CpE654 / NIS654
Design and Analysis of Network Systems

Network Management Architecture

Readings!

McCabe's book: - Chapter 7

Please **read the book** along with this presentation. **Chapter 4 onwards are important chapters that cover the core of the topic for this class**

Network Management

Network management consists of the set of functions to control, plan, allocate, deploy, coordinate, and monitor network resources.

Requirements

Satisfaction of major requirements (collected during network analysis phase) can be achieved by having a network management plan.

Example of these requirements:

- Reconfiguring the network to meet different requirements.
- Implementing high-level asset management for the network.
- Monitoring the network.
- Testing service-provider compliance with service-level agreements (SLAs) and policies.

  see www.verizonenterprise.com/terms/us/products/ for Verizon examples
- Proactively monitoring (discovering performance problems before users, applications, and devices be affected by them).

Other Requirements

Some other requirements define some constrains in the network management.

Example:

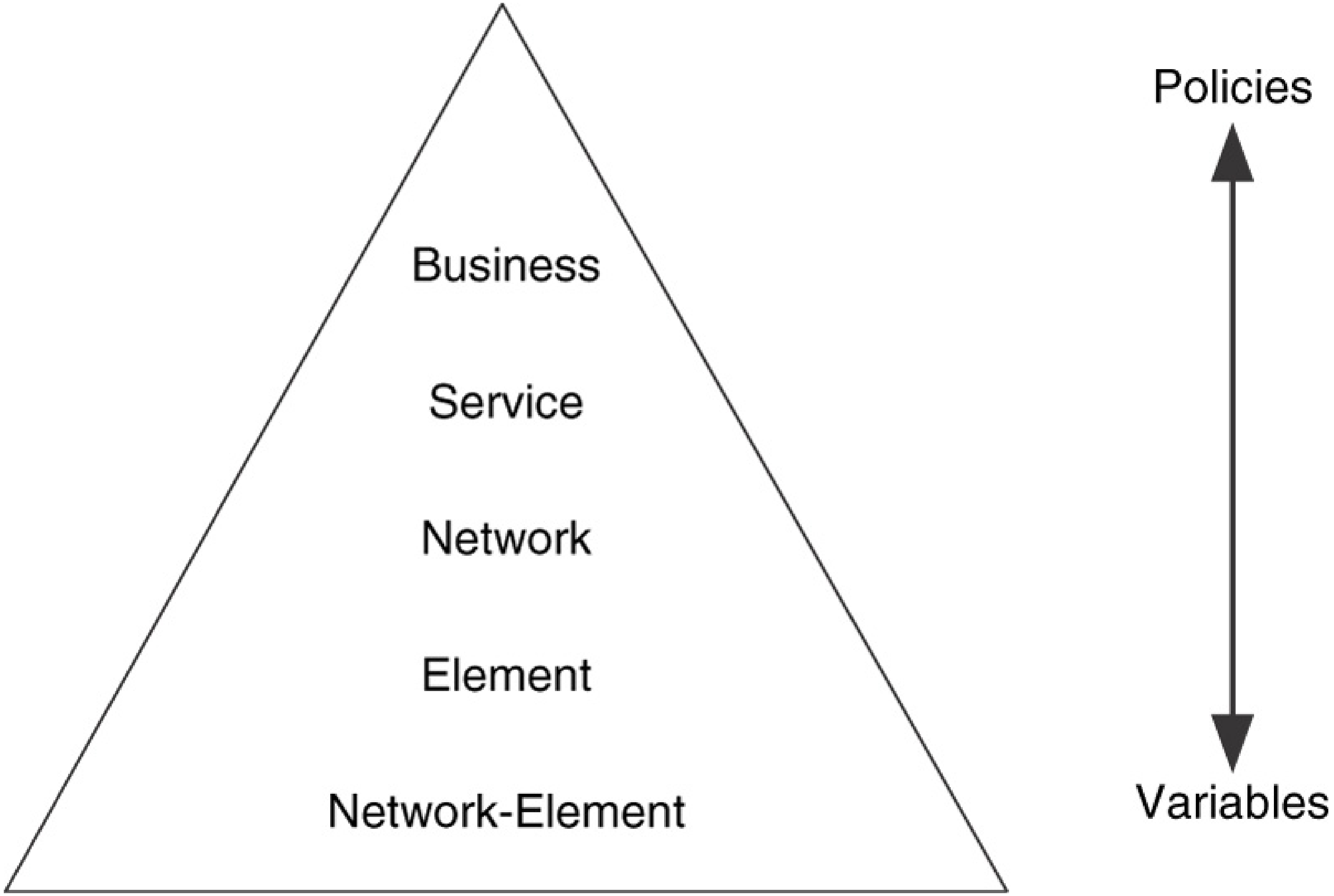
- Deciding which network management protocol to apply.
- Fulfilling requirements for out-of-band access.

