Chapter 6.1:
Network Management

NGUYỄN CAO ĐẠT
E-mail:dat@hcmut.edu.vn

Outline

- Introduction
- What is network management?
- Evolution of Network Management
- ISO Network Management Categories
- Infrastructure for network management

Introduction

- In the early days, network was small
- Network management job includes
  - Installation: attach PCs, printers, etc. to LAN
  - Configuration: NICs, protocol stack, user app's shared printers, etc.
  - Testing: Ping was sufficient to "manage" network
  - Config more devices: hub, switch, router, ..

Introduction

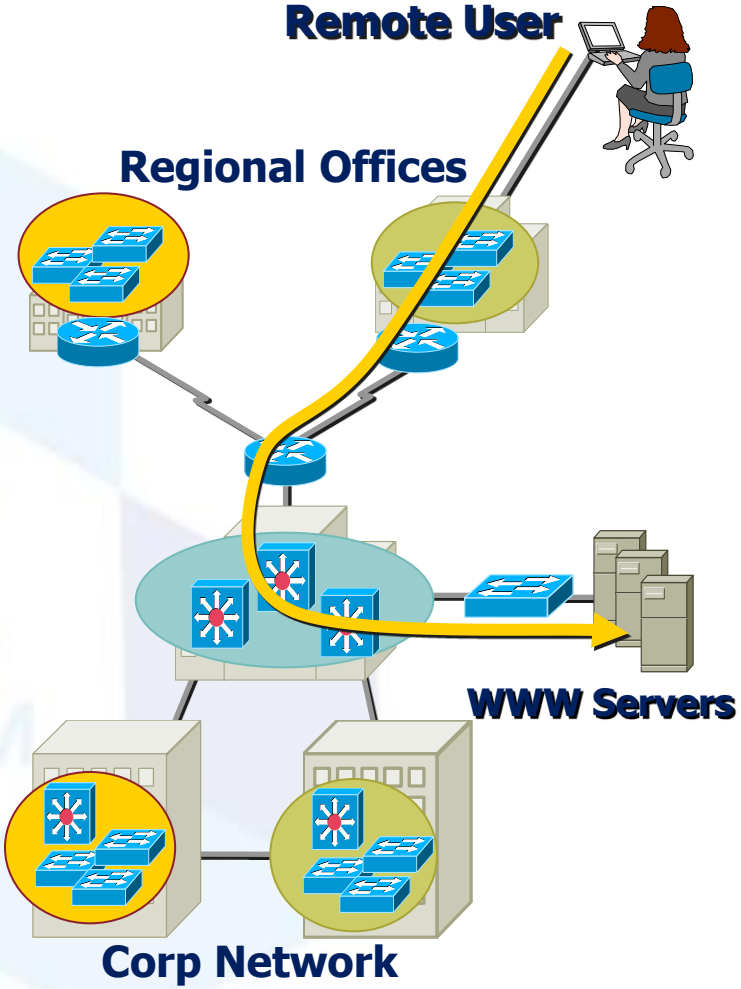
- Above only deals with configuration
- Ongoing maintenance issues
  - How to optimize performance?
  - How to handle failures and network changes?
  - How to extend network capacity?
  - How to account for network usages?
  - How to solve network security issues?

Introduction

- Today, networks are larger and more complicated, so more demands on network manager
- How to monitor and control the network effectively and timely?
  - Management tools are needed
  - Network-based management tools: use the network to manage the network (remotely)
- Solving problem procedures

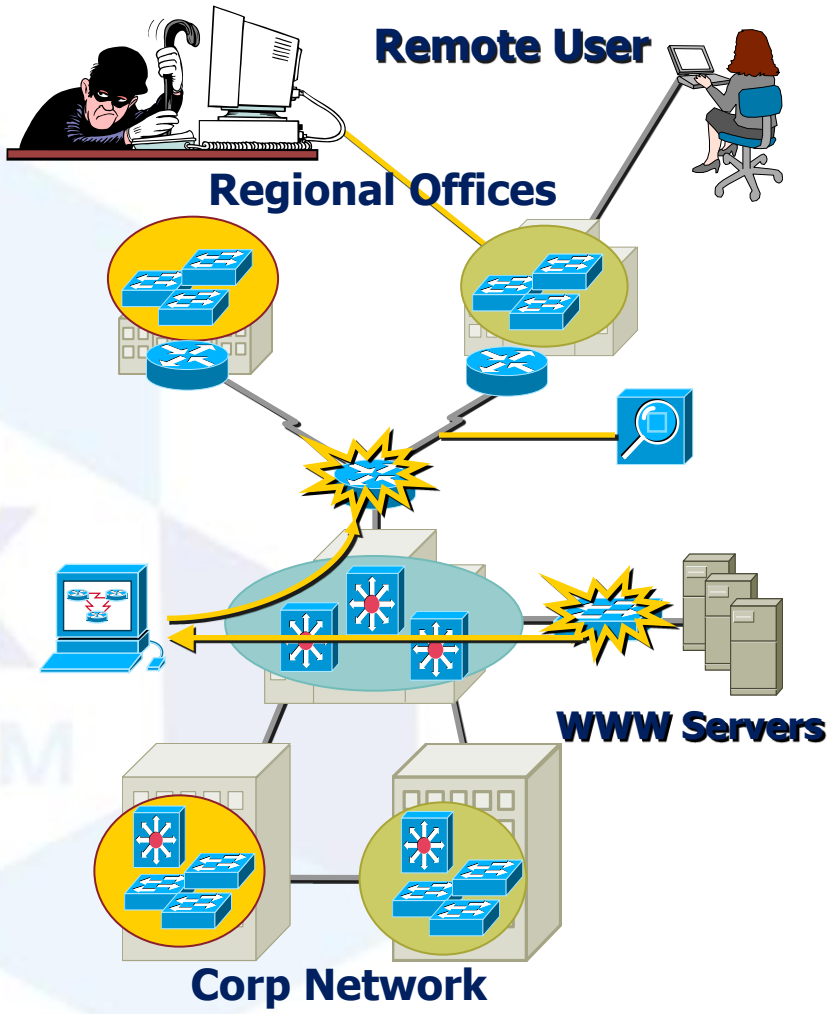
A Case Study

- Typical problem
  - Remote user arrives at regional office and experiences slow or no response from corporate web server
- Where do you begin?
  - Where is the problem?
  - What is the problem?
  - What is the solution?
- Without proper network management, these questions are difficult to answer



