Unit 1

Principles of Network Management

What is Management ?

- Management: defined as monitoring & controlling
  - the resources in computers,
  - the resources used in the connection & communication of computers,
  - the applications used in the computers
- Involves: collecting of data, processing data to generate information, making decisions and enactment of activities to implement those decisions

What is Network Management (NM) & Systems Management?

Several Definitions available!

- ‘NM provides mechanisms for the monitoring, control and coordination of all managed objects within the physical and data link layer of a network node’ [IEEE]
- ‘Systems Mgt. provides mechanisms for the monitoring, control and coordination of all managed objects within open systems. This is effected through application layer protocol’ [IEEE]

=> NM is subset of Systems Management

What is NM & SM (cont. 2) ?

- **Monitoring:** continuous watching of resources for deterioration of function. Is more pro-active rather than re-active
- **Control:** make effective modifications to functioning of resources for optimization/rectification
- **Co-ordination:** involves both co-ordination of resources and co-ordination of monitoring/control activities

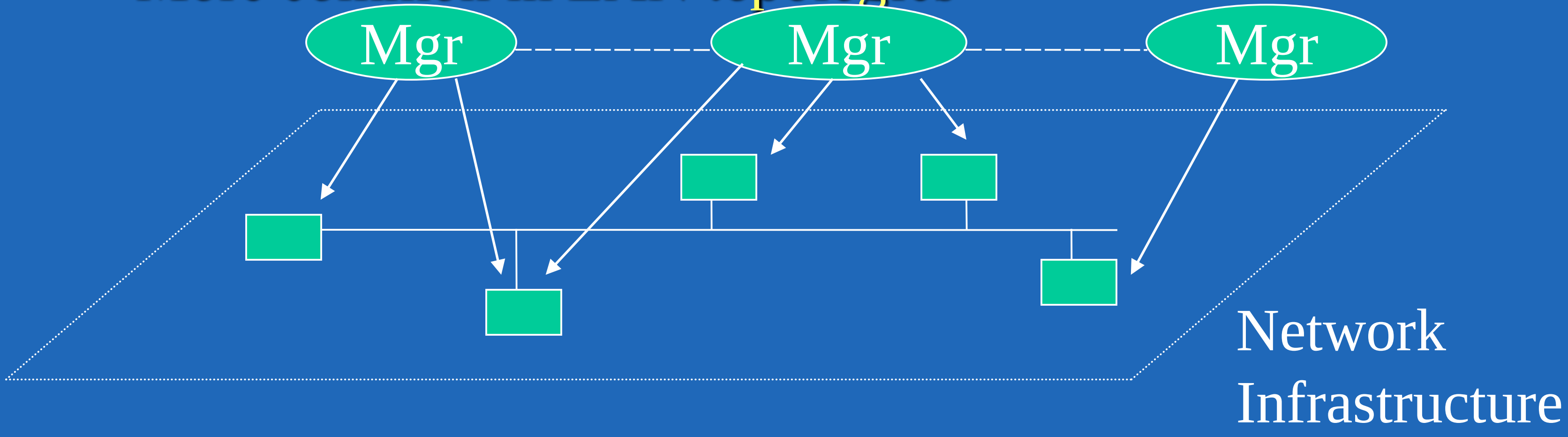
Why Systems/network Management

- Higher network availability
- Reduce Network operational costs
- Reduce network bottlenecks
- Increase flexibility of operation and integration
- Higher efficiency
- Security

Two basic Models of Network Management

Peer-to-Peer Net. Mgt

- Managers who undertake mgt activities act more as peers and there is no central manager
- More common in LAN topologies