Network Management Layers

Network management can be viewed as a structure consisting of multiple layers (ISO Defined):

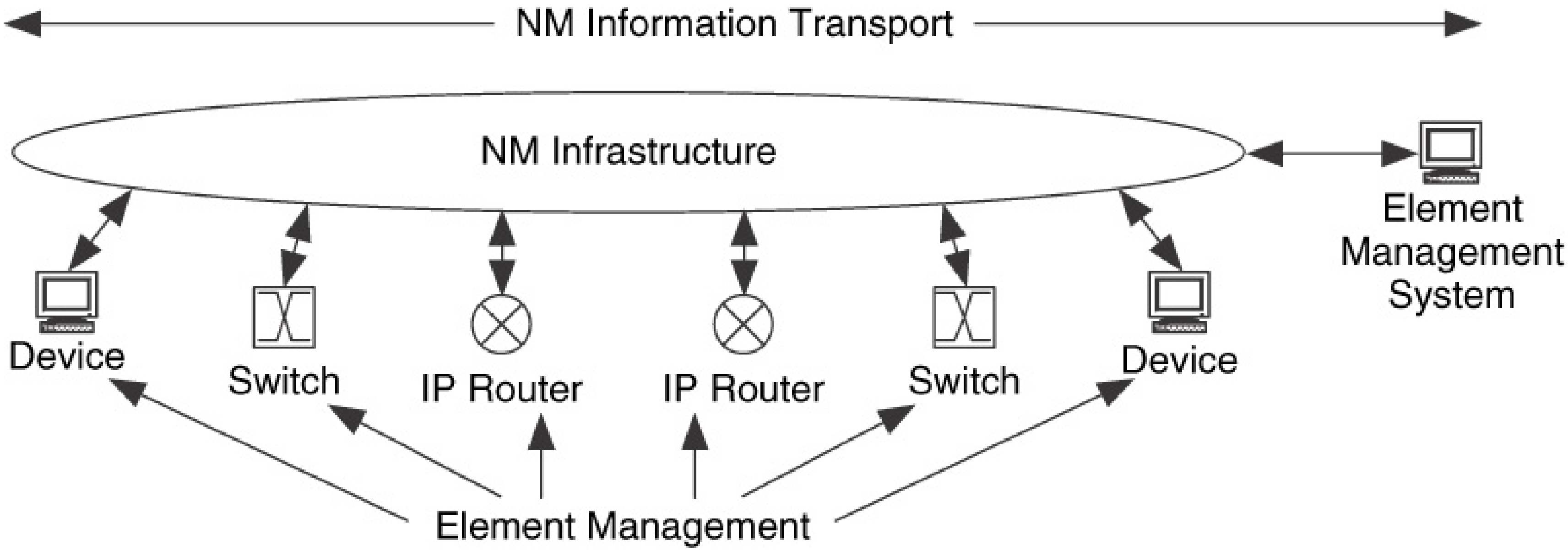
- **Business management:** This is the management of the business aspects of a network (e.g. the management of budget/resources, planning, and agreements).
- **Service management:** This is the management of delivery of services to users (e.g. the management of access bandwidth or connectivity availability).
- **Network Management:** This is the management of all network devices across the entire network.
- **Element management:** This is the management of a collation of network devices (e.g. a collection of routers or switches).
- **Network-element management:** This is the management of individual network devices (e.g. a single router, switch, or hub).

