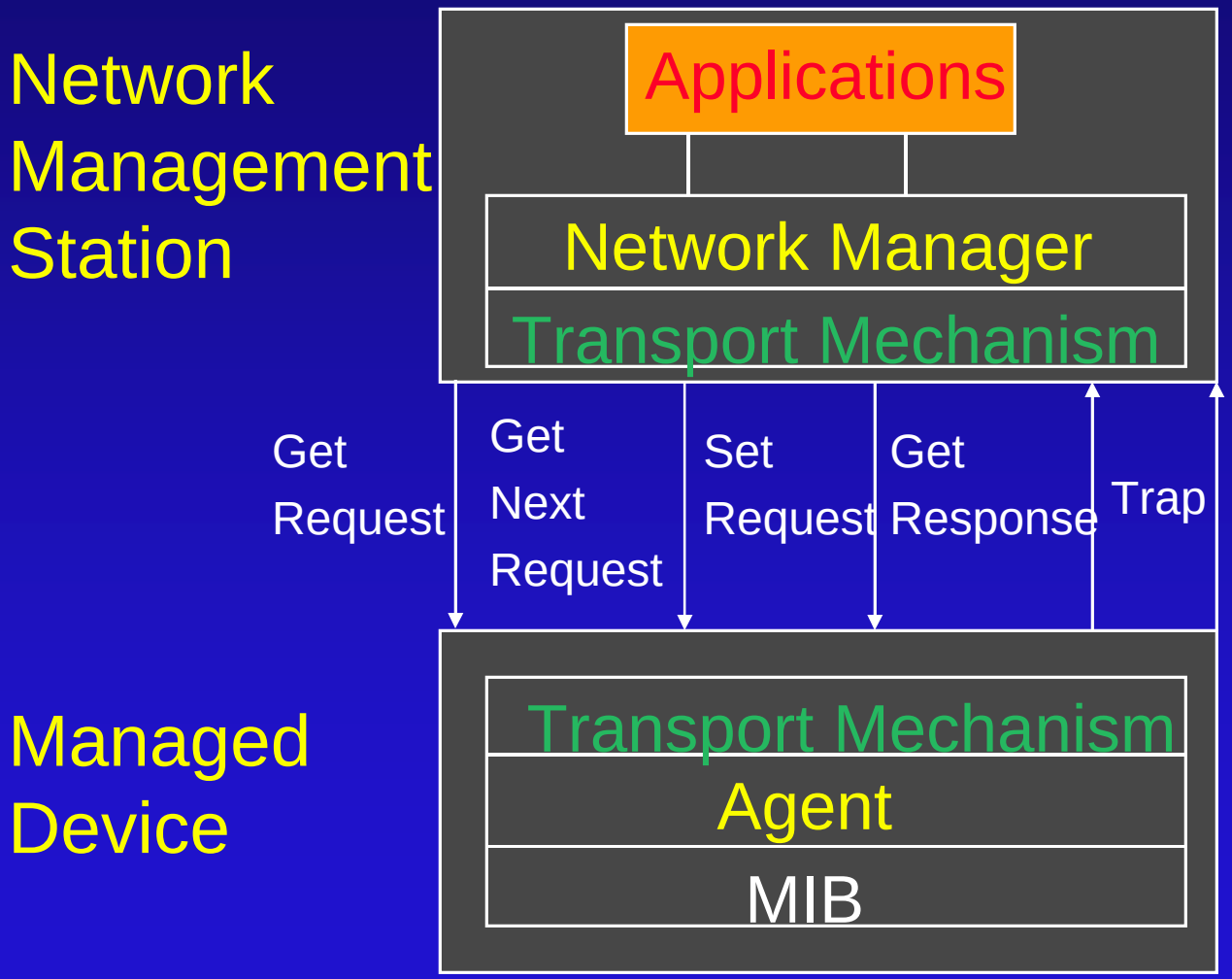
SNMP Commands

Commands	Operational Result
GetRequest	Requests the values of one or more Management Information Base (MIB) variables.
GetNextRequest	Enables MIB variables to be read sequentially, one variable at a time.
SetRequest	Permits one or more MIB values to be updated

SNMP Commands (contd.)

Commands	Operational Result
GetResponse	Used to respond to a GETRequest, GetNextRequest, or SetRequest.
Trap	Indicates the occurrence of a predefined condition.