A Case Study

- With proper management tools and procedures in place, you may already have the answer
- Consider some possibilities
  - What configuration changes were made overnight?
  - Have you received a device fault notification indicating the issue?
  - Have you detected a security breach?
  - Has your performance baseline predicted this behavior on an increasingly congested network link?



Solving Problem Procedure

- An accurate database of your network's **topology, configuration, and performance**
- A solid understanding of the **protocols and models** used in communication between your management server and the managed devices
- **Methods and tools** that allow you to interpret and act upon gathered information

Outline

- Introduction
- What is network management?
- Evolution of Network Management
- ISO Network Management Categories
- Infrastructure for network management

What is network management?

Definition by Saydam (in Journal of Networks and System Management, published in Dec. 1996)

"Network management includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost."

What is network management?

- Goal
  - To ensure that the users of a network receive the IT services with the quality of service (QoS) that they expect.

Outline

- Introduction
- What is network management?
- Evolution of Network Management
- ISO Network Management Categories
- Infrastructure for network management

Evolution of Network Management

- In 1977 International Organization for Standards (ISO) began work on Open Systems Interconnection (OSI) reference model
  - Purpose was to "provide a common basis for the coordination of standards developments for the purpose of system interconnection, while allowing existing standards to be placed in perspective within the overall Reference Model"
- OSI model published in 1984

Evolution of Network Management

- In March 1987, effort to develop Simple Gateway Monitoring Protocol (SGMP)
  - SGMP out by November 1987
  - Could "get" and "set" variable values
- About same time Common Mgmt Information Protocol (CMIP) developed for OSI model
  - CMIP is roughly SNMP for the OSI model
- Effort to develop CMIP Over TCP (CMOT) as alternative to SGMP

Evolution of Network Management

- CMIP uses Remote Operations Services Elements (ROSE)
  - ROSE is for communication with distributed apps in OSI model
- OSI mgmt process is richer and more comprehensive than that provided by SNMP
- But OSI approach is more complex and took longer to develop
  - SNMP: "keep it simple", and it's good enough
  - So SNMP won out in practice

