CSIT985
Strategic Network Design

Spring 2023

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Lecture week 9:

Network Management

Presented by: Dr. Chau Nguyen

Lecturer, School of Computing and Information Technology, UOW

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Outline

- Network Management Architectures
- Network Devices and Characteristics
- Network Management Mechanisms
  - Monitoring Mechanisms
  - Instrumentation Mechanisms
  - Configuration Mechanisms
- Architectural Considerations
  - In-band and Out-of-band management
  - Centralized, distributed, and hierarchical management
  - Scaling network management traffic
  - Checks and balances
  - Management of Network Management Data
  - MIB selection
  - Internal relationships
  - External relationships

Network Management Architectures

Network Management Architectures

- Network management's functions: *control, plan, allocate, deploy, coordinate,* and *monitor* network resources.

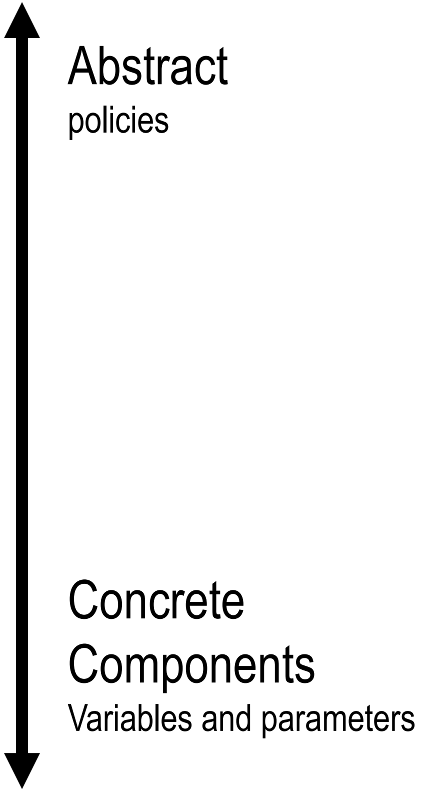
- Areas to be addressed include
  - Deciding which network management protocol
  - Reconfiguration of the network to meet changing requirements
  - Testing service-provider compliance with SLAs and policies
  - Proactive monitoring
  - Implementing high-level asset management

Network Management Architectures

- What dose the structure cover?
  - Business management
  - Service management
  - Network management
  - Element management
  - Network-element management

Network Management Architectures

- Network management can be viewed as a multiple layer structure
  - Business Management
    - Budgets, resources, planning, agreements
  - Service Management
    - Access bandwidth, data storage, application delivery
  - Network Management
    - All devices across the entire network
  - Element Management
    - Collections of similar network devices
    - E.g., access routers, subscriber management systems
  - Network-Element Management
    - Individual network devices
    - E.g., a single router



Abstract
policies

Concrete
Components
Variables and parameters

Network Management Architectures

- Two Basic Functions
  - Transport of management information across the network
  - Management of network management information elements
- Four Categories of Network Tasks
  - Monitoring for event notification, or for trend analysis and planning
  - Configuring network parameters
  - Troubleshooting the network
  - Planning

Network Management Architectures

- Two Basic Functions
  - Transport of management information across the network – (SNMP)
  - Definition and Management of network management information elements → MIB

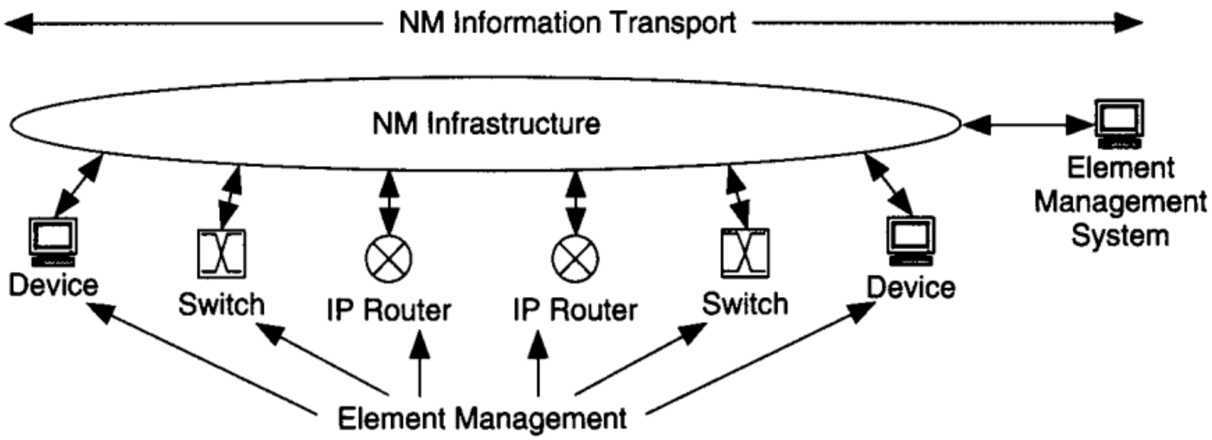


Fig. Network Management is composed of Managing Elements and Transporting Management Data (McCabe, 2010, p.302)

Network Management Architectures

- Four Categories of Network Tasks
  - Monitoring for event notification
  - Monitoring for trend analysis and planning
  - Configuring network parameters
  - Troubleshooting the network
- Examples of some of the things we can monitor as availability, capacity, delay, throughput, error rates, disc space etc.

Network Device and Characteristics

Network Devices and Characteristics

- Network device
  - An individual component of the network that participates at one or more layers of the protocol
  - End devices, routers, switches, hubs etc.

Network Devices and Characteristics

- Network characteristics can be per element, per link, per network, or end-to-end.

- End-to-end characteristics
  - Can be measured across multiple network devices in the path of one or more traffic flows
  - May be extended across the entire network or between devices
  - Availability, capacity, delay, jitter, throughput, error rates etc.