SNMP version 1 command flow



RMON

- Main problem with SNMP is the Request-Response operations.
  - » Has minor effect on bandwidth utilization in a LAN.
  - » Can result in significant degradation of lower operating rate WAN bandwidth when monitoring geographically separated networks.

RMON (contd.)

- Recognizing this problem, the Remote Network Monitoring working group of the IETF developed the Remote Monitoring (RMON) network management standard
- RMON represents an extension of the network manager's operation to distant networks.

RMON (contd.)

- At remote networks, intelligent devices known as probes or RMON agents monitor the traffic flow on the remote network, organizing it into information the manager can easily access and interpret, with SNMP used as the transport mechanism between the manager and agent.

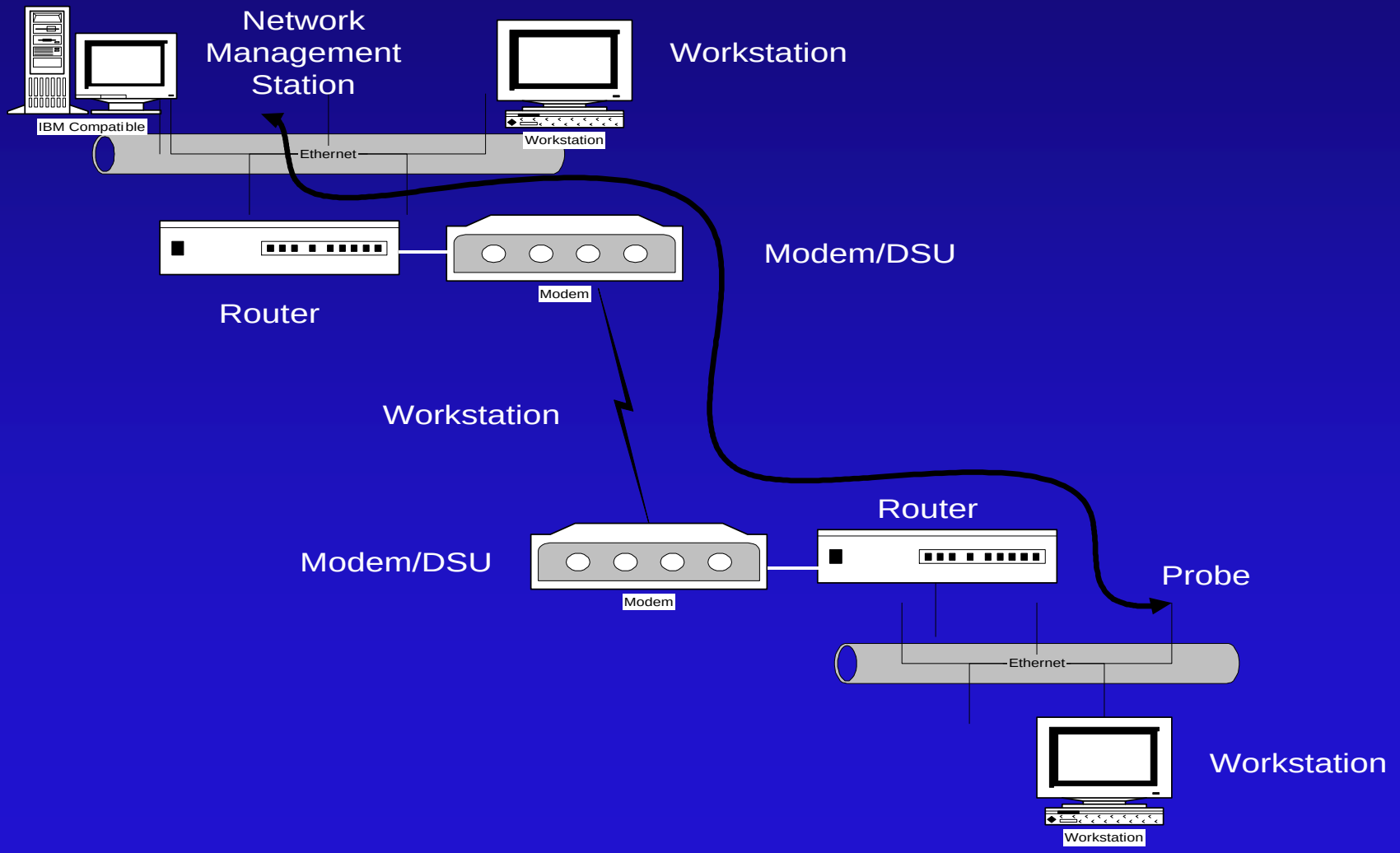
RMON (contd.)

