UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

Network Security Administration and Management

BITS 3353

Lecture 2: Network Management

Lesson Outline

- What is Network Management
- Goal of Network Management
- Network Management Standard
- Network Management Model
- Infrastructure for Network Management
- Simple Network Management Protocol (SNMP)

WHAT IS NETWORK MANAGEMENT

- The process of administering and managing computer network.
- Network management involves several different components.
  - Network administration
  - Network maintenance
  - Network operation
  - Network provisioning
  - Network security

WHAT IS NETWORK MANAGEMENT

- Network manager's 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
  - More devices: bridge, router

- 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?

WHAT IS NETWORK MANAGEMENT

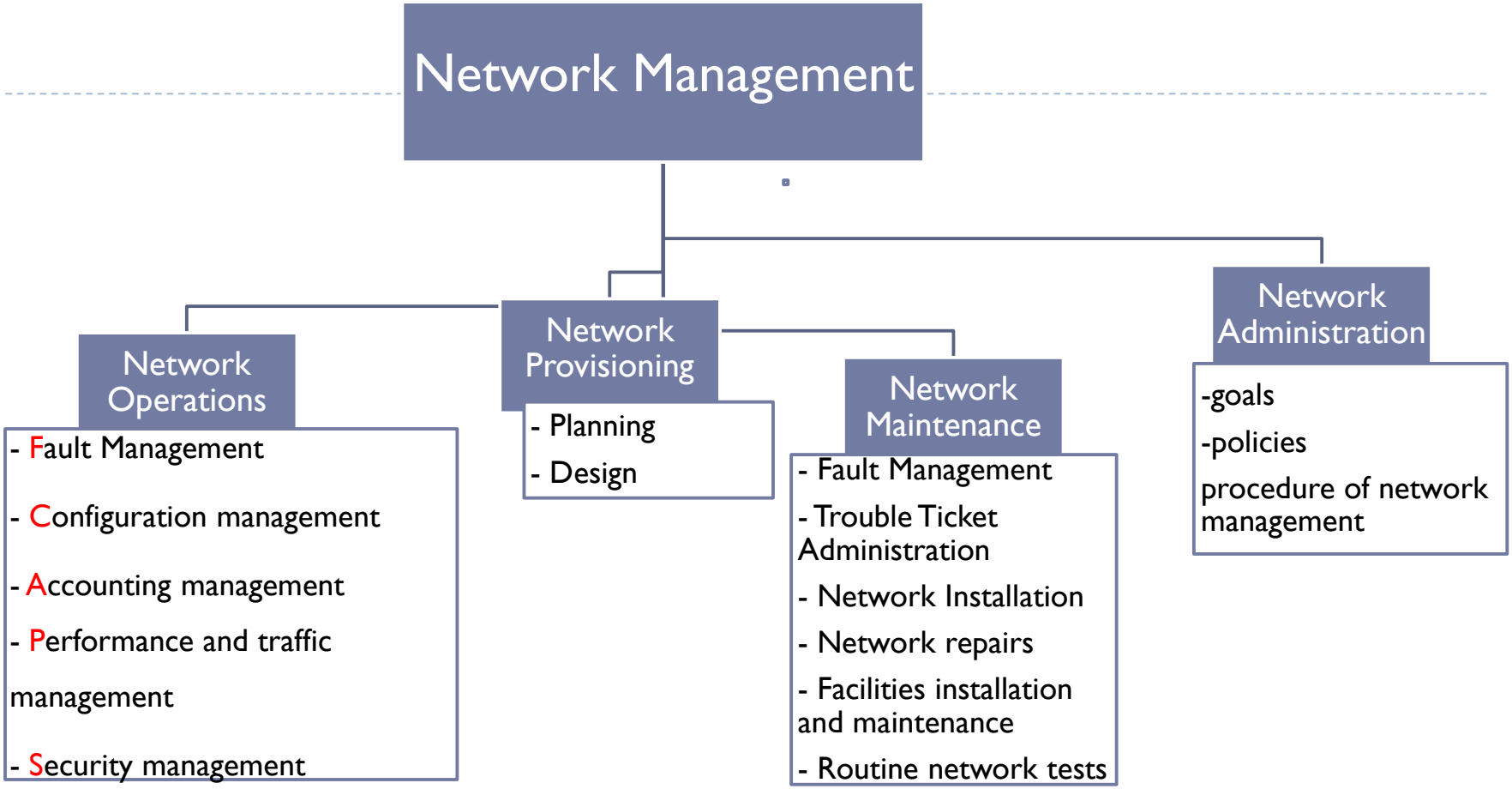
- Today the task has divided into specialties:
  - Server admin
  - System admin
  - Network admin
  - Security specialist
  - Different certifications for these
    - Cisco, Novell, Microsoft, Sun, $(ISC)^2$, etc.