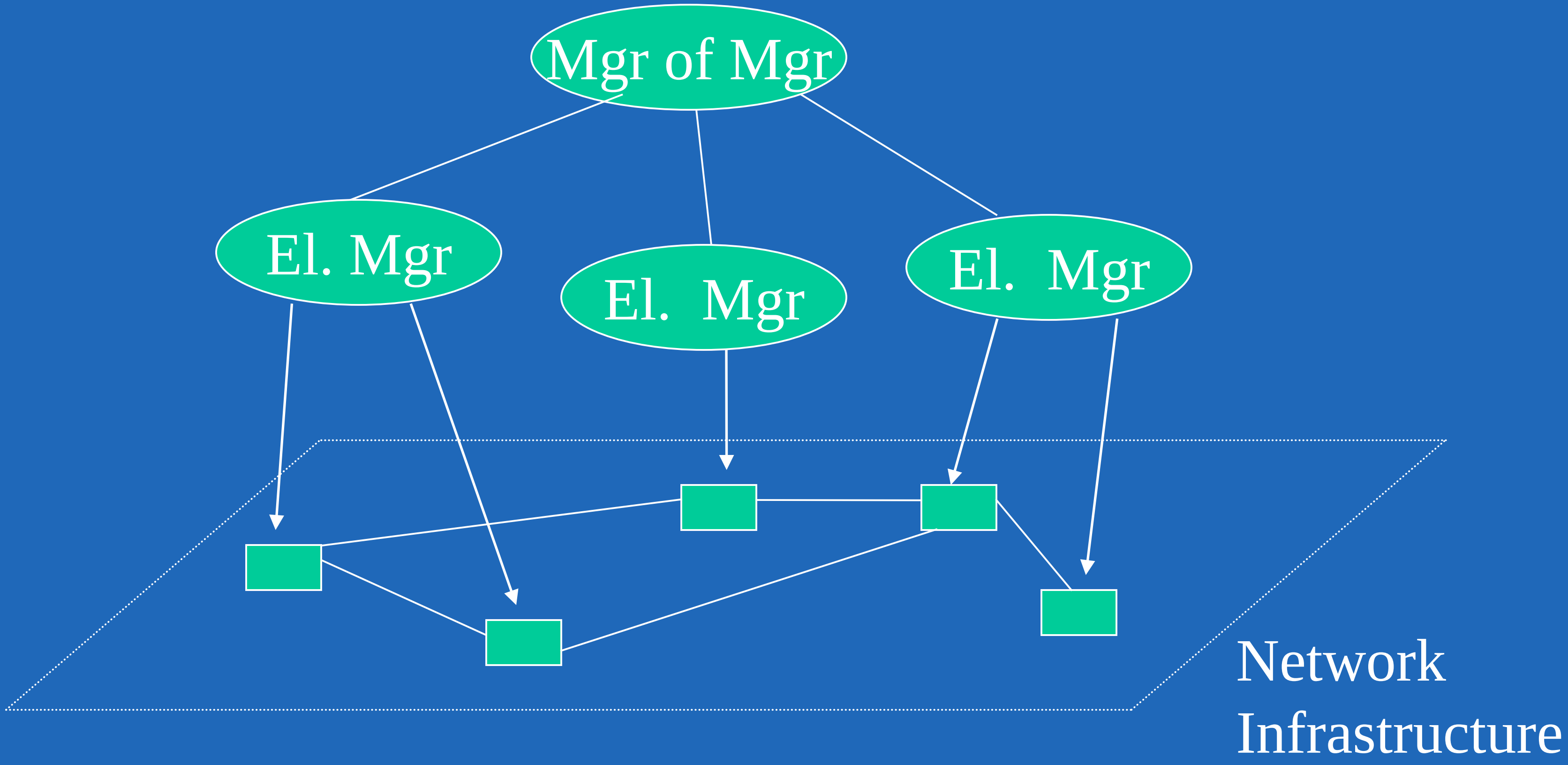


Hierarchical Mgrs

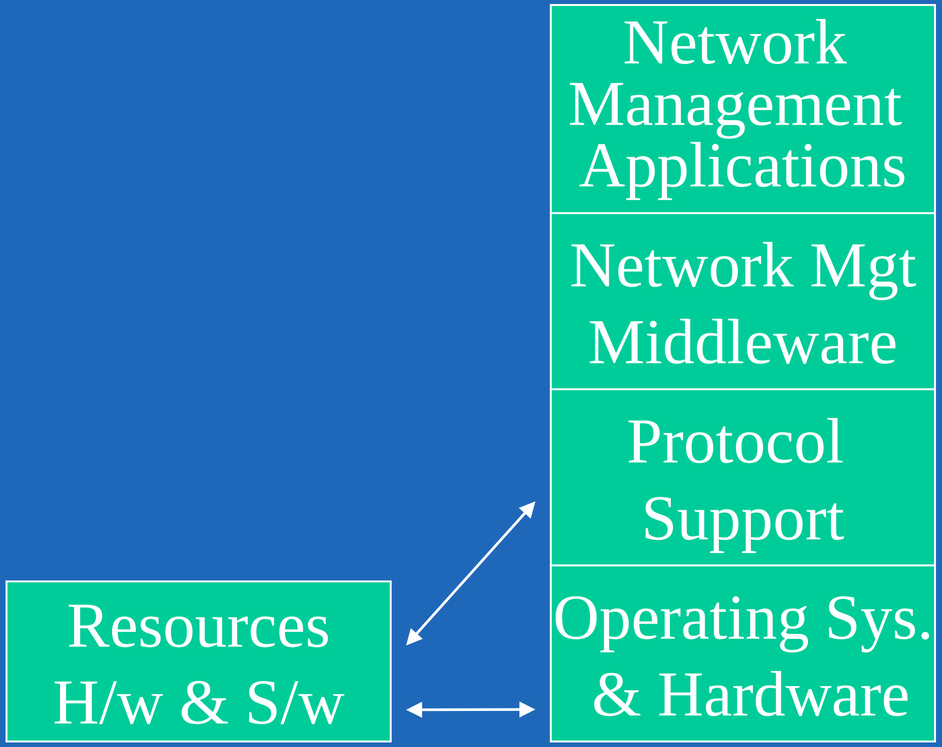
Hierarchical Net. Mgt

- Managers responsible for specific network resources (element managers)
- Allows hierarchy of managers (so called managers of managers or ‘MOMS’!)
- More common in large scale (WAN) networks