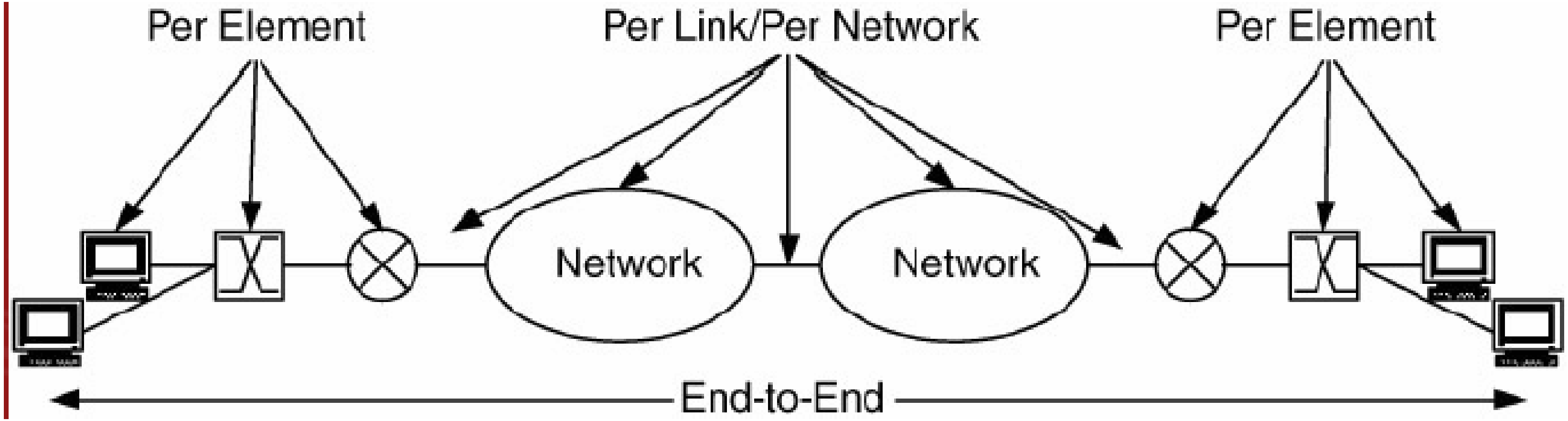


Fig. Network Characteristics Can Be per-Element, per-link, per-Network, or End-to-End (McCabe, 2010, p.303)

Network Devices and Characteristics

- Per link/network/element characteristics
  - Specific to the type of element or connection between elements
  - May be used individually or combined to form an end-to-end characteristic
  - Per link : Propagation delay, link utilization
  - Per element: IP forwarding rates, buffer utilization

Network Devices and Characteristics

- Management of network devices includes
  - Network planning
  - Initial resource allocation
  - FCAPS model from the telecommunication network management: **fault**, **configuration**, **accounting**, **performance**, **security management**

Network Management Mechanisms

Network Management Mechanisms

- Providing mechanisms for retrieving, changing, and transport of management information across the network

- One major protocol you should have knowledge of:
  - Simple Network Management Protocol (SNMP)
    - Dominant method you should spend time learning

- The next protocol is of historic interest
  - Common Management Information Protocol (CMIP)
    - Including CMOT which is CMIP Over TCP/IP
    - More complicated than SNMP

Network Management Mechanisms

- SNMP (*IETF*)
  - Provides facilities for collecting and configuring parameters from network devices
  - Unsolicited notification of events through traps
  - Accessible parameters are group into Management Information Bases (MIBs)
  - SNMPv3
    - More secure authentication
    - Ability to retrieve blocks of parameters
    - Trap generation for most parameters

Network Management Mechanisms

- CMIP/CMOT (OSI)
  - Parameter collection and setting
  - More operation types than SNMP
  - These can be provided by SNMP by creating new MIBs

Network Management Mechanisms

- Defining properties that need to be measured and managed in devices
  - Management Information Base (MIB)

What is an MIB?

- An MIB contains definitions and information about the properties of managed resources and the services that the agents support.

- The manageable features of resources, as defined in an SNMP-compliant MIB, are called managed objects or management variables (or just objects or variables).

MIB-II

- An example of a base set of parameters to monitor can be developed from the standard MIB-II.
- The following parameters can be collected on a per-interface basis:

ifInOctets	Number of bytes received
ifOutOctets	Number of bytes sent
ifInUcastPkts	Number of unicast packets received
ifOutUcastPkts	Number of unicast packets sent
ifInNUcastPkts	Number of multicast/broadcast packets received
ifOutNUcastPkts	Number of multicast/broadcast packets sent
ifInErrors	Number of erroneous packets received
ifOutErrors	Number of packets that could not be sent

Remember!

- MIB is not a database!
- Its an abstraction of the real word!

Network Management Mechanisms

- Monitoring mechanisms
- Instrumentation mechanisms
- Configuration mechanisms

Network Management Mechanisms:

Monitoring Mechanisms

Monitoring Mechanisms

Obtaining values for end-to-end, per link/element characteristics

- Collection (polling) – actively probing devices
- Processing
  - event notification or
  - trend analysis – data averaged over time
- Display (tables or graphs on a VDU, flashing lights, log, etc.)
  - VDU (Virtual Display Unit)
- Archiving
  - what should be stored, where should it be stored and when should it be stored

Monitoring Mechanisms

- Values for some characteristics will need to be derived from gathered data

- How and what you display about this information needs to be decided
  - Type of monitor
    - Standard VDU, Wide screen, multi screen etc.
  - Display techniques
    - Logs, textual, graphs, charts, alarms
    - Animation, abstraction (e.g. clouds)

- Some or all of this information will need to be saved

Monitoring Mechanisms

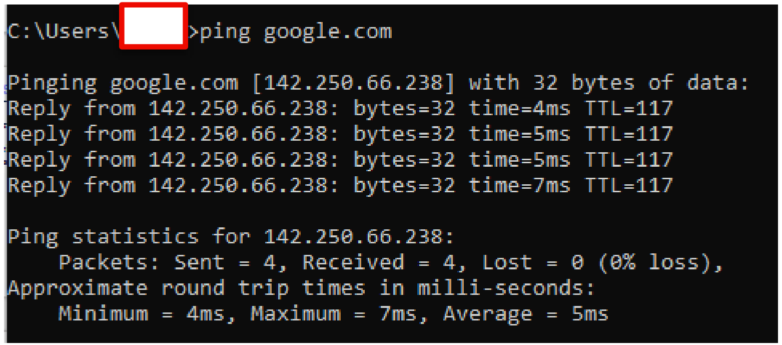
- Direct access e.g. via CLI (command line interface)
- Programs such as Nagios, Zabbix provide the means by which various information can be consolidated