WHAT IS NETWORK MANAGEMENT

- 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.

GOAL OF NETWORK MANAGEMENT

- Effectively manage specific set of devices
- To ensure that the users of a network receive the information technology services with the quality of services that they expect.
  - With minimum service interruption


Network Management
Network Operations
- Fault Management
- Configuration management
- Accounting management
- Performance and traffic management
- Security management
Network Provisioning
- Planning
- Design
Network Maintenance
- Fault Management
- Trouble Ticket Administration
- Network Installation
- Network repairs
- Facilities installation and maintenance
- Routine network tests
Network Administration
-goals
-policies
procedure of network management

Network Operation

International Organization for Standardization (ISO) has define 5 Network Management functional areas

- **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.
  - Determine exactly where the fault is
  - Isolating the problem.
  - Fixing the problem automatically (if possible) or manually.
  - Logging the detection and resolution of the problem.
  - Test : connectivity, data integrity, response time , etc.

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
- Steps:
  - Installation of new hardware / software
  - Tracking changes in control configuration
  - Who, what and why? – network topology
  - Revert/undo the changes
  - Change management
  - Configuration audit
  - Does it do what was intended

Configuration Management (2)

- 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.

Accounting Management

- Measures network utilization parameters in order to regulate individual and group uses of the network.
- Involves granting or removing permission for access to the network
- Mapping network resources consumption to customer identity

Performance Management

- Maintains internetwork performance at acceptable levels by measuring and managing various network performance variables.
- Performance variables include network throughput, user response times, utilization, and others.
- Indicators: availability, response time and accuracy, throughput, utilization
- 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.

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

Network Management Standard

The following are the network management standards in use:

1. OSI / CMIP Model
2. SNMP/ Internet Model
3. TMN Model
4. IEEE LAN/MAN Model

Network Management Standard: OSI/CMIP

- Open System Interconnection (OSI) is the standard adopted by the International Organization for Standardization (ISO)
- It is the most comprehensive set of specifications and addresses all seven layers.
- Object oriented
- Management of data communications network—LAN and WAN.
- Well structured and layered
- Consume large resource of implementation

Network Management Standard:
SNMP / Internet Model

The major positive points of Simple Network Management Protocol (SNMP) /Internet standard are,

- Industry standard (IETF)
- Originally intended for management of Internet components, currently adopted for WAN and telecommunication systems
- Easy to implement
- Most widely implemented