Hierarchy of Mgrs



Generalised Architecture for Network Management Systems



Network Management Applications

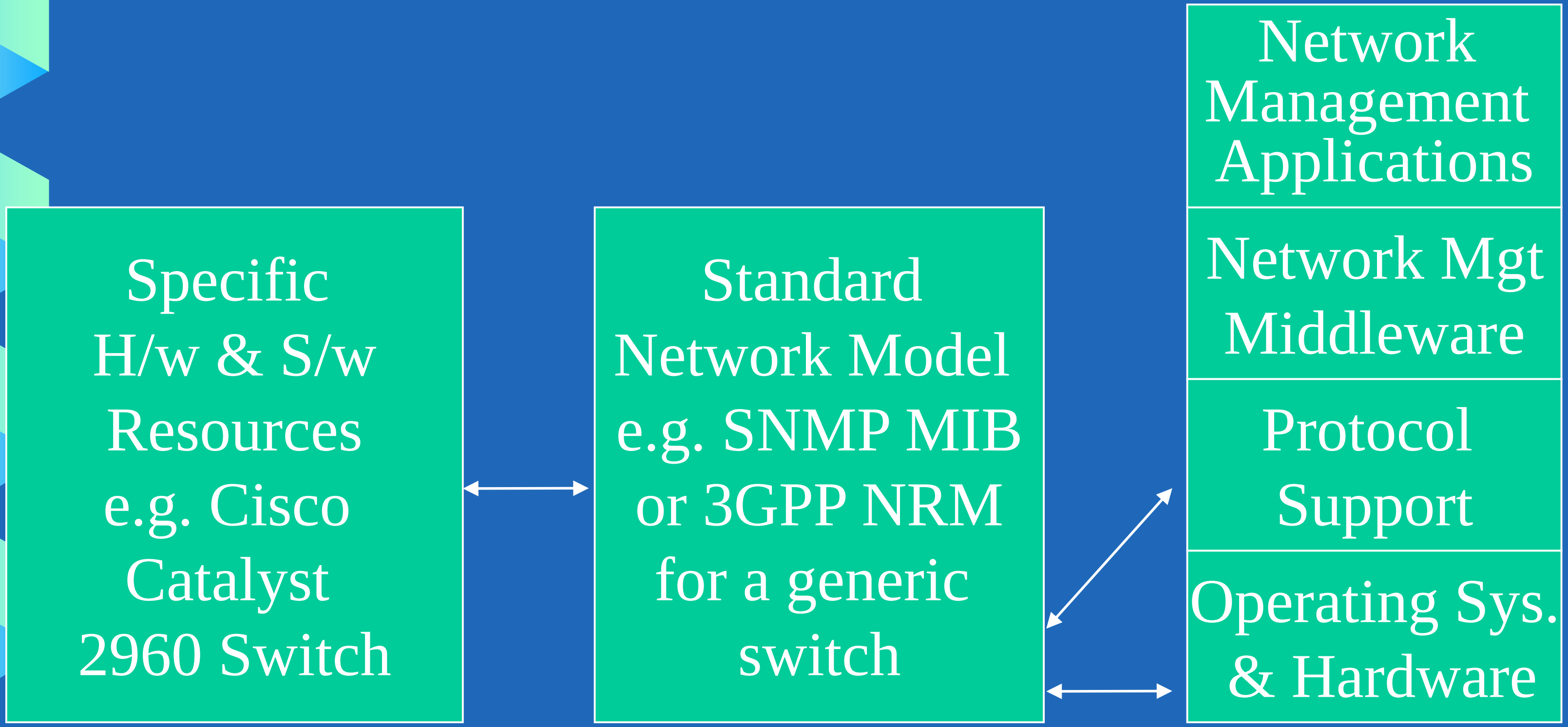
Network Mgt Middleware

Protocol Support

Operating Sys. & Hardware

Resources H/w & S/w

Extending Architecture with Standard Network Models



Specific H/w & S/w Resources e.g. Cisco Catalyst 2960 Switch

Standard Network Model e.g. SNMP MIB or 3GPP NRM for a generic switch

Network Management Applications

Network Mgt Middleware

Protocol Support

Operating Sys. & Hardware

Hardware Resources to be Managed

- Physical media & connections
- Computer Components (e.g. processors, printers)
- Connectivity & Interconnections components (e.g. routers, bridges, gateways, modems, hubs, . .)
- Telecommunications devices (e.g. switches . . .)

Software resources to be managed

- Application s/w & software tools including clients & servers
- Middleware (e.g. CORBA platform, NetWare ..)
- Operating systems
- Telecom Software (e.g. ATM controllers, etc.)

What Protocols support Mgt

- As management can be reduced down to monitoring & controlling, any protocol that can

  (1) retrieve information

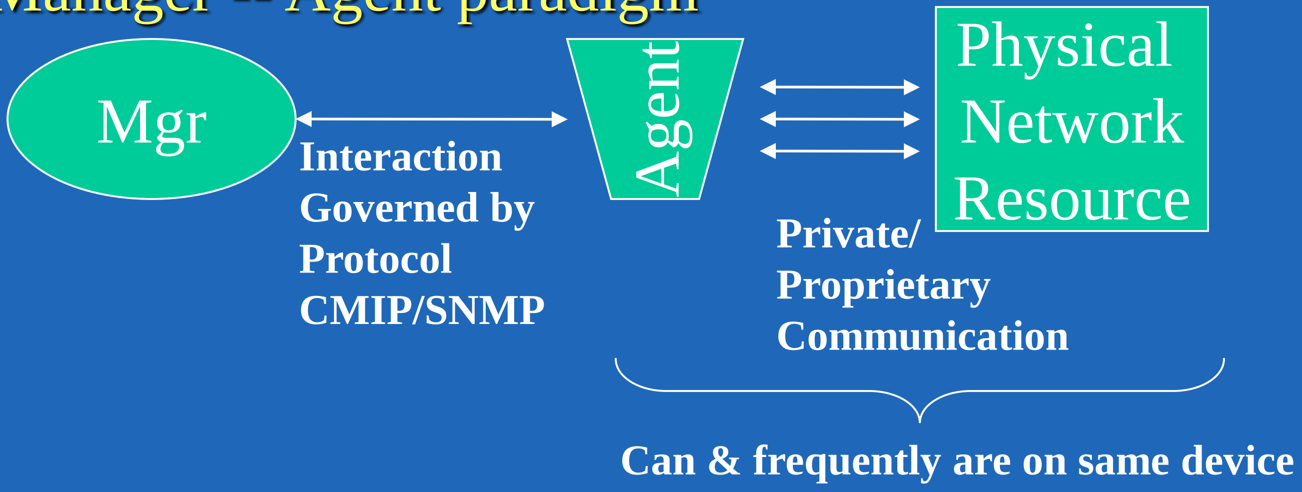
  (2) set/send information

  can be used as a management protocol

- However, two 'specific' mgt protocols have been agreed
  - Common Management Information Protocol (CMIP) from the Telecom Community (ITU)
  - Simple Network Management Protocol (SNMP) from the computer industry (IETF)
  - HTTP (?)

Network Management Middleware

- The choice of middleware is greatly affected by the choice of management protocol
- General Model (for SNMP & CMIP) is the use of the Manager -- Agent paradigm


Mgr
Agent
Physical Network Resource
Interaction Governed by Protocol CMIP/SNMP
Private/ Proprietary Communication
Can & frequently are on same device

Network Management Agents

- Varies in size & complexity greatly depending on CMIP/SNMP usage
- SNMP -
  - Agent very simple. Just consists of tables of information called a Management Information Base (MIB)
  - Small memory footprint and processing requirements
  - Primitive interaction between Mgr and Agent
  - Master / slave relationship between SNMP Mgr & Agent

    i.e. mgr must call or poll agent continuously for reliable information
  - Standard MIB specs. for different types of devices
  - Agent implemented by equipment vendor

Network Management Agents (cont 2)

- CMIP Agents
  - Much more complex & greater memory and processing overhead
  - Typically implemented on larger/more complex communication devices e.g. switches, some routers
  - Fully Object Oriented Information model (MIB)
  - Much more sophisticated interaction with manager
  - Much more local processing of raw data possible before returning information to manager
  - Agent can initiate Agent -- Manager dialogue (Alarm/Alert reporting)
  - Better security
  - Agent implemented by equipment vendor

Network Management Models (AKA Information Models, Network Resource Models, Management Information Bases)

- Provide a standard way to describe network resources in an application and vendor-independent way for manipulation/query by network management applications
- Typically defines
  - A modelling language for defining network resources, e.g.
    - Their configuration settings, e.g. WLAN SSID
    - Their state variables, e.g. number of connected devices
    - The notifications/events they generate e.g. No Internet connection
    - The hierarchy/connections of resources in the network
  - A global addressing/naming scheme for network resources
  - A set of standard or generic models for common network elements and resources e.g. routers, switches

Network Management Applications

- Generally speaking there is no uniform partition of the functional areas within network management

However:

- Most network mgmt. applications follow (loosely) the ISO functional mgmt. areas of **FCAPS**:
  - Fault - Performance
  - Configuration - Accounting
  - Security

- In ISO community these are referred to as systems mgt functions! Whereas in Internet community they are referred to as network mgt functions!

