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."
In brief:

- Network management is mostly a combination of local and remote configuration and management with software.
- Remote network management is accomplished when one computer is used to monitor, access, and control the configuration of other devices on the network.

Functions of Network Managers

- Installation: attach PCs, printers, etc. to LAN
- Configuration: NICs, protocol stack, user app's shared printers, etc.
- Testing: Ping was sufficient to "manage" network
- More devices: bridge, router

Issues of Maintenances?

- 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?

Responsibilities of Network Manager

- Server admin
- System admin
- Network admin
- Security specialist
- Different certifications for these
  - Cisco, Novell, Microsoft, Sun, $(ISC)^2$ etc.

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)

- To control
  - Simple Network Management Protocol (SNMP)
  - Management Information Base (MIB)
  - Network Management System (NMS)
- To monitor
  - Remote Monitor (RMON1)

Benefits of Network Management

- Detecting failure of an interface card at a host or a router
- Host monitoring
- Monitoring traffic to aid in resource deployment
- Detecting rapid changes in routing tables
- Monitoring for SLAs (Service Level Agreements)
- Intrusion detection

ISO Network Management Categories

- Performance Management
- Fault Management
- Configuration Management
- Security Management
- Accounting Management

Performance Management

- Concerned with
  - Response time
  - Utilization
  - Error rates, etc.
- Must collect and analyze data
  - Number and type of packets
  - Might also rely on simulations

Fault Management

- Preventions, detection and isolation of abnormal behavior
  - May be caused by malfunction, cable issue, the janitor, etc.
- Traffic, trends, connectivity, etc.
  - SNMP **polls**
  - **Alarms** for automatic fault detection
  - Monitor statistics
  - Timeliness etc.

Configuration Management

- Device configuration
  - May be done locally or remotely
- Network configuration
  - Sometimes called “capacity mgmt”
  - Critical to have sufficient capacity
- Desirable to automate as much as possible
  - For example, DHCP and DNS
- Extensions to SNMP MIB

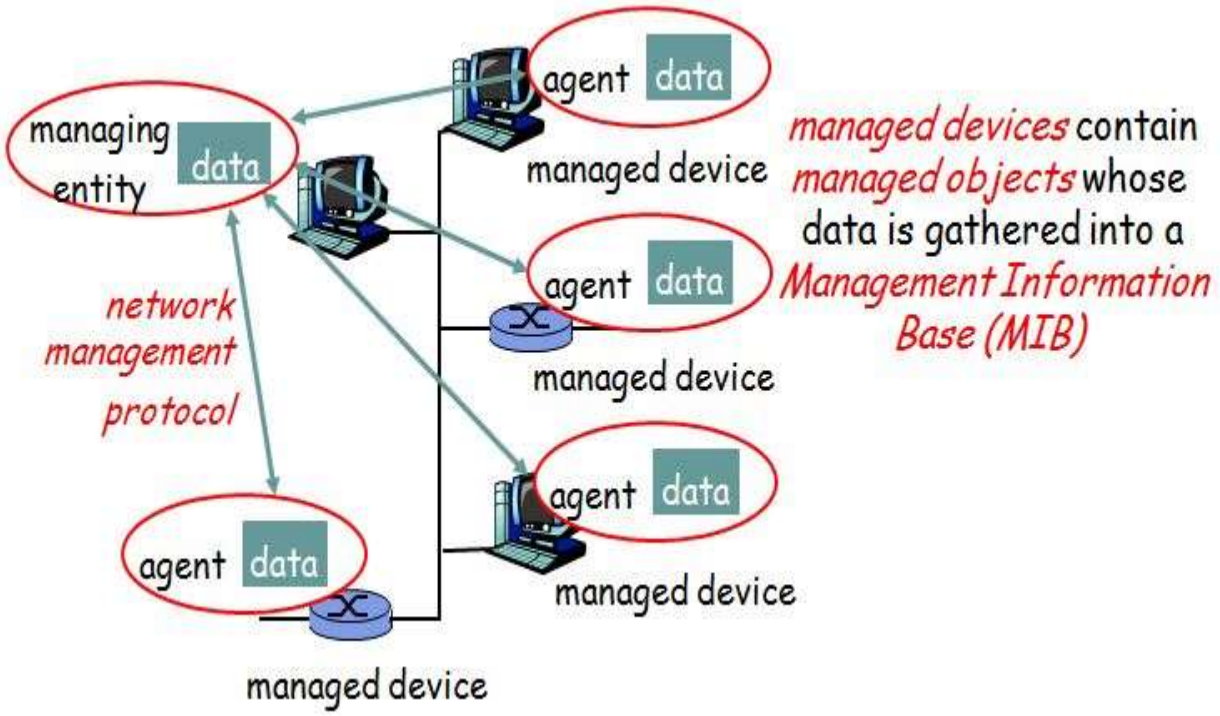
Security Management

- Control access to network/resources
  - Authentication: who goes there?
  - Authorization: are you allowed to do that?
  - Firewalls
  - Intrusion detection systems (IDS)
  - Notification of (attempted) breaches, etc.
- Critical to always authenticate participants
- SNMPv1 has very little security
- SNMPv3 has lots of security built in

Accounting Management

- Measuring the usage of network resources in order to distribute costs and resources
- Allows the network manager to specify, log and control user and device access to network resources
- E.g., monitoring the use of a server by users in a specific department and charging the department accordingly

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
  - Managed objects mean pieces of hardware, and sets of configuration parameters for hardware and software such as routing protocols
  - A software (agent) is installed to provide **access** to information/parameters (data) about the device, which is called Management Information Base (MIB)
- Managing Entity
  - An application used by the manager/Admin to do network management
  - It controls the collection, processing, analysis, and/or display of network management information
  - PC, notebook, terminal, etc., installed with a software called Network Management System (NMS)
  - NMS displays/analyzes data from management agents
- 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.

Internet-Standard Management Framework

This addresses

- What is being monitored? And what form of control can be exercised by the network administrator?
- What is the specific form of the information that will be reported and/or exchanged?
- What is the communication protocol for exchanging this information?

4 parts

- MIB (Management Information Base)
- SMI (Structure of Management Information)
- SNMP (Simple Network Management Protocol)
- Security and administration capabilities

MIB

- Represented as a collection of managed objects that together form a virtual information store
- Might be a counter, such as the number of IP datagrams discarded at a router due to errors in the IP datagram header; or the number of carrier sense errors in an Ethernet interface card; descriptive information such as the version of software running on a DNS server, status information such as whether a particular device is functioning properly; or protocol-specific information such as a routing path to a destination
- MIB objects thus define the management information maintained by a managed device
- Related MIB objects are gathered into MIB modules

SMI

- Data definition language
- Defines the data types, an object model, and rules for writing and revising management information
- MIB objects are specified in this data definition language

SNMP

- Protocol used for conveying information and commands between a managing entity and an agent executing on behalf of that entity within a managed network device

Security and administration capabilities

- The addition of these capabilities represents the major enhancement in SNMPv3 over SNMPv2

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

Additional Network Management Capabilities

- For efficiency, multiple values can be constructed in a single Get-Response packet
- Can traverse MIB in logical order
- Mgmt agent can send unsolicited messages
    - These are known as **traps**
    - E.g., if a device goes down
- Can request info from probes or remote monitors (RMON)
    - Monitoring activity (traffic) on a network segment