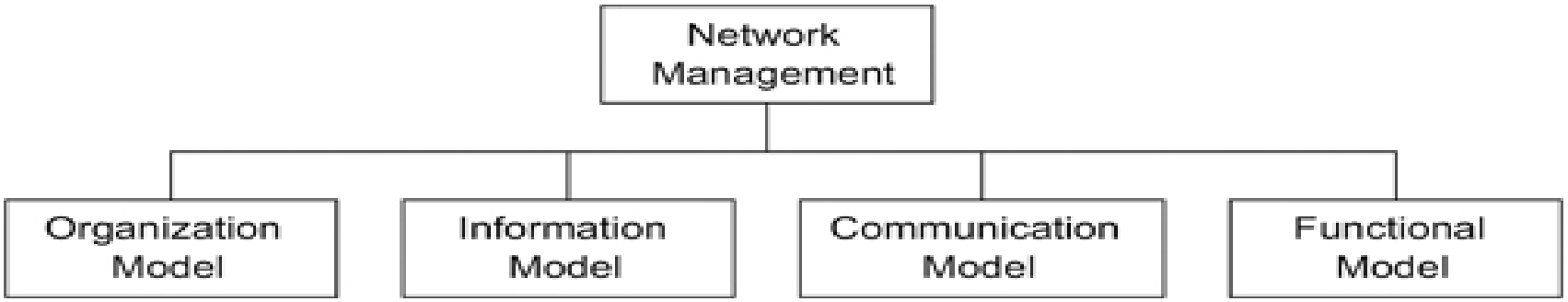
Network Management Standard: TMN Model

- International standard (ITU-T)
- Management of telecommunications network
- Based on OSI network management framework
- Addresses both network and administrative aspects of management

Network Management Standard: IEEE

- IEEE standards adopted internationally
- Addresses LAN and MAN management
- Adopts OSI standards significantly
- Deals with first two layers of OSI RM (Reference model)

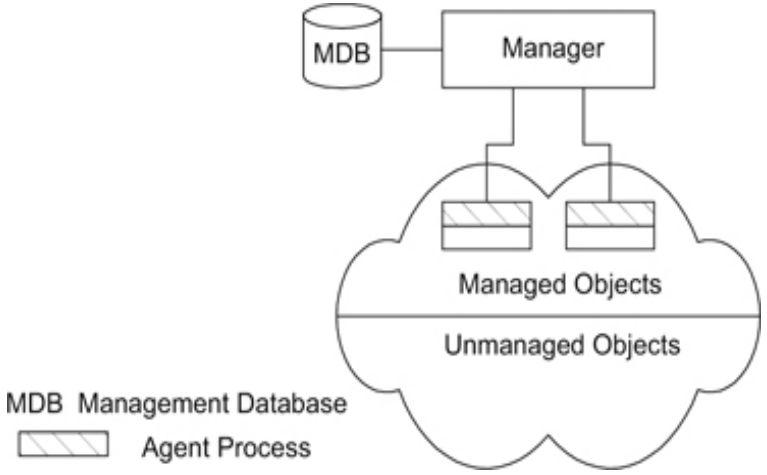
Network Management Model



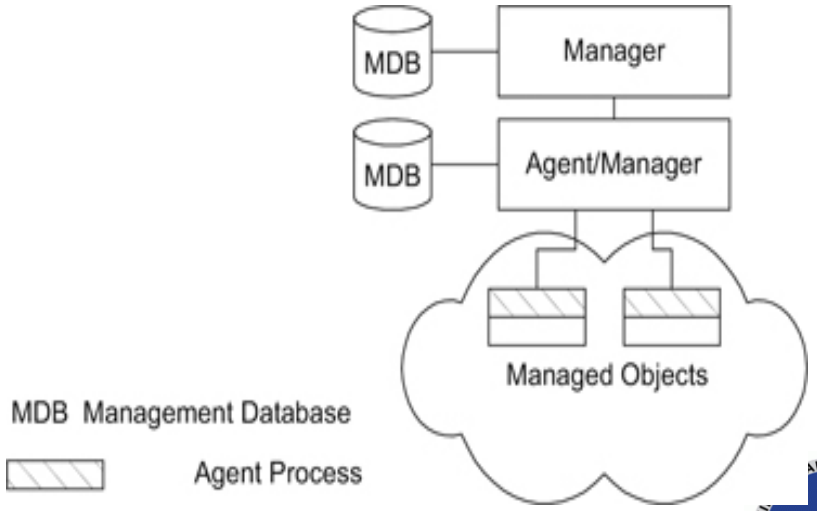
Network Management Model: Organizational Model

- It describes the components of network management and their relationships.
- Network objects consist of network elements such as hosts, hubs, routers, etc.
- Objects can be classified into managed and unmanaged objects or elements.