Fault Management

- Responsible for:
  - detection of a problem
  - fault Isolation
  - correction to normal operation
- uses **Polling** of managed objects to search for error conditions and/or report alarms/alerts,
  - Can also use **event reporting**
- illustrates the problem detected either as a graphic or in textual format

Configuration Management

Responsible for:

- Changes, additions and deletions on the managed object parameter(s)
- Needs to be co-ordinated with the network management systems personnel (frequently involve some manual work scheduling)
- Underlies most of the other network management functional areas

Accounting

Responsible for:

- Usually divided into three stages: metering, tariffing and billing.
  - **Metering** logs a particular usage of the managed object
  - **Tariffing** is the means by which a charge can be calculated e.g. Flat rate (e.g. leased line), incremental rate, variable rates etc.
  - **Billing** is the selection & application of a tariffing mechanism on the metered usage and the composition of the customer bill
- Typically ignored in LAN networks where tariffing and billing are irrelevant but VERY important for Telecom Network & Service providers

Performance Management

Responsible for:

- Optimisation of managed objects e.g. telephone truck line utilisation, bandwidth allocation in ATM network, load balancing on distributed servers
- Identification of bottlenecks in network and implementation of corrective action
- Divides into four main functions: Performance data collection, Data analysis, Problem Reporting, Display & formatting

Security management

Responsible for:

- administration of access controls on managed objects
- issuing of security alarm reports for violations. Several types of threat to assets:
  - Interruption, interception, modification and fabrication
- Assets:
  - Hardware, software, data and communication lines and networks
- Maintenance and security audit trail

But how is it all combined !!

- For simple management systems it is quite easy to choose a management product and management for a specific objective e.g. LAN traffic monitoring
- However, integrated network management applications for WAN are much more difficult
- Network Management Forum specified ‘Ensembles’ for ‘solutions to specific WAN scenarios e.g. configuration mgt for fixed point networks
- Ensembles are in fact vertical profiles of the total management architecture (i.e. spec. of mgt function, MIB objects, mgt protocol stack, and resource types to be managed)

Who Develops the management Systems?

Equipment Vendor

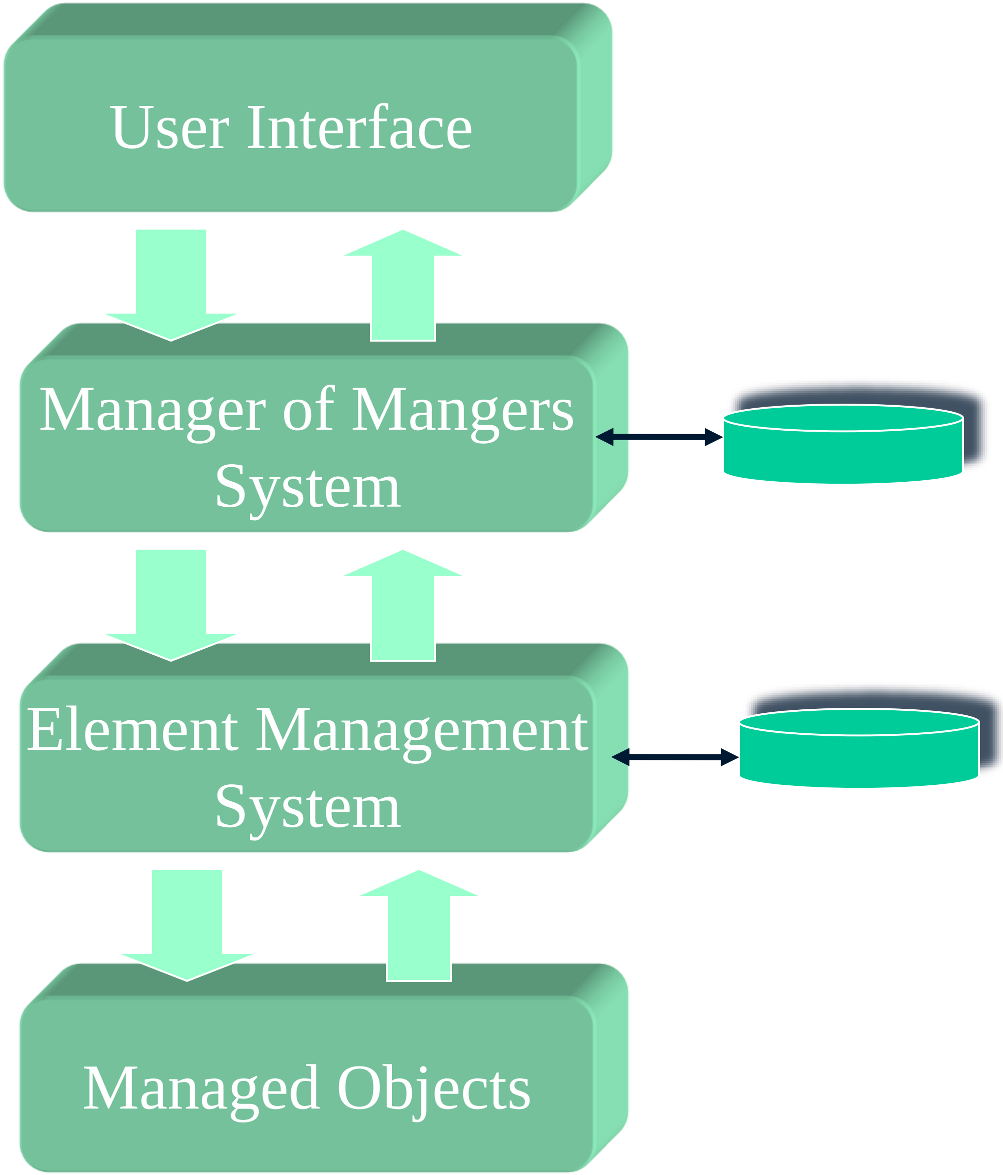
- responsible for implementation of Agent for particular network resource & implementation of network protocol to access/control that resource e.g. Cisco, Fore, etc . . .
- Can also develop management applications (bundled with equipment sale)

Management Platform vendor

- responsible for 'middleware' and some simple management application e.g. HP (HP Openview), IBM (TMN 6000), SUN (NetView)

Complex Management Applications & Integration

- outsourced to Niche network Management Integrator e.g. Siemens or implemented by Telcom operators themselves e.g. AT&T, B T