Monitoring Mechanisms

- Using ICMP e.g. ping command in Unix, Linux, or Windows command line or software package
  - Internet Control Message Protocol, an extension to the Internet Protocol (IP)
  - ICMP allows for the generation of error messages, test packets and informational messages related to IP

Monitoring Mechanisms

- From Windows/Mac Terminal try the following
  - C:\>ping google.com
  - The default is only 32 bytes which is fine for simple connectivity tests but does not put much load on the link.

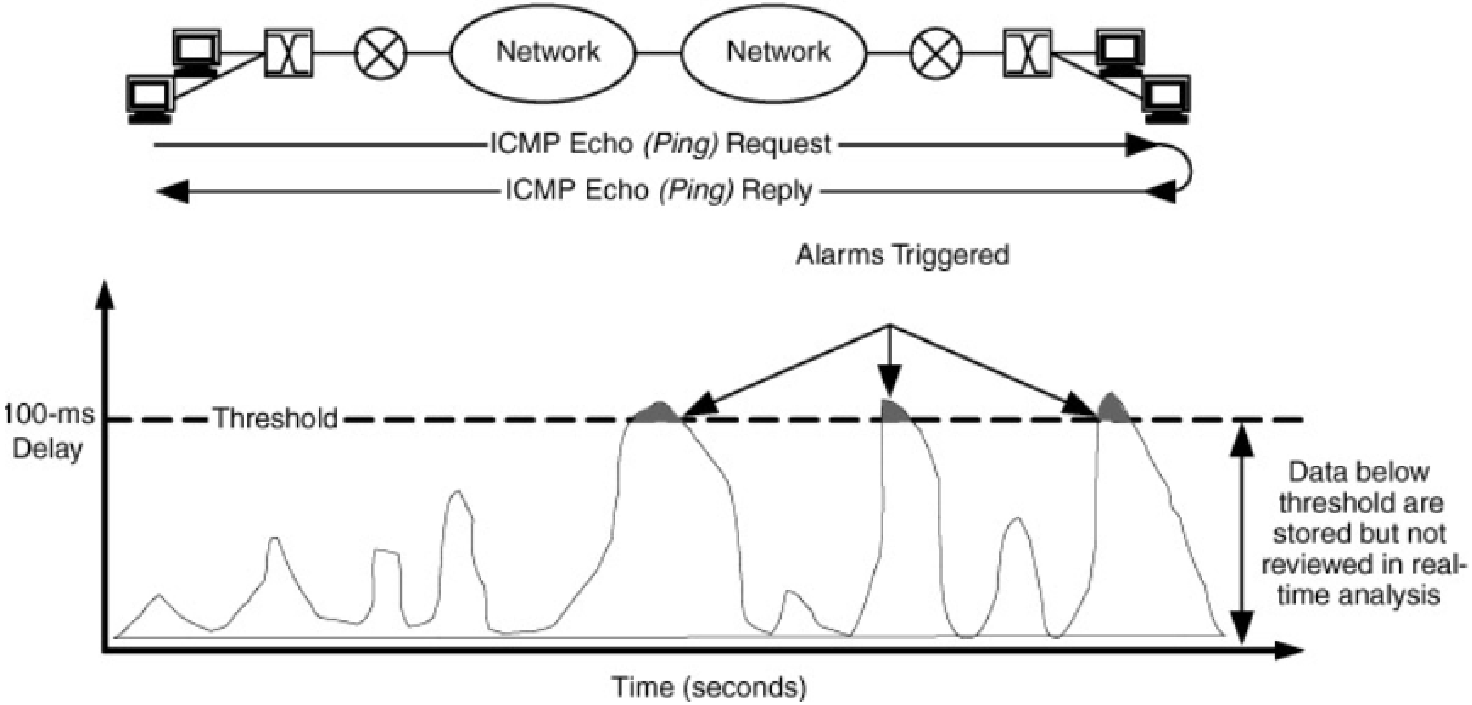


```
C:\Users\[redacted]>ping google.com

Pinging google.com [142.250.66.238] with 32 bytes of data:
Reply from 142.250.66.238: bytes=32 time=4ms TTL=117
Reply from 142.250.66.238: bytes=32 time=5ms TTL=117
Reply from 142.250.66.238: bytes=32 time=5ms TTL=117
Reply from 142.250.66.238: bytes=32 time=7ms TTL=117

Ping statistics for 142.250.66.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 7ms, Average = 5ms
```

Monitoring for Event Notification

- An event is something that occurs in the network that is worth noticing
  - Problems and failures
  - Characteristics that cross thresholds
  - Informational to user, administrator or manager
    - Notification of upgrade
- Events that are short-lived changes in the behaviour of the network
  - require real-time analysis
- Real-time analysis has short polling intervals
  - Trade off between
    - Number of characteristics and network devices polled
    - Resources required to support the analysis

Figure 7.5: Monitoring for event notification


Network
Network
ICMP Echo *(Ping)* Request
ICMP Echo *(Ping)* Reply
Alarms Triggered
100-ms Delay
Threshold
Data below threshold are stored but not reviewed in real-time analysis
Time (seconds)

(McCabe, 2010, p.306)

Monitoring for Event Notification

- May be noted
  - In a log file
  - On a display
  - By issuing an alarm

Monitoring for Event Notification – Example

- The data from Real Time Analysis can affect overall network performance
- Consider a network with one hundred (100) network devices
- Each device has an average of four (4) interfaces
- Each interface monitored for eight (8) characteristics