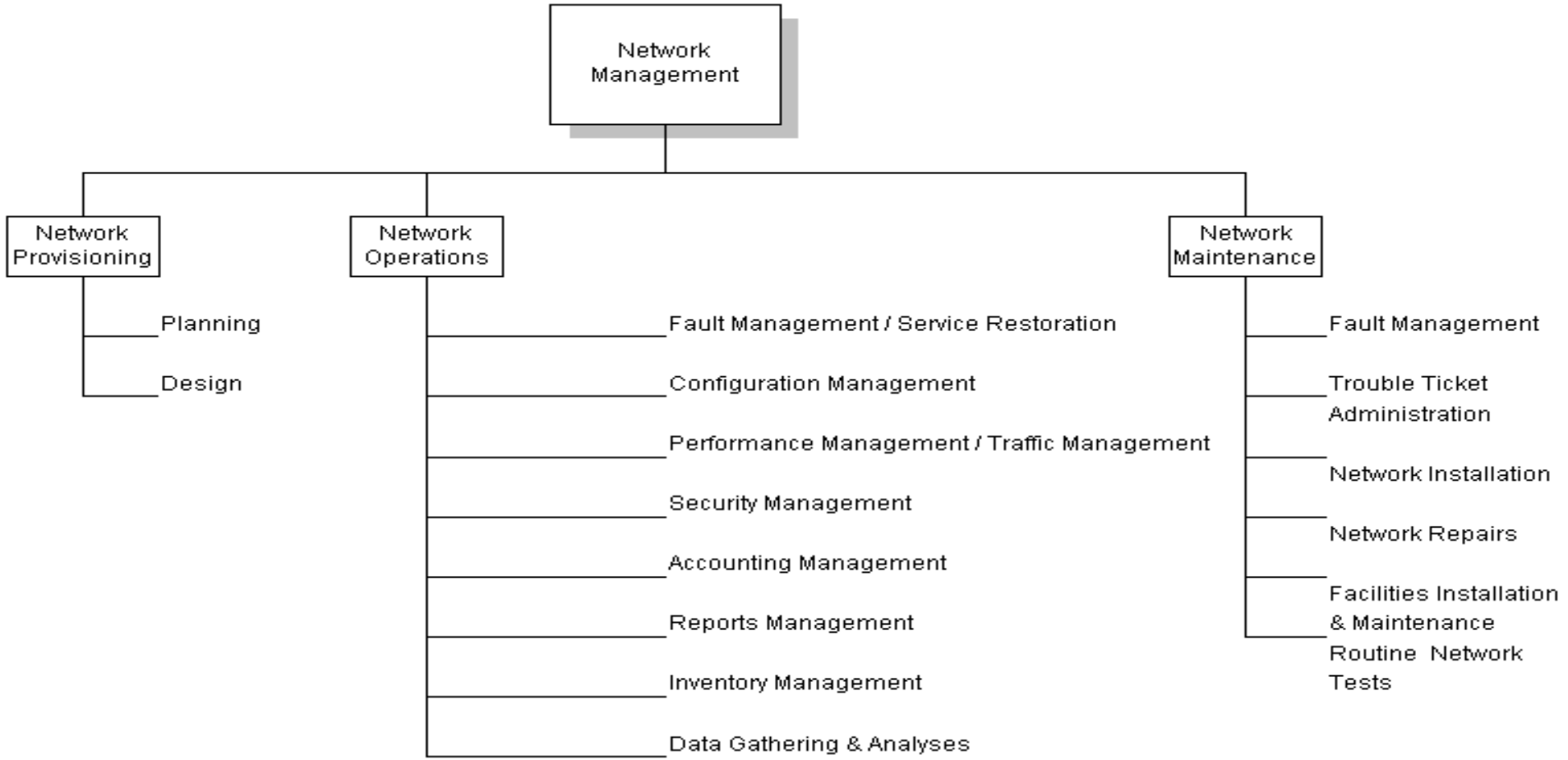
Evolution of Network Management

- Due to controversy/delays in OSI approach, Internet Activities Board (IAB) held meeting in 1988
  - Decided to pursue both CMOT and SGMP
  - Eventually abandoned CMOT (complexity)
- Eventually, three RFCs resulted…
- The three RFCs
  - Structure of Management Information (SMI), uses Abstract Syntax Notation One (ASN.1)
  - Management Information Base (MIB), the data structure on the mgmt agent
  - Simple Network Management Protocol (SNMP)
- By 1989, SNMP was the *de facto* standard for management of TCP/IP networks

Outline

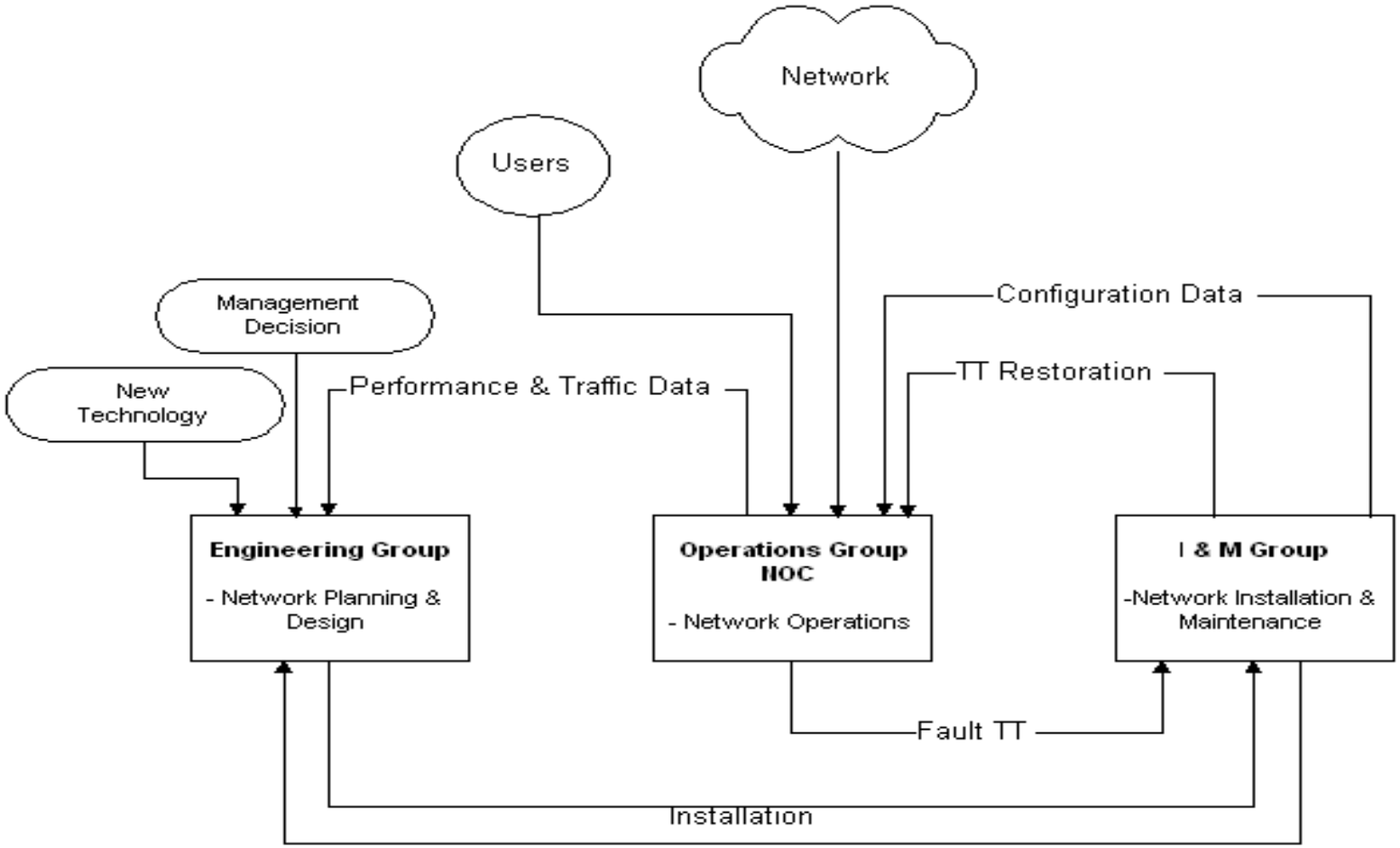
- Introduction
- What is network management?
- Evolution of Network Management
- ISO Network Management Categories
- Infrastructure for network management

Top-down View of NM functions



Network Management Functional Groupings

Nework Management Functional



Network Management Functional Flow Chart

ISO Network Management Categories

- **Fault Management**
  - detection, isolation and correction of abnormal operations
- **Configuration Management**
  - identify managed resources and their connectivity, discovery
- **Accounting Management**
  - keep track of usage for charging
- **Performance Management**
  - monitor and evaluate the behavior of managed resources
- **Security Management**
  - allow only authorized access and control