- The first RMON MIB, RFC 1271,was published in Nov. 1991, and was limited to Ethernet LANs.
- RFC 1513 published is September 1993, extended RMON to Token Ring.
- Extensions to other networks followed later to include other networks such as ATM.

RMON (contd.)

- No need to poll individually each device on remote network.
- Each RMON agent or probe includes as MIB that defines the attributes of the objects being monitored.

RMON Probe



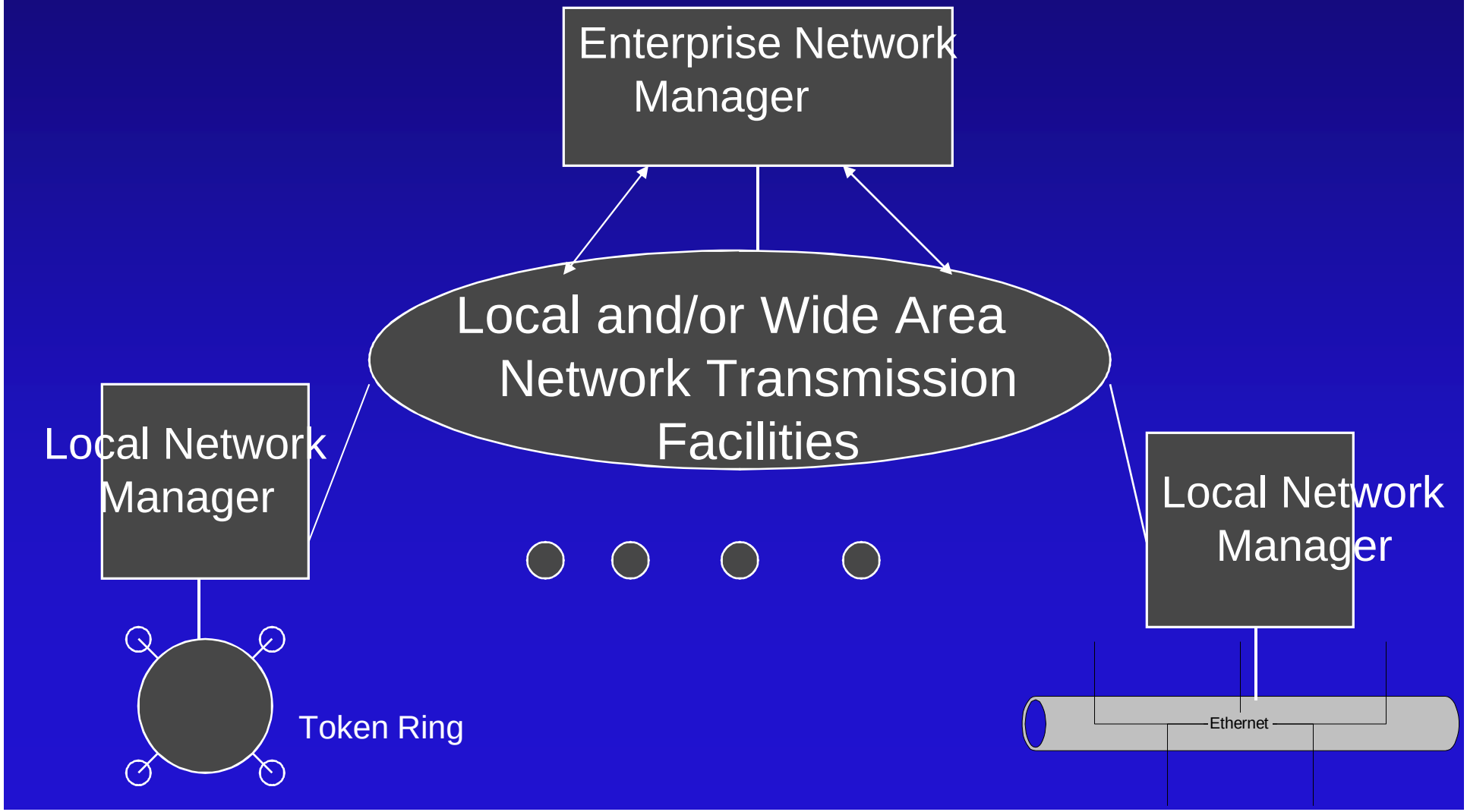
SNMPv2

- SNMPv2 is an extension of SNMPv1
  - » Adds security
  - » Allows get to access larger data elements
  - » Supports the concept of a hierarchy of Network Management Stations
  - » Other enhancements

SNMPv2 (contd.)