Monitoring for Trend Notification – Example

- This is calculated as follows
  - (100 network devices) x (4 interfaces/network device) x (8 characteristics/interface) = 3200 characteristics
- If each characteristic generates an average of 8 bytes of data and 60 bytes of protocol overhead, each polling session generates
  - (3200 characteristics) x (68 bytes) = 217600 bytes of data or 1740800 bits/session or 1.74 Mb of traffic

Monitoring for Trend Notification – Example

- If we assume each polling interval is 5 secs
  - at best each polling interval will generate 348Kb/s (if spread over 5 secs)
  - If we assume the worst, there will be a 1.74Mb/s spike after each poll.
- For a period of one day
  - (1,740,800 bits per polling interval) x (720 polling intervals/hour) x (24 hours/day) = 30081024000 bits per day approximate 30.2 Gb of traffic
- Data stored
  - (3200 characteristics/polling interval) x (8 bytes) x (720 polling intervals/day) x (24 hours/day) = 442368000 approximate 442 MB of data stored/day
- Over a year, this would add up to more than 161 GB of data

Monitoring for Trend Analysis

- Trend analysis uses network management data to determine the long-term network behaviour
- Continuous, uninterrupted data collection can be used for baseline establishment
- These baselines can be used to plot trend behaviour

Monitoring for Trend Analysis

- Availability, Delay and Utilisation
- Upwards trends are clearly visible for delay and percentage of utilization

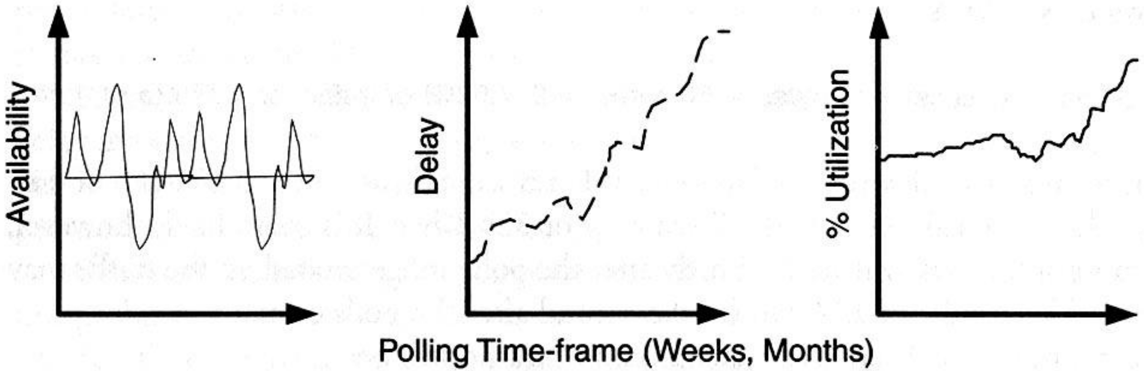


FIGURE 7.6 Monitoring for metrics and planning.

(McCabe, 2010, p.308)

Network Management Mechanisms:
Instrumentation Mechanisms

Instrumentation

- Set of tools and utilities needed to monitor and probe the network for management data
- Includes access to management data via
  - SNMP
  - Monitoring tools
  - Direct access

Instrumentation

- Monitoring tools include
  - Utilities
    - Ping, traceroute, TCPdump
  - Direct access
    - Telnet, FTP, TFTP

Instrumentation

- Need to ensure accuracy of data
  - Collection from different points
- Needs to be dependable
  - Separation and replication

Network Management Mechanisms:

Configuration Mechanisms

Configuration Mechanisms

- Setting parameters for operation and control of network device
- Including
  - Direct access to devices
  - Remote access to devices
  - Downloading configuration files

Configuration Mechanisms

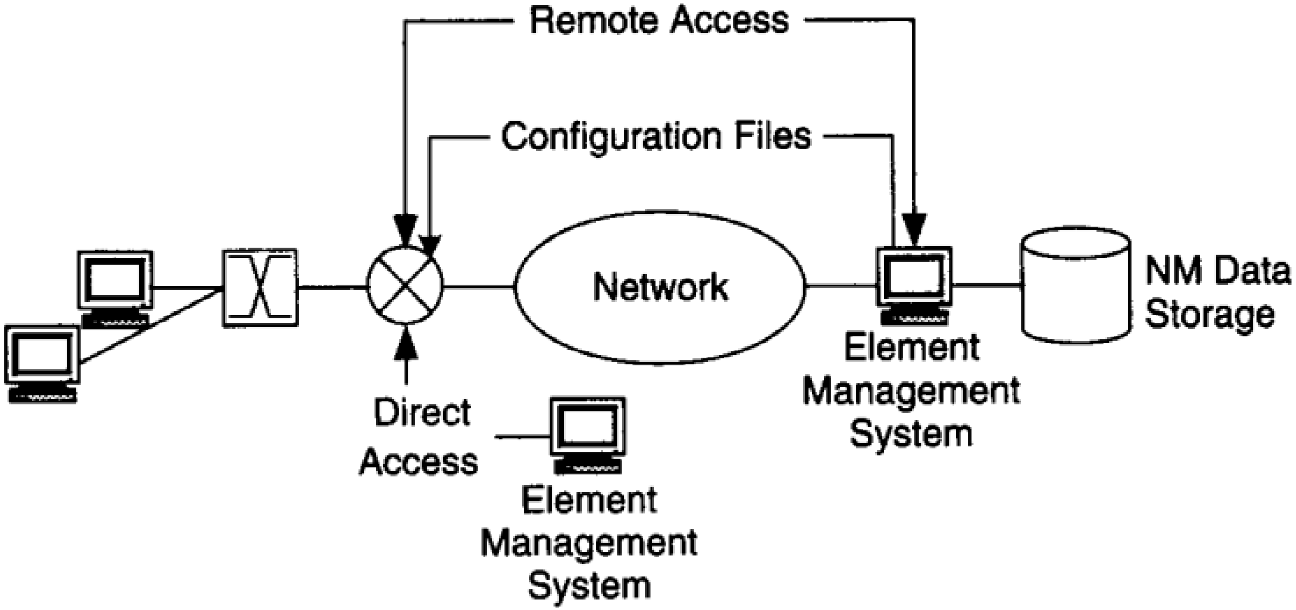


FIGURE 7.7 Configuration Mechanisms for Network Management

(McCabe, 2010, p.310)

Architectural Considerations

Architectural Considerations

- Need to choose
  - Which characteristics to monitor/manage?
  - What instrumentation is required?
  - What information will be displayed? How?
  - What data will be stored? For how long?