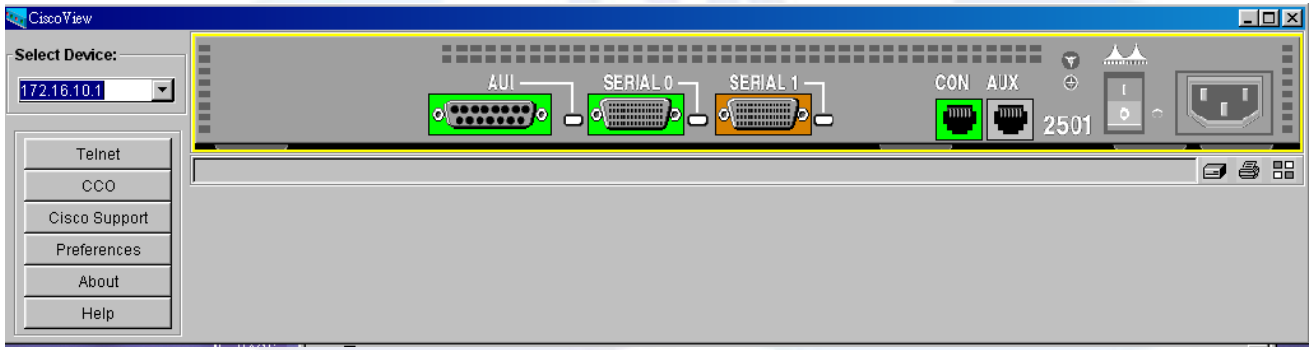
FCAPS

Fault Management

- Manages network problems to keep the network running reliably and efficiently.
- Fault management process involves the following steps
  - Detecting the problem symptoms.
  - Isolating the problem.
  - Fixing the problem automatically (if possible) or manually.
  - Logging the detection and resolution of the problem.

Configuration Management

- Configuration Management monitors network and system configuration information and stores it in a configuration management database.
- The maintenance of this database allows network administrators to track hardware, software, and other network resources

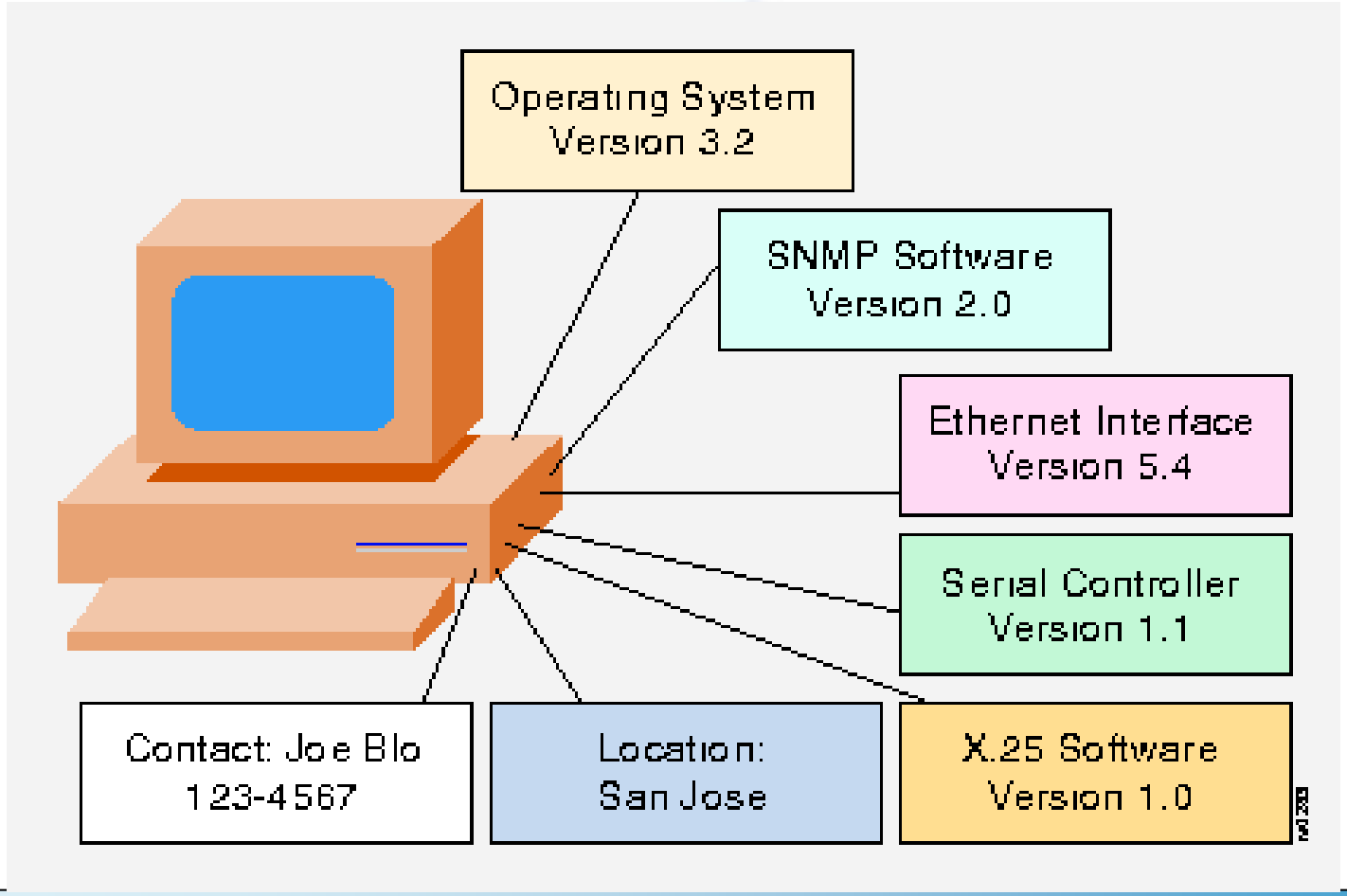


Configuration Management

- Each network device has a variety of information associated with it:
  - Software version information for the operating system, protocol software, or management software.
  - Hardware version information for the interfaces or hardware controllers.
  - Contact information indicating who to contact if problems with the device arise.
  - Location information indicating the physical location of the device.