User Interface

Manager of Mangers System

Element Management System

Managed Objects

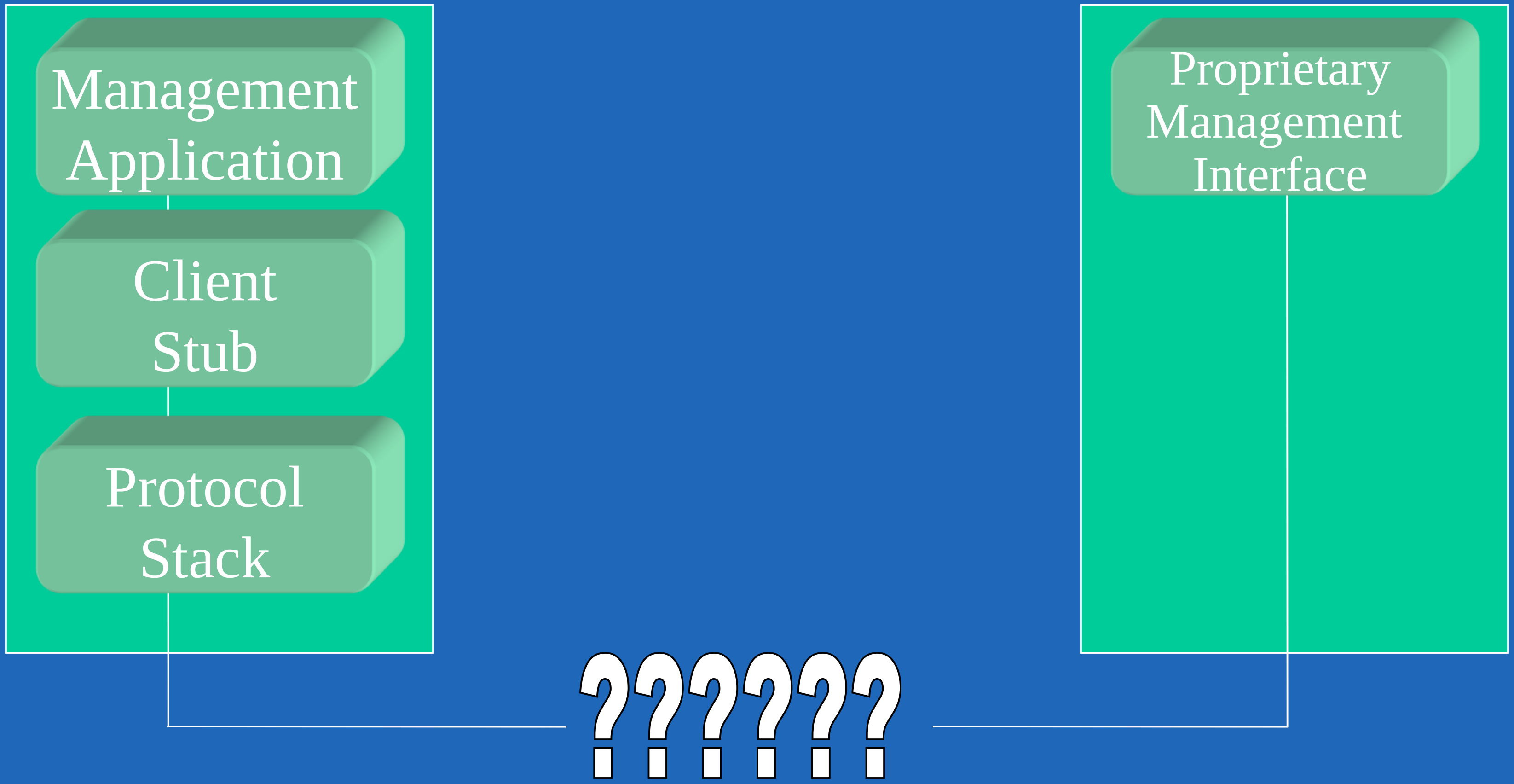
EXAMPLES

Integrates several mgr systems e.g. OSI NetExpert

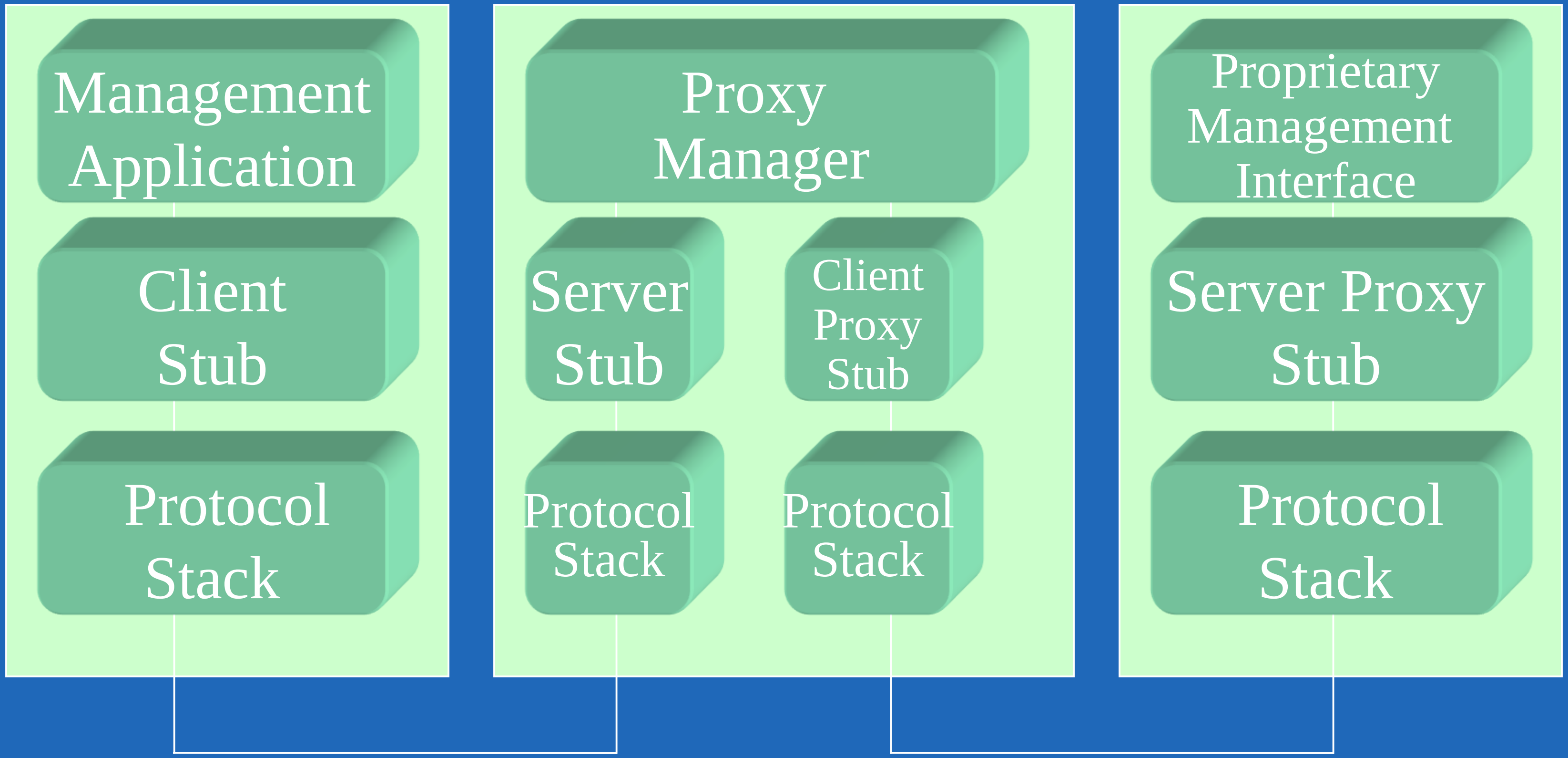
SunNet Manager, SNMP Manager

Routers, hosts, service & applications

Interworking between Different Network Management Systems



Interworking between Different Network Management Systems



Network Monitoring (revisited)

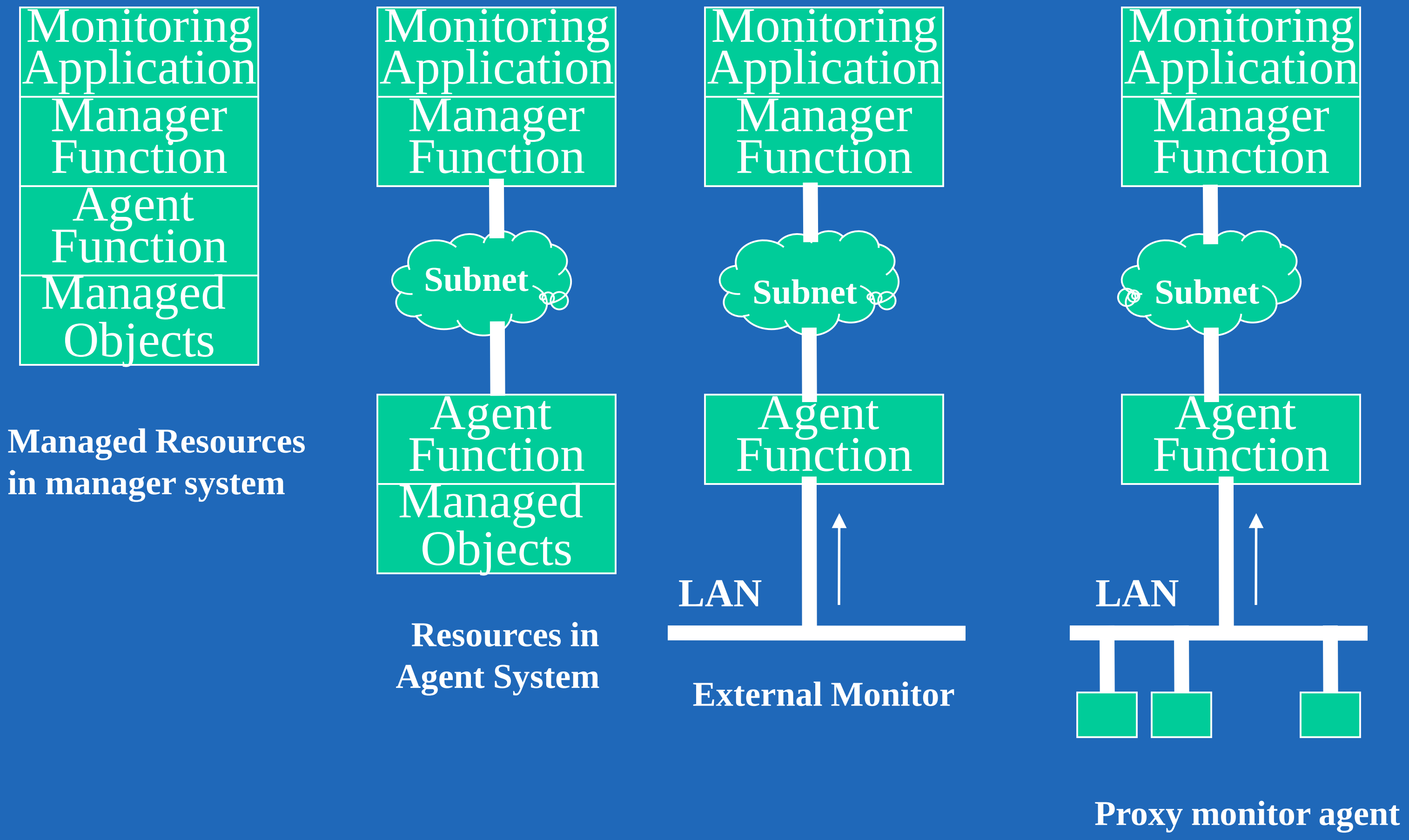
Recap:

- Net. Monitoring concerned with observing & analysing the status and behaviour of:
  - End Systems
  - Intermediate Systems
  - Sub networks
- Challenges of Net. Monitoring :
  - Gaining access to monitored information (e.g. definition of monitoring information, retrieval of that info.)
  - Design of monitoring mechanism
  - Usage of monitored information (e.g. by fault or performance accounting management applications)

Network Monitoring Information

- Static Information:
  - characterises current configuration (e.g. network element)
  - stored in network element
- Dynamic Information:
  - related to events in the network e.g. number of packets transmitted
  - collected and stored in network element but can be stored remotely (e.g. for some LAN based network elements)
- Statistical:
  - derived from dynamic information
  - gathered by any systems with access to dynamic information, i.e. by network element, remote monitor, or management application

Network Monitoring Configurations



Monitoring Application
Manager Function
Agent Function
Managed Objects

Managed Resources in manager system

Monitoring Application
Manager Function
Subnet
Agent Function
Managed Objects

Resources in Agent System

Monitoring Application
Manager Function
Subnet
Agent Function
LAN

External Monitor

Monitoring Application
Manager Function
Subnet
Agent Function
LAN

Proxy monitor agent

Polling vs Event Reporting

- Managers can gather information about network element via Polling and/or Event Reporting

Polling:

- Request - Response interaction between manager & Agent.
- Query can be specific (named parameter/object) or a general search
- Example uses: investigate (ping) problem
- Implementation effort centred on Manager

Polling Vs Event Reporting (cont.)