Architectural Considerations

- FCAPS model:
  - Fault management
  - Configuration management
  - Accounting management
  - Performance management
  - Security management

Architectural Considerations

- The network management architecture needs to consider
  - In-band and out-of-band management
  - Centralized, distributed and hierarchical management
  - Scaling of network management traffic
  - Checks and Balances (do two sources of information exist)
  - Management of network management data
  - MIB selection
  - Internal relationship
  - External relationship

In-band and Out-of-band Management

- In-band
  - Network management data uses the same network paths as flows for users and their applications
  - A separate management path/network is NOT required but…
  - Management data flows CAN be affected by the same problems as user traffic

In-band and Out-of-band Management

- Out-of-band
  - An alternative path is provided for network management data flows
  - Network management systems can continue to monitor network during MOST network events
  - Usually provided via a separate network
    - E.g., POTS *(Plain Old Telephone Service)*
  - Additional security features can be integrated into this network
  - Added expense and complexity of having a separate network

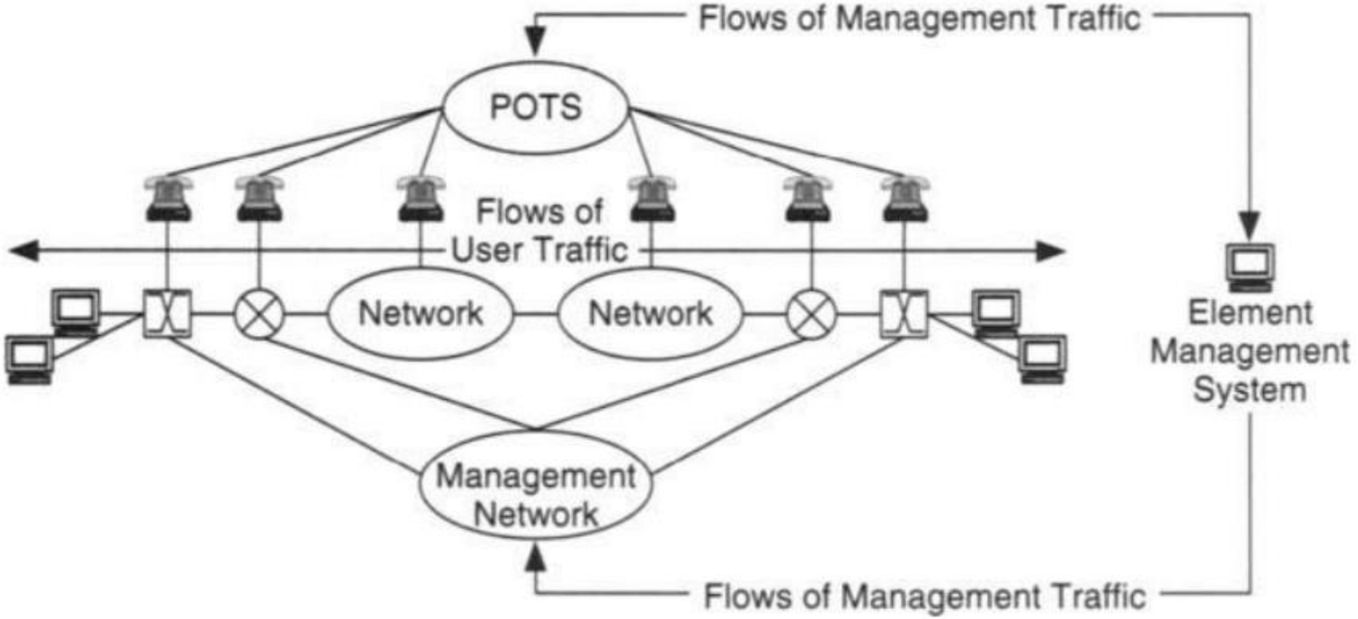


FIGURE 7.9 Traffic Flows for Out-of-Band Management

(McCabe, 2010, p.313)

In-band and Out-of-band Management

- Hybrid In-band/Out-of-band
  - There is sense in having a combination of both where in band methods enables data intensive network management applications while out of band provides basic monitoring should the user data network fails
  - The weaknesses of both are also incurred
    - increased security vulnerability and added expense of a separate network.

Centralized, Distributed and Hierarchical Management

Centralized

- All management data radiates from a single management system
- Management flows then behave like a client server system

- Advantage
  - Simplified architecture
  - Reduced costs
- Trade offs
  - Single point of failure
  - All management flows converge to a single point
    - Congestion