Configuration Management

- CM Information Associated with a Managed Device



Accounting Management

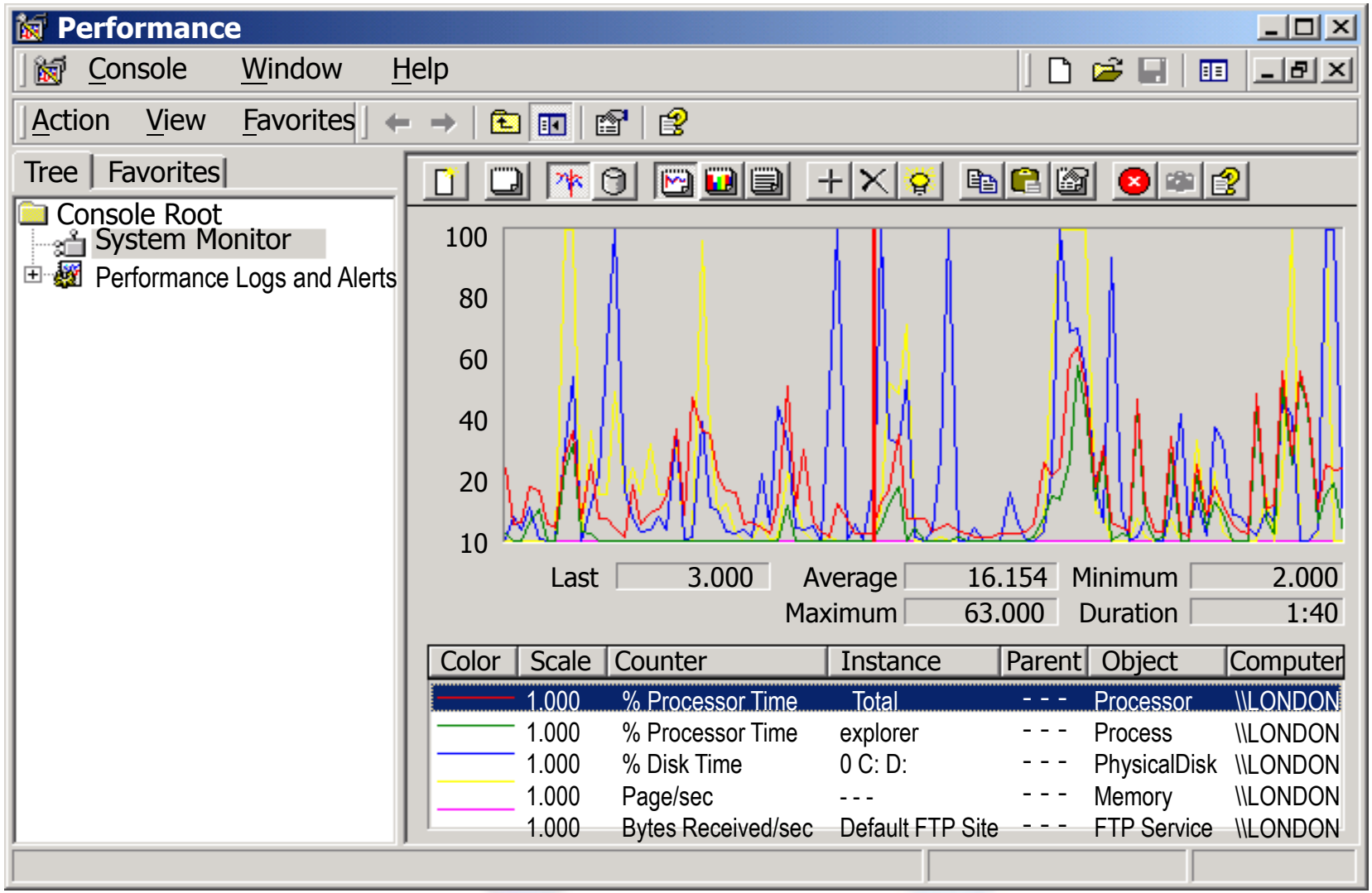
- Measures network utilization parameters in order to regulate individual and group uses of the network.
- Minimizes network problems and maximizes fairness of user access to the network because network resources can be portioned based on network capacity and user needs.

Gather Network Device Utilization Data	• Measure usage of resources by cost center • Set quotas to enable fair use of resources • Site metering to track adherence to software licensing
Bill Users of Network Resources	• Set charges based on usage. • Measure one of the following ❑ Number of transactions ❑ Number of packets • Number of bytes • Set charges on direction of information flow
Use and Accounting Management Tools	• Query usage database to measure statistics versus quotas • Define network billing domains • Implement automatic billing based on usage by users in the domain • Enable billing predictions • Enable user selection of billing domains on the network map
Reporting	• Create historical billings trends • Automatic distribution of billing to Cost Centers • Project future billings by cost center

Performance Management

- Maintains internetwork performance at acceptable levels by measuring and managing various network performance variables.
- Performance variables include network throughput, user response times, line utilization, and others.
- Performance management involves three basic steps:
  1. Gathering data relating to key performance variables.
  2. Analyzing data to determine the normal (baseline) performance levels.
  3. Determining appropriate performance thresholds for each variable so that exceeding these thresholds indicates a network problem worthy of attention.