- InformRequest
  - » Provides SNMPv2 with the ability to support a hierarchy of network management stations
  - » The use of this command enables one management station to communicate with another management station, a feature not support under SNMPv1.

SNMPv2 (contd.)



OSI Network Management

- OSI network management is much more complex than SNMP
  - A more comprehensie command set than Get, Set, and Trap
  - A more comprehensive MIB
  - Provides a broad and general framework for looking at network management
- Protocols of OSI network management are
  - Common Management Information Service (CMIS)
  - Common Management Information Protocol (CMIP)
  - Remote Operations Service Element (ROSE)
  - The Directory Service (X.500)

Contrasting CMIP with SNMP

- CMIP and SNMP are supported by different standard committees
- They differ in the way they retrieve and report data across the network
- The two protocols
  - » offer different functions,
  - » make use of a different set of lower level protocols to send and receive management information, and
  - » require different amounts of processing power.

Contrasting CMIP with SNMP (contd.)

- Data Access
  - SNMP and CMIP have different data retrieval functions
  - SNMP is better at accessing individual items of information while CMIP is oriented more toward retrieving collections of information
    - Wit SNMP, you ask for the paricular item you want
    - CMIP requires you to make a general request and then qualify that request with specifics about what you dong want
    - SNMP operates in a more focused manner, while CMIP deals with classes of data that you constrain with stated qualifications

Contrasting CMIP with SNMP (contd.)

- Polling vs. Reporting
  - SNMP works by polling a central management processor (such as a workstation), thus asking regularly each device on the network for its status.
  - CMIP uses reporting, where the device only informs the central management station about changes in the device status.
  - With the SNMP approach, a large number of network devices will cause a great deal of network traffic.
  - However, with SNMP you can have on the network devices that are not intelligent enough to detect and report problems.
  - SNMP makes it simpler to detect a device that has failed completely and that is unable to report its failure.

Contrasting CMIP with SNMP (contd.)

- Size and Performance
  - A network management system built on SNMP is smaller, faster, and less expensive than a CMIP implementation.
  - CMIP requires a faster machine and more memory (polling requires less intelligence from the managed device than does reporting).
  - CMIP is broader in scope and has more features/capabilities.

Contrasting CMIP with SNMP (contd.)

- Transport Protocols
  - SNMP uses simple datagrams to communicate management information
    - connectionless and no guarantee of delivery
    - SNMP rides on UDP
  - CMIP relies on connection oriented sessions
    - this approach is more suitable for retrieving large volumes of data

Contrasting CMIP with SNMP (contd.)

- Protocol Standards
  - » CMIP is an OSI protocol of ISO.
  - » In contrast, SNMP is not an international standard. SNMP, like other TCP/IP protocols is controlled by the Internet Activities Board.
- SNMP is older and widely supported by network equipment vendors; CMIP has not been implemented in as many products.

Which to choose, CMIP or SNMP?

- SNMP is more oriented toward managing specific devices, while CMIP is better at communicating information between two or more network management systems.
- SNMP and CMIP play complementary roles; depending on the size of the network, itmay be best to adopt a network management system that uses both.
  - » SNMP is used to manage specific LANs
  - » CMIP is used to manage a WAN of LANs

Network Management Products

- Most important reasons to buy Network Management Products:
  - » Ability to obtain information concerning the operational status of equipment & communication/computing facilities
  - » Network size & complexity
  - » Personnel productivity & cost control
  - » Network planning (performance management & trend analysis)
  - » Security management

Network Management Products (contd.)

- Typically, the network management system
  - » runs on a dedicated station
  - » provides a user-friendly interface with
    - Ð multiple windows
    - Ð multiple colors
      - Red for failing portions of network, Yellow for portions with problems, and Green for portions that are up and running
    - Ð icons for selection with mouse
    - Ð multiple menus
  - » Zoom-in capability

Network Management Products (contd.)

- HP OpenView
  - NNM -- Network Node Manager
  - DTA -- Desk Top Administrator
  - ASA -- Advanced Stack Assistant
  - Jet Admin
  - Can integrate US Robotics Total Control for the management of a Modem Server
  - Etc.

Network Management Products (contd.)

- Unicenter -- Computer Associates
- NetCon -- CapaCity Software
- Enterprise Manager -- SUN MicroSystems
- NetView / Netfinity -- IBM
- 3COM Enterprise Manager
- Microsoft System Management Server