Centralised, Distributed and Hierarchical Management

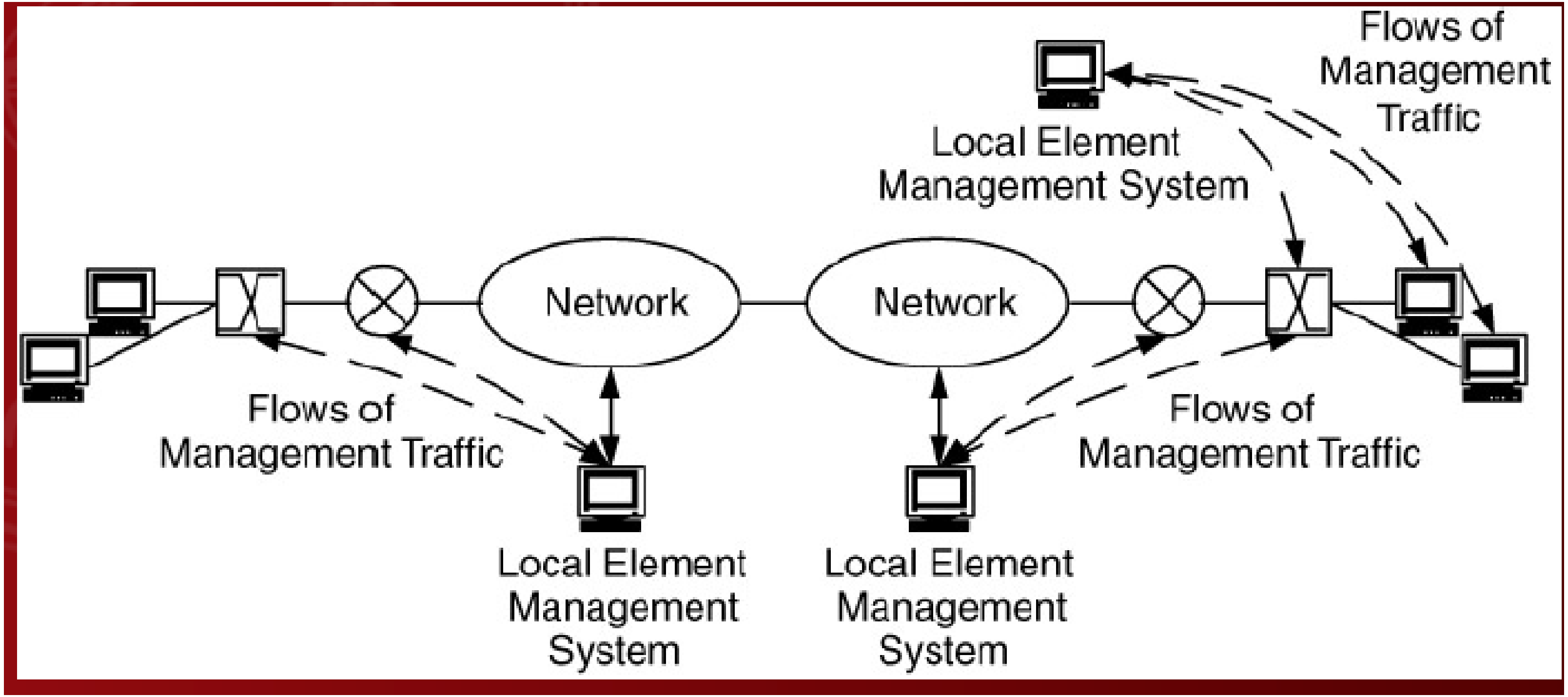
Distributed

- Multiple separate components
  - Strategically placed
  - Distributing management domains
  - Either components provide all management functions or distributed devices are monitoring devices

- Advantage
  - Monitoring devices localize traffic
  - Redundancy of monitoring

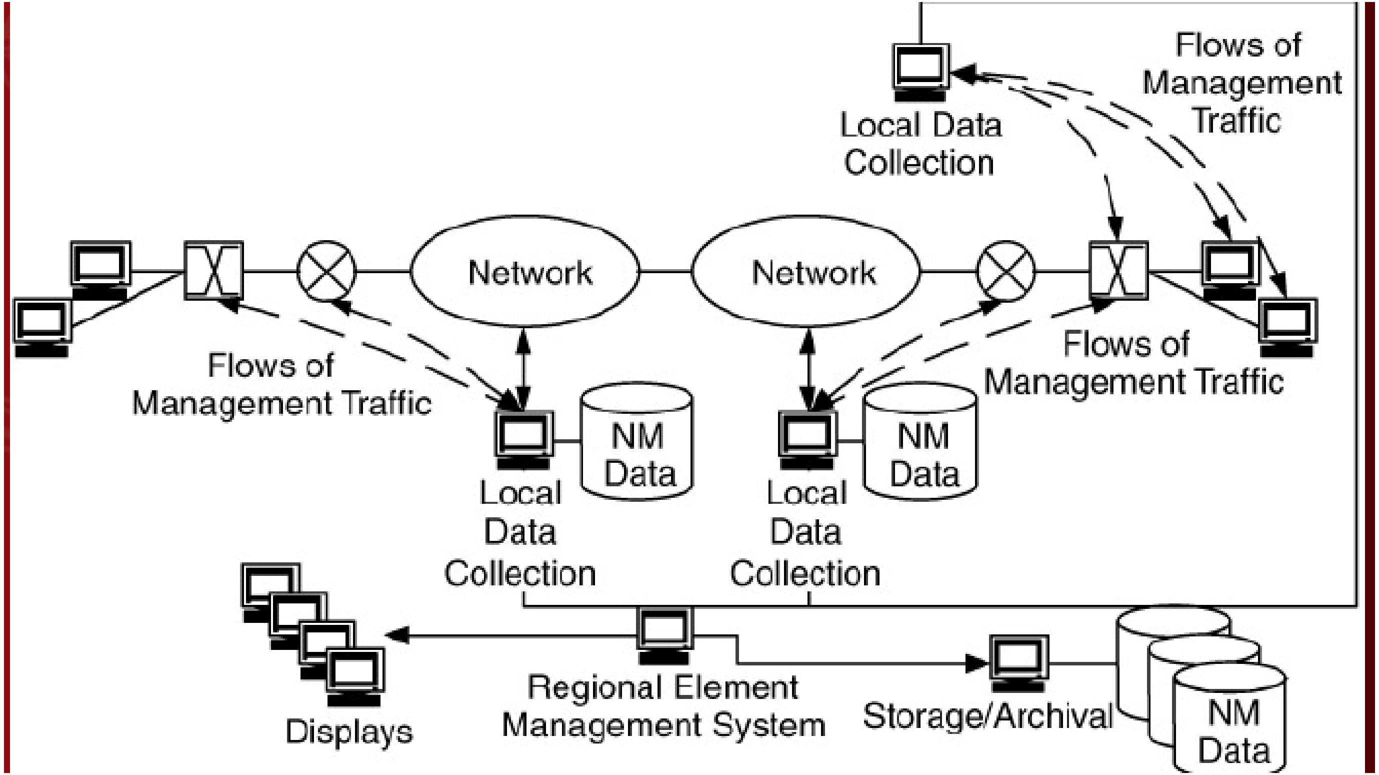
- Trade offs
  - Increased costs

Figure 7.11: Distributed management where each local EMS has its own management domain.