Performance Management



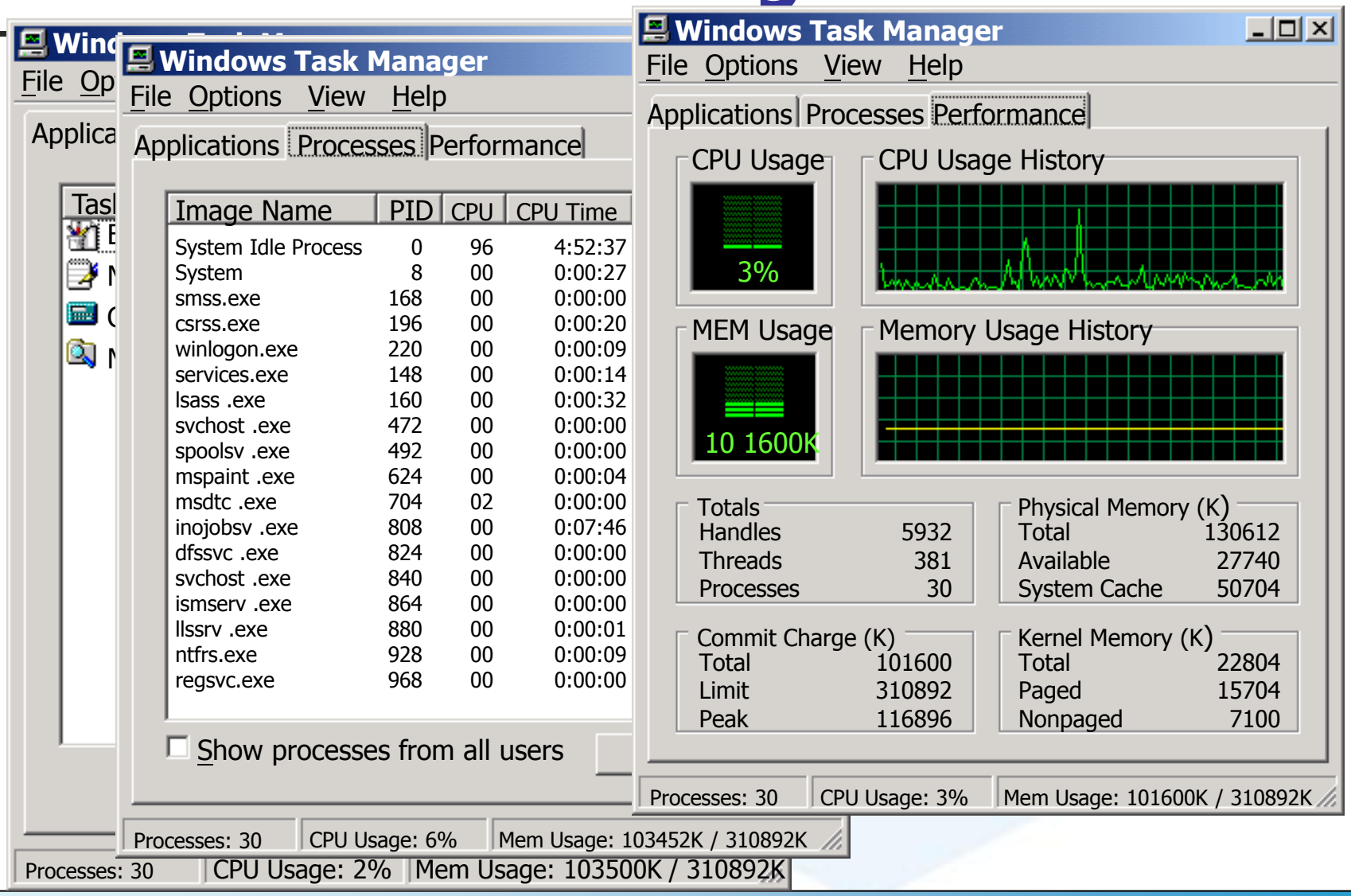
Performance Management

- Reactive
  - when performance becomes unacceptable (that is, a user-defined threshold is exceeded), the managed device reacts by sending an alert to the network management system (NMS).
- Proactive
  - simulation is used to project how network growth will affect performance metrics. These simulations alert administrators to impending problems before they affect network users.

Performance Management

- Reactive PM Components
  - The management entity continually monitors performance variables in managed devices.
  - When a particular performance threshold is exceeded, the NMS or the managed device detects the problem.
  - If the managed device detects the problem, it generates an alert and sends it to the NMS.
  - The NMS takes an appropriate action, such as alerting the network administrator.

Windows Task Manager



Security Management

- Access control
  - Controls access to network resources, and prevents network sabotage (intentional or unintentional) and unauthorized access to sensitive information.
  - Aids administrators in creating a secure network environment. This includes:
    - partitioning network resources into authorized and unauthorized areas,
    - mapping groups of users to those areas, and
    - monitoring, policing, and logging user access to resources in those areas.

Security Management

- Security monitoring
  - Security event collection
  - Event analysis, correlation and alert generation
  - Alert handling

Applying Basic Techniques	• Identifying hosts that store sensitive information • Management of passwords • Assigning user rights and permissions • Recording failed logins • Setting remote access barrier codes • Employing virus scanning • Limiting views of the Enterprise network • Tracking time and origin of remote accesses to servers
Identifying Access Methods Used	• Electronic Mail • File Transfer • Web Browsing • Directory Service • Remote Login • Remote Procedure Call • Remote Execution • Network Monitors • Network Management System