Network Management Hierarchy



Network Management Basic Functions

- The transport of management information across the system
- The management of network devices and networks includes network planning, initial resource allocation (e.g. frequency or bandwidth allocation), and Fault, Configuration, Accounting, Performance, and Security (FCAPS).



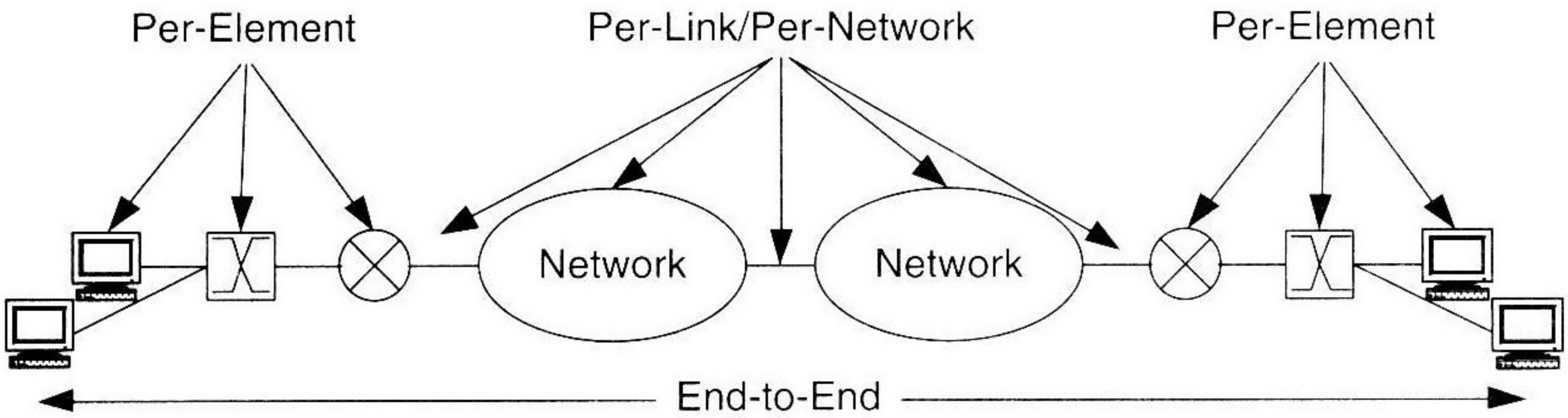
Network Management Tasks

- Monitoring for event notification
- Monitoring for trend analysis and planning (for planning for future network growth)
- Configuring network parameters
- Troubleshooting the network

Network Characteristics Measurements

Network devices such as routers, switches, hubs, and network interface cards (NICs) have characteristic that can be measured. They can be grouped into:

- End-to-end characteristics (e.g. availability, capacity, jitter, and network utilizations).
- Per-link/per-network (e.g. propagation delay and link utilization).
- Per-element characteristics (e.g. IP forwarding rates and buffer utilization for the router).



Network Managements (NM) Protocols

There are two major NM protocols

- SNMP (Simple Network Management Protocol).
- CMIP (Common Management Information Protocol), defined by the ITU-T X.700series recommendations. A special version of CMIP is CMOT (CMIP Over TCP/IP).

  CMIP is based on TMN (Telecommunication Management Network), a system used by telcos for telephony networks. It is defined in ITU-T Recommendation series M.3000.

These network managements protocols provide the mechanism for retrieving, changing, and transport of network management data across the network

SNMP Commands - Example

SNMP is a application layer protocol simple request/response protocol. Examples of SNMP commands include:

get: to collect the value of a parameter

get-next: to collect the value of the next parameter in the list

set: to change the value of a parameter

trap: to notify about a special event.

Inform: for one NMS to send trap information to another.