Flows of Management Traffic
Local Element Management System
Network
Network
Flows of Management Traffic
Flows of Management Traffic
Local Element Management System
Local Element Management System

(McCabe, 2010, p.315)

Figure 7.13: Hierarchical management separates management into distinct functions that are distributed across multiple platforms.



(McCabe, 2010, p.317)

Scaling of Network Management Traffic

- Recommendation 1:
  - For a LAN start with one monitoring device per subnet
  - Estimate the following for each subnet
    - Number of devices to be polled
    - Average interfaces per device
    - Number of parameters to be collected
    - frequency of polling
  - Combining these will give you the average data rate for network management traffic
  - If greater than 10% → consider reducing management traffic by reducing one or more of these variable
- For most standard LAN protocols aim for 2% to 5% of LAN capacity

Scaling of Network Management Traffic

- Recommendation 2:
  - For a WAN environment start with one monitoring device per WAN- LAN interface
    - In addition to monitoring devices indicated in recommendation one
    - If a monitoring device is on a LAN subnet that is also a WAN-LAN interface it can be used to collect data for both the LAN and WAN
  - Placing a monitoring device at each WAN-LAN interface allows us to
    - Monitor network at each location
    - Measure, verify and possibly guarantee service and performance requirements across the network

Checks and Balances

- Methods to duplicate measurements in order to verify and validate network management data
- Aims to locate and identify
  - Errors in recording or presenting network management data
  - Rollovers of counters (or non movement)
  - Changes in MIB variables
  - Help normalise data across multiple vendors
- Verification of accuracy

Management of Network Management Data

- Local storage vs Archival
  - Local
    - Event analysis and short-term trends
- Selective copying of data
  - If data is being used for both event notification and trend analysis → consider copying regular instances of parameter to a separate database location for trend analysis
- Data migration
  - When do we archive data?
- Metadata
  - Additional information about the collected data
  - Data types, time stamps etc.

Management of Network Management Data

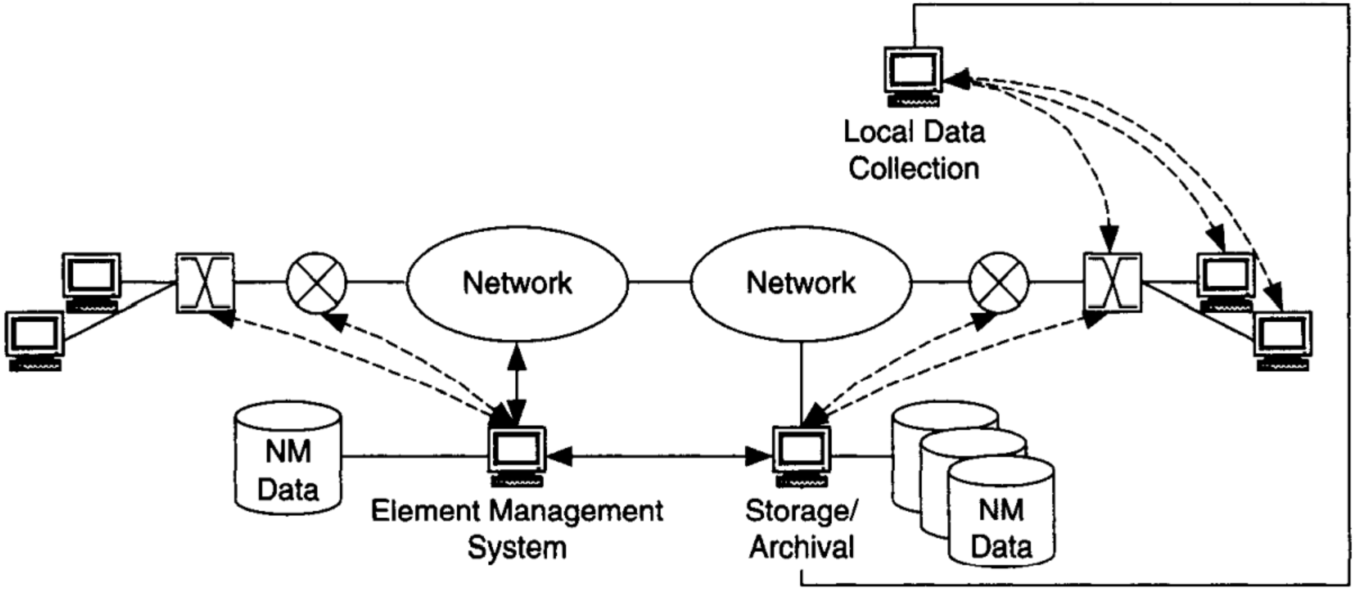


FIGURE 7.15 Local and Archival Storage for Management Data

(McCabe, 2010, p.320)

Management of Network Management Data

- Data migration
  - Data stored locally can be downloaded to storage/archival when traffic is expected to be low e.g., at night).