Two-Tier Network Management Organization Model



Three-Tier Network Management Organization Model



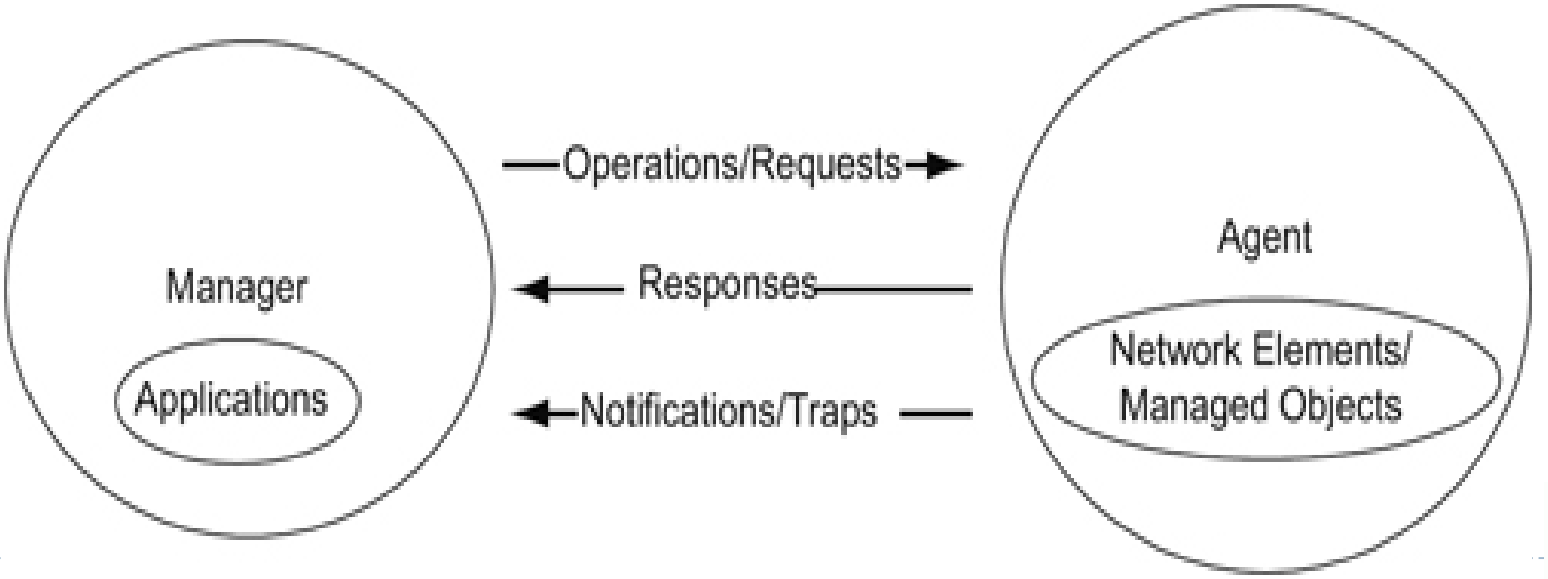
Network Management Model:
Information Model

- An information model is concerned with the structure and storage of information.
- Information Model specify:

- Structure of Management Information (SMI) (describe how the management information is structured)
- Management Information Base (MIB) (deals with the relationship and storage of management information)