- Event Reporting:
  - Agent initiative to generate periodic report & send to manager
  - Reporting condition(s) may be pre-configured by manager
  - Example uses: significant change in Managed object values, unusual event.
  - Can be more efficient than Polling e.g. for monitoring managed objects whose states or values change relatively infrequently
  - Has less communication overhead that Polling

Polling vs Event Reporting (cont. 2)

- Both are useful information gathering techniques
- Telecoms world traditionally rely on event reporting where as SNMP world puts very little reliance on event reporting
- Choice depends on:
  - **Amount of network traffic generated by each method**
  - **Robustness in critical situations**
  - **Time delay in notifying network manager**
  - **Amount of processing in Managed devices**
  - **Particular network monitoring applications being supported**
  - **Contingencies required in case of notifying device fails before sending a report**

Performance Monitoring

First let's consider what indicators of performance are important

- Two categories of Performance indication
  - Service Oriented Measures
    - relate to satisfaction of service level agreements with users
  - Efficiency Oriented Measures
    - relation to meeting network requirements at minimum cost

Service Oriented Network Performance Indicators

- Availability:
  - Percentage of time a network system, component, or an application is available for a user
- Response Time:
  - Length of time it takes a response to appear at a user’s terminal after a user action calls for it
- Accuracy:
  - Percentage of time that no errors occur in the transmission and delivery of information

Efficiency Oriented Network Performance Indicators

- Throughput:
  - Rate at which application-oriented events occur e.g. transaction messages, file transfers, number of session for an application over a given time, number of calls for a circuit switched environment
- Utilisation:
  - Percentage of the theoretical capacity of a resource that is being used (e.g. transmission line, switch etc.)

Availability

- Expressed as percentage of time a network system, component, or an application is available for a user

  => Based on reliability of individual components of network

- Reliability is the probability that a component will perform its specified function for a specified time used under specified conditions

- Component failure is expressed as ‘mean time between failures’ (MTBF)

$$\Rightarrow \text{Availability} = \frac{\text{MTBF}}{(\text{MTBF} + \text{MTTR})}$$

  where MTTR is ‘Mean time between Repair’ following a failure

Response Time

- Is time it takes to react to a given input
- Achievable with

  (i) increased cost of computer processing power

  (ii) trade-offs with other requirements

- Two forms of response time:
  - User Response Time - timespan between moment user receives complete reply to one command and enters the next command
  - System Response Time - timespan between moment a user enters a command and the moment a complete response is displayed on the terminal

Elements of Response Time

- Seven elements of response time typically found in most monitoring applications
- Inbound terminal delay: delay in getting an inquiry from the terminal to the communication line. Is directly dependent on transmission rate from terminal to controller
- Inbound queuing time: time required for processing by the controller or PAD* device. E.g. can be dependent on buffer/queue size and load on controller
- Inbound service time: time taken to transmit over comms. link, network or other communications facility from the controller to the host's front -end processor

*packet assembler/disassembler

Elements of Response Time (cont. 2)

- Processor delay: Time front-end processor, disk drives etc. on computer spend preparing a reply to the original inquiry
- Outbound queuing time: time reply spends at a port in the front-end processor waiting to be dispatched on the network or communication line
- Outbound service time: time to transmit the communications facility from the host’s front end processor to the controller

Elements of Response Time (cont. 3)

- Outbound Terminal delay: the delay at the terminal itself - primarily due to line speed.

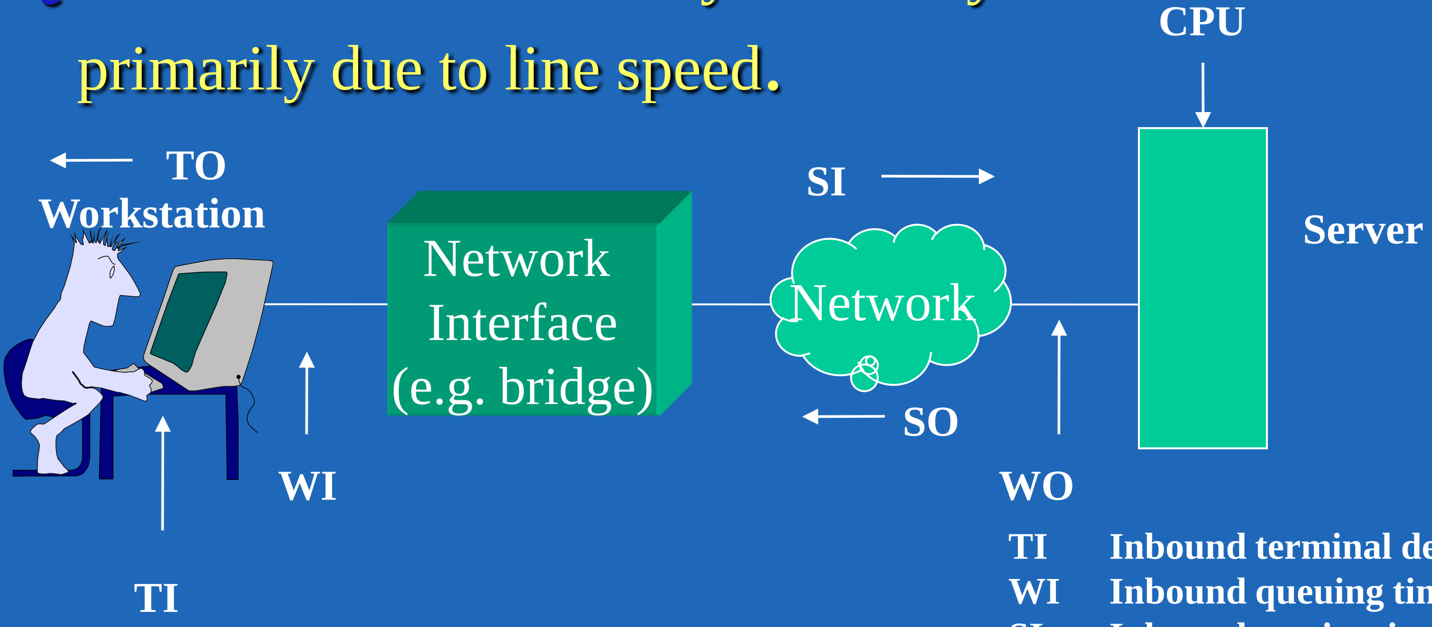


Illustration of Response Elements

TI	Inbound terminal delay
WI	Inbound queuing time
SI	Inbound service time
CPU	CPU Processor Delay
WO	Outbound queuing time
SO	Outbound service time
TO	Outbound Terminal Delay