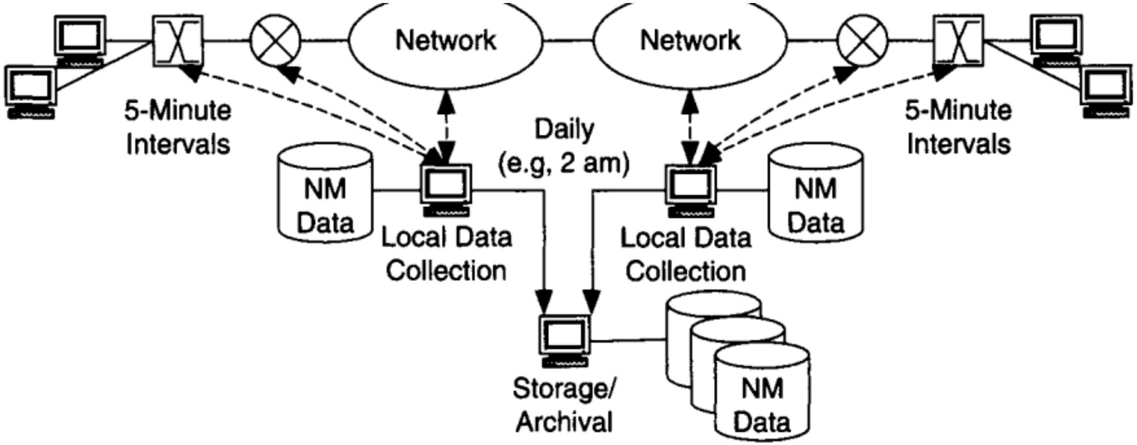


FIGURE 7.17 Data Migration

(McCabe, 2010, p.322)

Management of Network Management Data

- Recommendation 4: Metadata
  - Include additional information about the collected data, such as references to:
    - data types
    - time stamps of when the data were generated; and
    - any indications that these data reference any other data.

MIB Selection

- Which MIBs do you need?
  - Are enterprise specific MIBs required?
  - Do you need to monitor:
    - basic network health or
    - Is monitoring and management of supported entities required
      - ✓ Server, user devices
      - ✓ Network parameters that are part of SLAs, policies and network reconfiguration
- and what about higher level business processes?

Internal Relationship

- Interactions
- Dependencies
- Trade-offs

Internal Relationship – Interactions

- OSS *(Operations Support System)*
- When the network includes an interface to an OSS, the network management architecture should consider how management would be integrated with the OSS.
- The interface from network management to OSS is often termed the northbound interface because it is in the direction of service and business management.
- This northbound interface is typically CORBA *(Common Object Request Broker Architecture)* or SNMP or HTTP (Figure 7.18).

Internal Relationship – Interactions

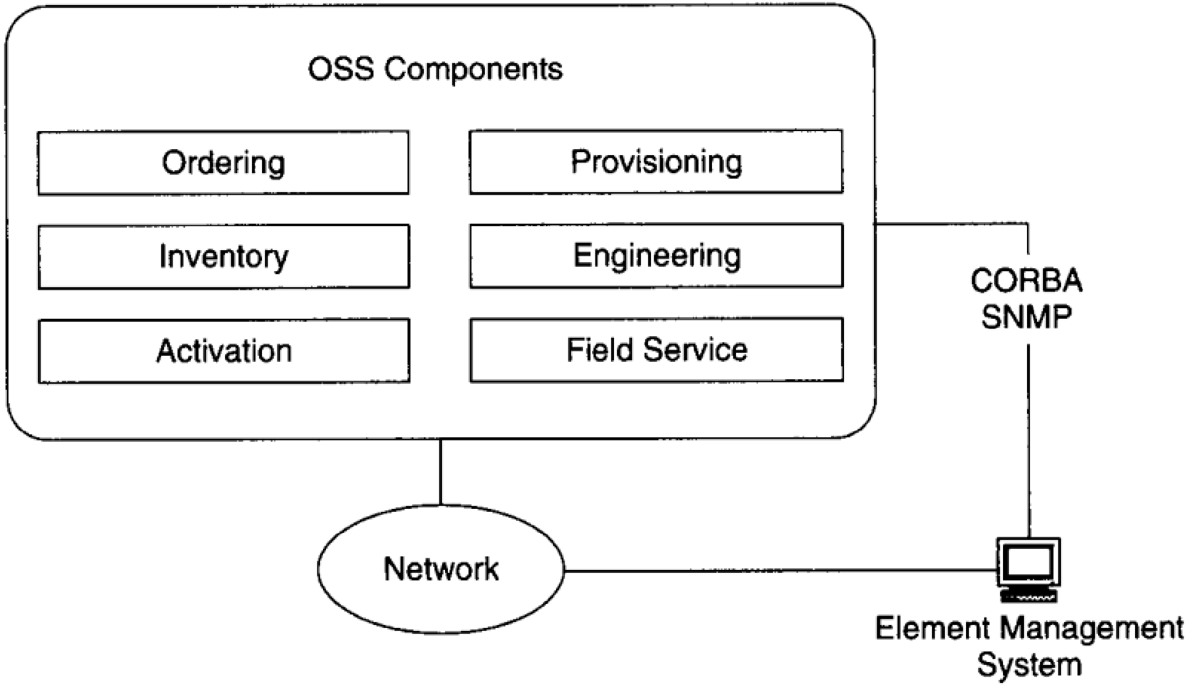


FIGURE 7.18 The Integration of Network Management with OSS

(McCabe, 2010, p.323)

Internal Relationships – Dependencies

- Dependencies on
  - Capacity and reliability of the network for managing data flows
  - Amount of data storage available for managing data
  - OSS for the northbound interface requirement
  - Maybe the underlying network for supporting the data flows management

Internal Relationships – Trade-offs

- Costs and reliability
  - in-band and out-of-band
- Simplified architecture and reduced costs vs redundancy and flexibility
  - Centralized
  - Distributed
  - Hierarchical

External Relationships

- Network Management and Addressing/Routing
  - Network management information flows are dependent on addressing and routing
  - Also determines network boundaries
    - Management domain = autonomous domain

External Relationships

- Network Management and Performance
  - Performance is measured by NM data.
  - Trade-off between performance and the burden NM data flows place on the system
  - Flow estimates need to include NM data overheads
  - If NM data is critically important this needs to be given priority and necessary, support provided

External Relationships

- Network Management and Security
  - Security perimeters/policies may impede NM data flows
  - Out-of-band management enables security vulnerabilities posed by network management to be managed better

References and Reading

- **Chapter 7 -** McCabe, J. D. (2010). *Network Analysis, Architecture, and Design*. San Diego, CA, USA: Elsevier Science.

Thank you
Q&A ?

UNIVERSITY
OF WOLLONGONG
AUSTRALIA