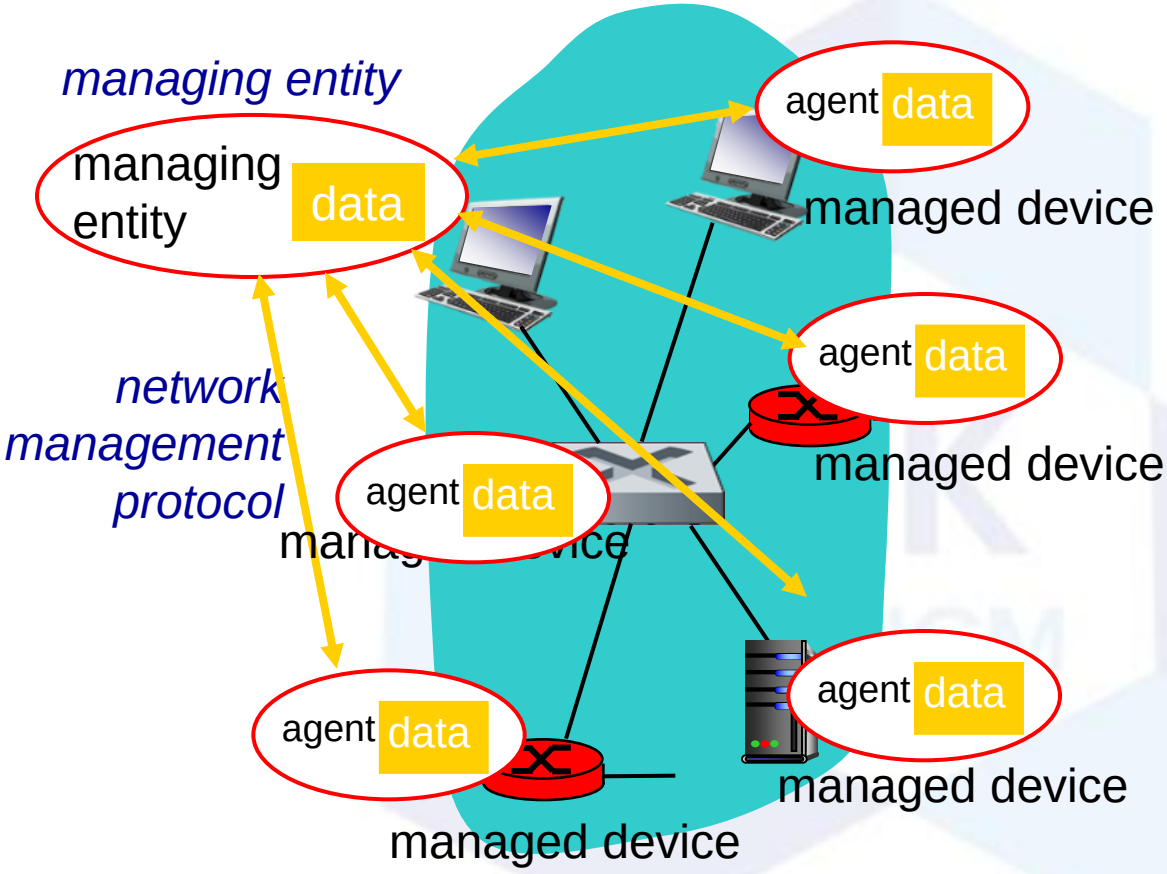
Using Access Control Methods	• Encryption • Packet filtering at routers • Packet filtering at firewalls • Source host authentication • Source user authentication
Maintenance	• Audits of the activity at secure access points • Executing security attack programs (Network Intrusion Detection) • Detecting and documenting breaches
Accessing Public Data Networks	• No restrictions - hosts are responsible for securing all access points • Limited access - only some hosts can interface with the Public Data Network using a proxy server
Using an Automated Security Manager	• Queries the configuration database to identify all access points for each device. • Reads event logs and notes security-related events. • Security Manager shows a security event on the network map. • Reports of invalid access point attempts are generated daily for analysis

Outline

- Introduction
- What is network management?
- Evolution of Network Management
- ISO Network Management Categories
- Infrastructure for network management

Infrastructure for network management

definitions:



managed devices contain *managed objects* whose data is gathered into a *Management Information Base (MIB)*

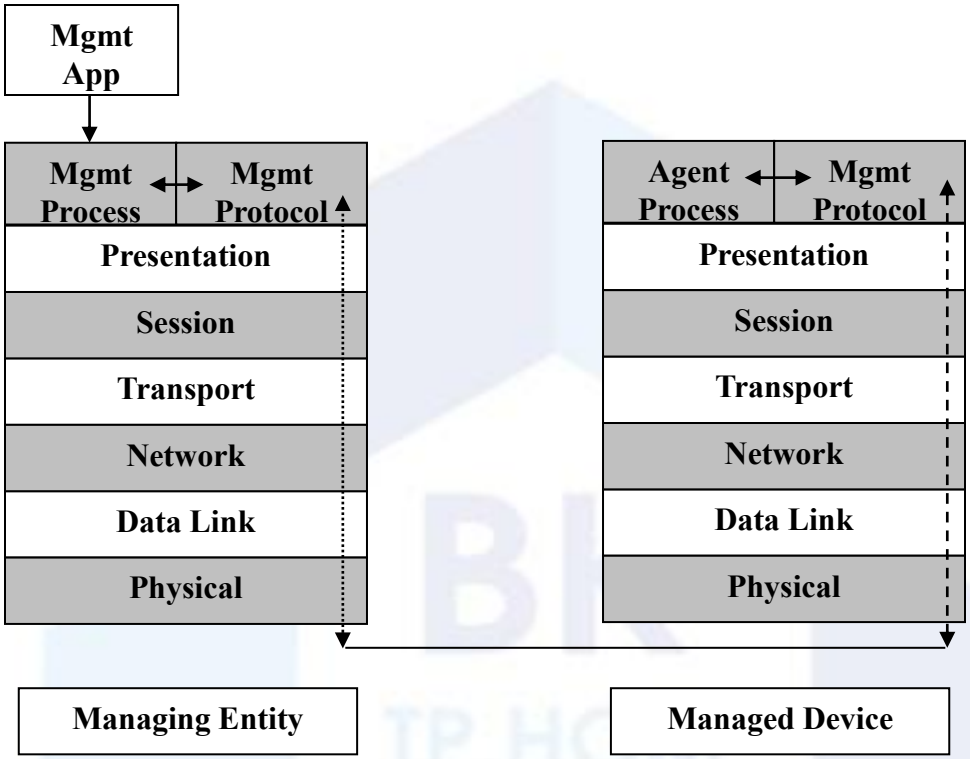
Infrastructure for network management

- Managed Device
  - Devices to be monitored/controlled, e.g., router, switch, hub, bridge, workstation.
  - A managed device may have several managed objects to be managed
  - A software (agent) is installed to provide **access** to information/parameters (data) about the device, which is called Management Information Base (MIB)
- Managing Entity
  - Used by the manager/Admin to do network management
  - PC, notebook, terminal, etc., installed with a software called Network Management System (NMS)
  - NMS displays/analyzes data from management agents