Network Management Model: Communication Model

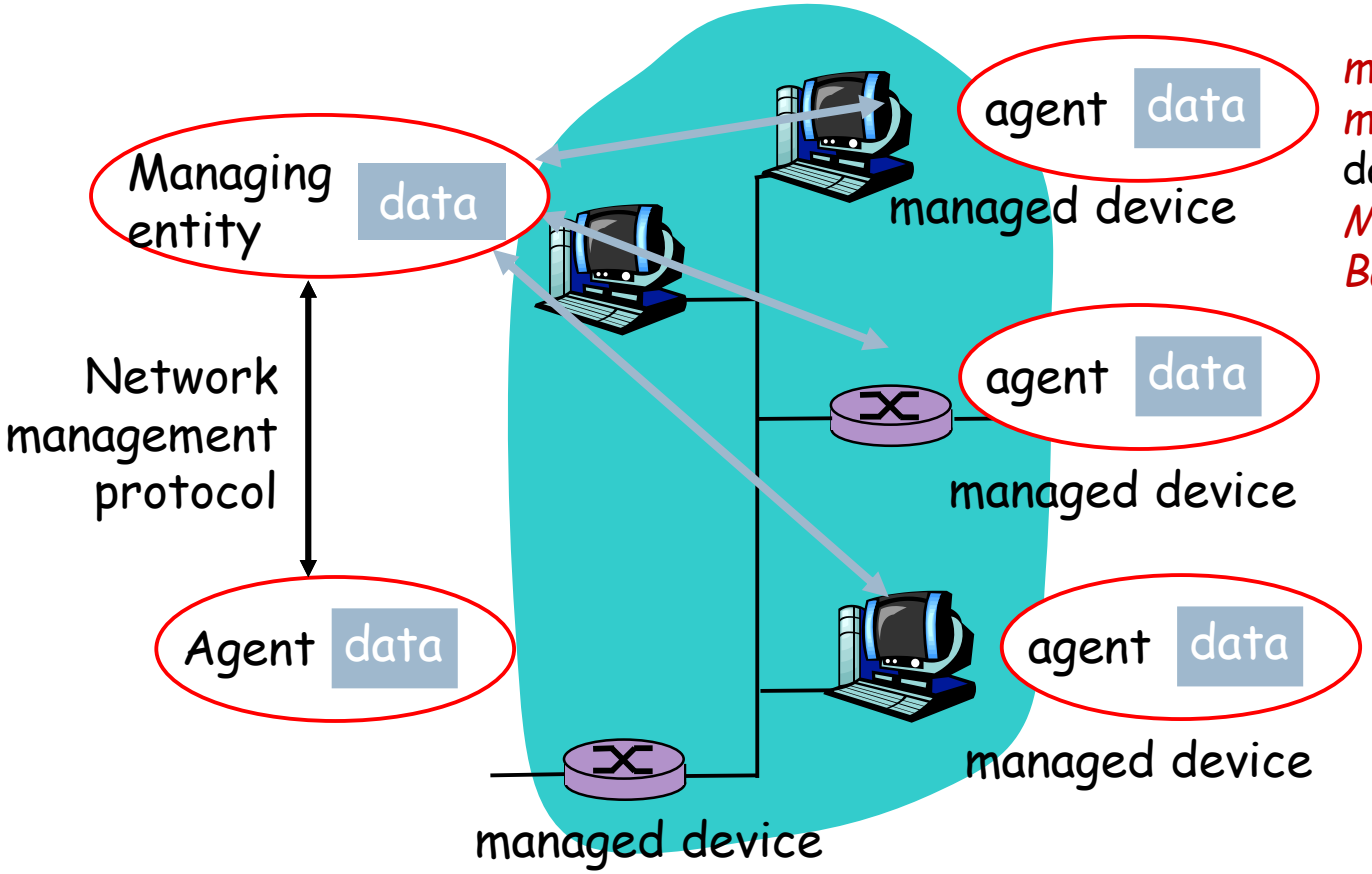
- This model is associated with how the information is exchanged between systems.
- Management data are communicated between agent and manager processes, as well as between manager processes.
- The applications in the manager module initiate *requests* to the agent in the Internet model.
- The agent executes the request on the network element; i.e., managed object.



Network Management Model: Functional Model

- Deals with the user-oriented requirement of network management
- OSI define five functional application namely ; configuration, fault performance, security and accounting.

Infrastructure for Network Management



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

Infrastructure for Network Management

- Managing Entity (BOSS)
  - Locus of activity for network management
  - Controls the collection, processing, analysis and/or display of network management information.
  - Used by the manager/Admin to do network management
  - PC, notebook, terminal, etc., installed with a software called Network Management System (NMS)
  - installed with a software called Network Management System (NMS) Managed Device (BRANCH OFFICE)
  - 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)

(MIB correspond to quantitative data (budget, activity) exchanged between the branch office and the main office)