Accuracy & Throughput

- Accuracy
  - Because of built-in error correction (in data link and transport protocols), accuracy is generally not a user concern
  - Nevertheless useful to monitor rate of errors that must be corrected
- Throughput
  - is an application oriented measurement (calculation of the rate at which they occur)
  - Examples include
    - Number of transactions of a given type in a certain period
    - Number of customer sessions for a given application during a certain period of time
    - Number of calls for a circuit-switched environment

Utilization

- Is a more fine grained measure than throughput
- Concerned with percentage of time that a resource is in use over a given period of time
- Useful in determining network bottlenecks and congestion
- Response time usually increases exponentially as utilization of a resource increases

Utilization (cont. 2)

- One technique to measure utilization is to observe differences between planned load and actual load on various links in a network
  - Planned load is reflected by capacity (bits per second) of each individual link
  - Actual load is the measured average traffic (bits per sec)
  - Comparison of the planned load and actual load on each link can identify inefficient allocation of resources
  - A closer balance between planned load and actual load can be achieved => reducing the total capacity and resulting in more efficient usage of resources

Performance-Monitoring Functions

- Having looked at Performance Indicators - now lets look at the actual Performance Monitoring Function/Activities
- Can be thought of as divided into three components:
  - Performance Measurement which is concerned with actual gathering of statistics about network traffic and timing
  - Performance Analysis which is concerned with software for reducing and presenting data
  - Synthetic Traffic Generation which is concerned with observation of network under controlled load(s)

Performance Measurement Functions

- Often performed by Agent within network element (e.g. router)
    - e.g. Observes the amount of traffic into/out of a network element, number of connections (at various levels of network protocol stack), and traffic per connection
- Can be expensive (in processing time) on the network element
- In LANs remote (external) monitoring can be used to observe network traffic (broadcast/shared network)

Example Questions that Performance Measurement reported in LAN should answer

- Is traffic evenly distributed among the network users or are there source-to-destination pairs with unusually heavy traffic ?
- What is the percentage of each type of packet? Are some packet types of unusually high frequency ? (could indicate an error or an inefficient protocol)
- What is the distribution of data packets sizes ?
- What is the channel utilization and throughput ?

Fault Monitoring Functions

- Must detect and report faults
- at minimum agent will maintain a log of significant events & errors
- If Managers use polling => heavy reliance on agent fault/error logs
- If Agents use event reporting => importance of tight criteria for issuing fault reports in order to avoid an ’event storm’
- Fault Monitor should also anticipate faults e.g. setting thresholds for event reporting

Fault Monitoring functions

- Should also assist in isolating & diagnosing faults
- For example Fault Monitoring functions might include:
  - Connectivity test
  - Protocol integrity test
  - Connection saturation test
  - Function test
  - Data integrity test
  - Data saturation test
  - Response time test
  - Loopback test

Accounting Monitoring Functions

- Keeps track of users' usage of network resources
- Typical accounting data for network may include:
  - user identification
  - receiver identification - network resource to which connection was attempted and/or made
  - number of packets transmitted
  - security levels – identify transmission and processing priorities
  - time stamps – for principle transmission & processing event, e.g. start and stop times
  - resources used

Network Control

- Much of network control is concerned with Configuration Management and Security Management
- Configuration Management is concerned with:
  - initialization, maintenance & shutdown of individual components and logical subsystems within total computer & communication installation
- Managed resources include physical resources (e.g. server, router) and logical resources (e.g. buffer queues, timers etc.)
- While network in operation, configuration management is responsible for monitoring the configuration and making changes in response to user commands

Configuration Management

Includes:

- Definition of configuration information
- Set and Modify operations (for attribute values)
- Definition and Modification of Relationships
- Initialization and Termination of Network Operations
- Distribution of software

Configuration Control

- Examination of values and relationships
- Reporting of configuration status

Configuration Monitoring

Configuration Information

- Describes nature & status of resources
- Covers both specification of resource(s) and attributes of those resources
- Resources can be physical (router) or logical (counters, timers)

Structure of Configuration Information

Several alternatives

- as simple structure list of data fields (each field containing single value)
- as fully object oriented model (encapsulation of data, inheritance, behaviours etc.)
- as relational tables

Storage of Configuration Information

- Although sometimes stored in manager, more typically configuration information is stored
  - in agent
  - in network element
  - in a proxy for a network element

Configuration Functions

- Enable user to specify range and type of values to which specified resource attributes at a particular agent should be set
- Enable user to define new object types (or data element types) online (rarely actually implemented in config. mgt systems) or off line (more common in config. mgt systems)
- Enable user to load pre-defined attribute values (e.g. default states & values) on a systemwide, individual node or individual layer basis

Set & Modify Attribute Values

- Config. Control function should enable a manager to remotely set & modify attribute values in agents & proxies
- Limitations
  - Mgr. authorised to make the setting/modification
  - Setting/modification reflect ‘reality’ of resource

Categories of Modification effects

- Data update only: modification of value(s) in agents database of values
- Data update & resource modification: modify command affects underlying resource (e.g. disable physical port of device)
- Data Update & Action: modification to value in Agent database causes agent to initiate certain action(s) e.g. reinitialize parameter in router

Define / Modify Relationships

- Relationship: describes association, connection or condition that exists between network resources e.g. Topology Relationship, Hierarchy, Physical or Logical Connection, Management Domain
- Management Domain: is set of resources that share a set of common management attributes or a set of common resources that share the same management authority
- Configuration Mgt should allow user to add, delete & modify the relationships among network resources

Initialize & Terminate Network Operations

- Include mechanisms to enable user to initialise & close down network or subnetwork operation
- Initialisation: includes verification of all settable resource attributes & relationship a proper; Notification of users of any resource, attribute or relationship requiring modification/setting; Validation of user's initialisation commands
- Termination: includes user retrieval of specified statistics, blocks or status information before termination procedures are completed

Distribution of Software

- Ability to distribute software throughout the configuration (e.g. hosts, servers, & workstations, bridges, routers, & applications)
- Facilitates software loading requests, transmission of specified versions of software, and update of configuration tracking system
- Includes distribution of tables and other data that drive behaviour of a system/resource
- Includes ability to examine, update & manage different version of software & routing information