Infrastructure for network management

- Network Management Protocol
  - Runs between the managing entity and the managed devices
  - The managing entity can query the status of the managed devices and take actions at the devices via its agents
  - Agents can use the protocol to inform the managing entity of exceptional events
  - E.g., SNMP: Simple Network Management Protocol
- Managing agents located at managed devices are periodically queried by the managing entity through a network management protocol.

Network management example



Network management example

- To get value of MIB variable from mgmt agent
  1. Mgmt app (part of NMS) on managing entity passes request to mgmt process
  2. Mgmt process calls network mgmt protocol (e.g., SNMP)
  3. SNMP constructs Get-Request packet and sent it to the managed device through the network
  4. Mgmt agent on managed device receives Get-Request
  5. Agent process accesses requested value
  6. SNMP constructs Get-Response packet and sent it to managing entity through the network
  7. Mgmt process on managing entity receives response
  8. Mgmt process passes data to mgmt app

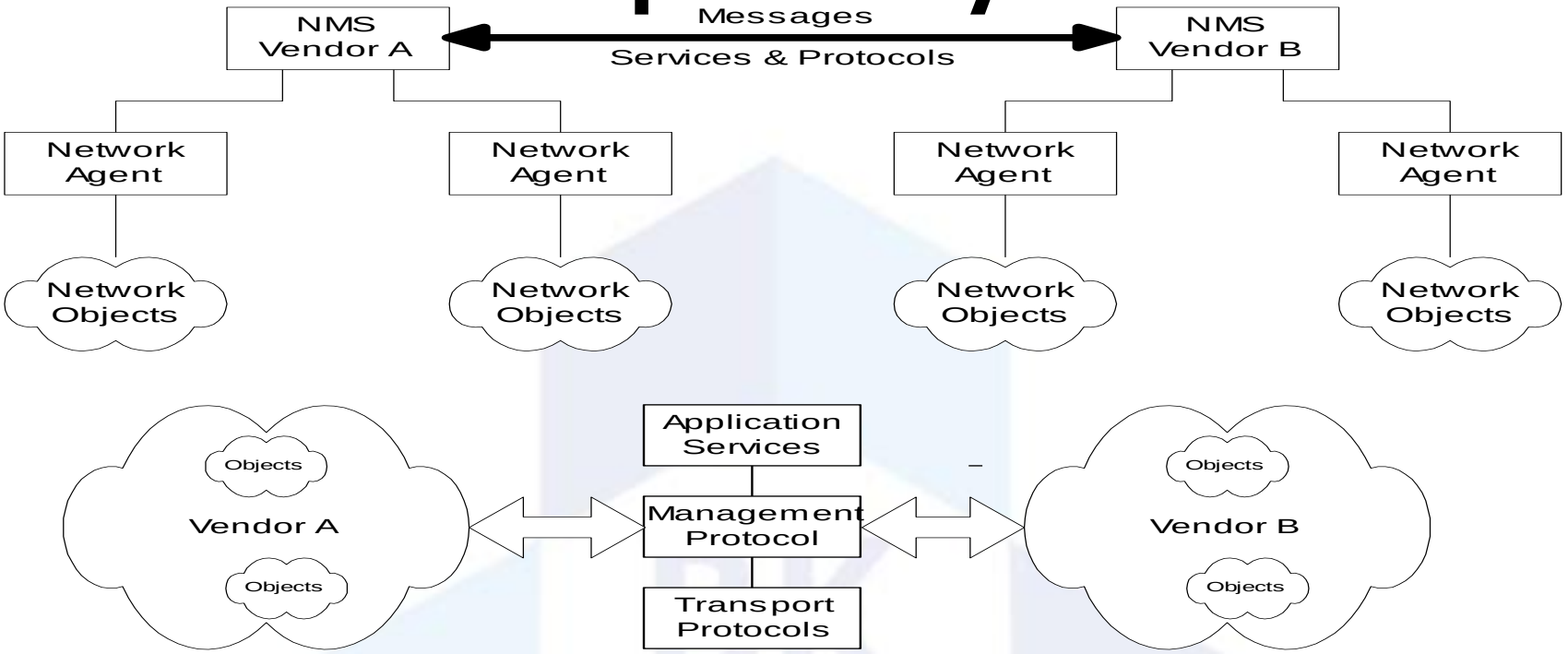
Network Management Overhead

- There is overhead in terms of
  - CPU cycles to generate and process information/packets
    - May require dedicated Managing Entity
  - Bandwidth usage for sending request and receiving responses
- A tradeoff between cost and benefit

Network Management Systems

- A network management system (NMS) is a collection of tools for network monitoring and control
- based on the manager-agent paradigm
  - the manager sends mgmt requests to one or more agents
  - an agent performs the requested operation and returns results
  - when agents detect faults and they report to the manager
- NMS typically provides a GUI through which most or all management tasks can be performed
- Many commercial and freely available NMSs exist:
  - Commercial: HP OpenView, IBM NetView, Sun Net Manager, Cisco works and etc.
  - Open source: OpenNMS , Nagios and etc.

Interoperability



(b) Services and Protocols

Figure 1.23 Network Management Dumbbell Architecture

Notes

- Message exchange between NMSs managing different domains