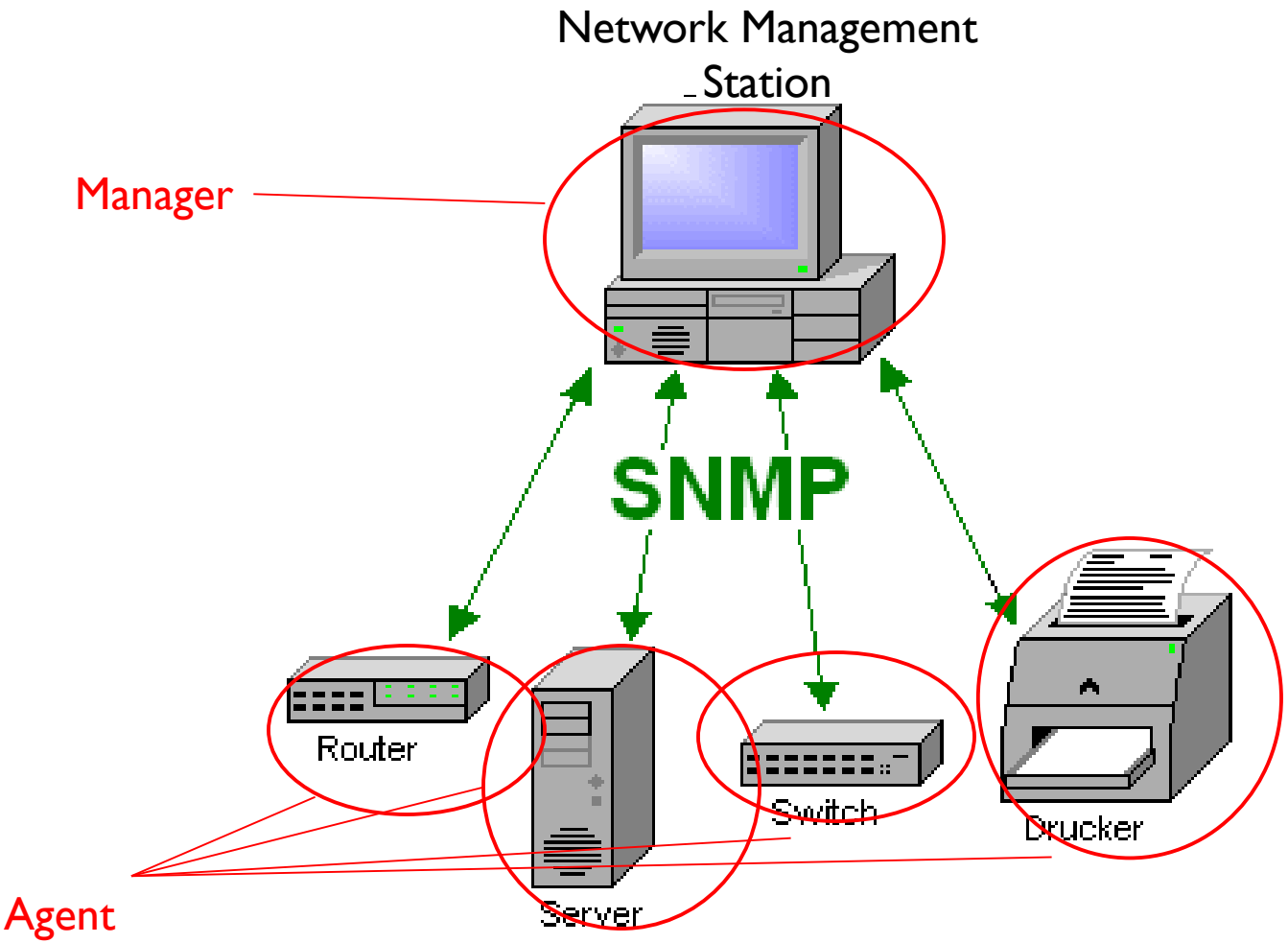
Infrastructure for Network Management

- 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.

Simple Network Management Protocol (SNMP)

- Network management systems use SNMP (Simple Network Management Protocol) to communicate with network elements.
- For this to work, the network element must be equipped with an SNMP agent.
- Purpose: to make sure network protocol and devices not only work but work well
- Communicate through SNMP message

Simple Network Management Protocol (SNMP)



Summary

- Network management
  - Extremely important : 80% of network cost
  - Netwotk Management Infrastructure
    - Managing entity, managed devices, network management protocol
  - Network management services ensure that your IT infrastructure management tools and devices work smoothly. Monitoring helps you to recognize the existence and changes within your organization's IT. It also assists you to define the importance of latest technologies for your business.