- Parameters that are accessible via SNMP are grouped into MIBs (Management Information Base).
- SNMPv3 provides:
  - ✓ more secure authentication
  - ✓ the ability to retrieve blocks of parameters
  - ✓ trap generation for most parameters
- CMIP/CMOT also does parameter collection, setting, and other features like SNMP.
- SNMP is easier to configure and use and is now universally used

Network Management Mechanisms

Classified into three types:

- Monitoring Mechanisms
- Instrumentation Mechanisms
- Configuration Mechanisms

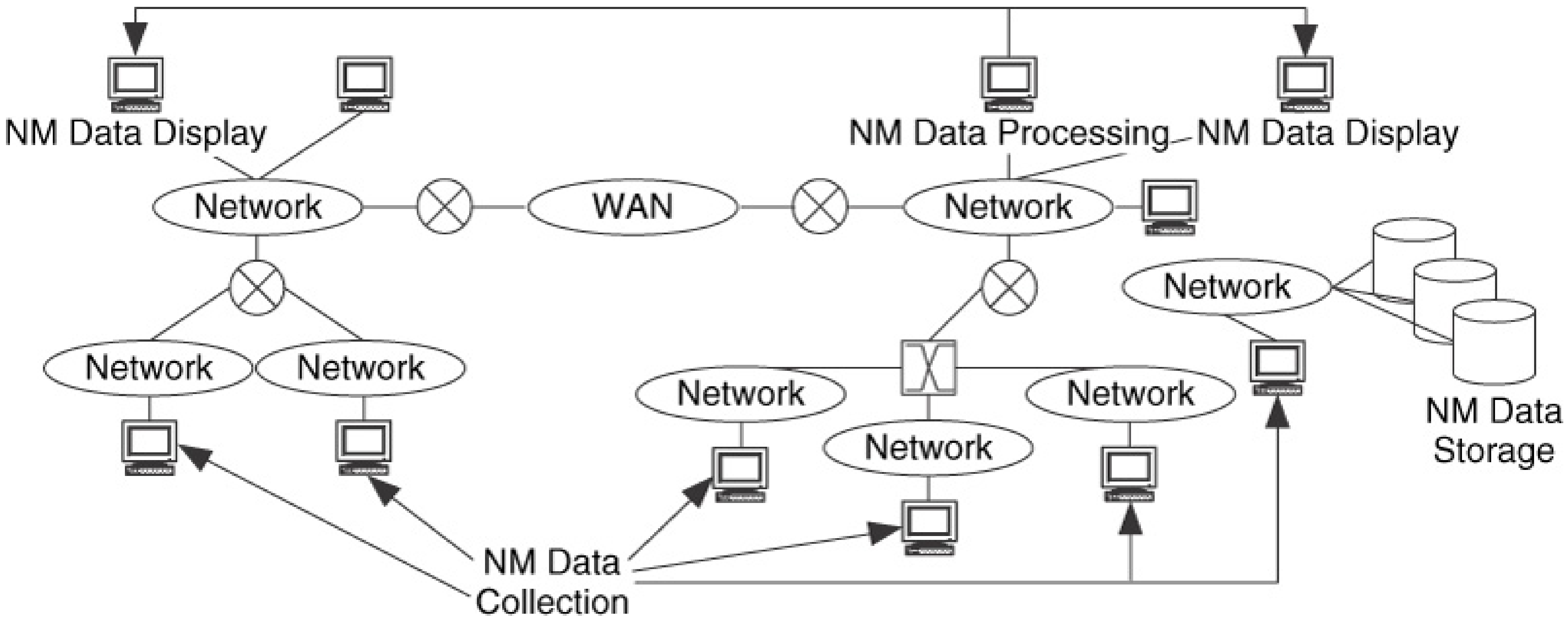
Monitoring Mechanisms

To obtain values of end-to-end, per-link, and per-element characteristics.

Monitoring process involves:

- Collecting data
- Processing some or all these data
- Displaying the (processed) data
- Archiving a subset of these data

Elements of Monitoring process

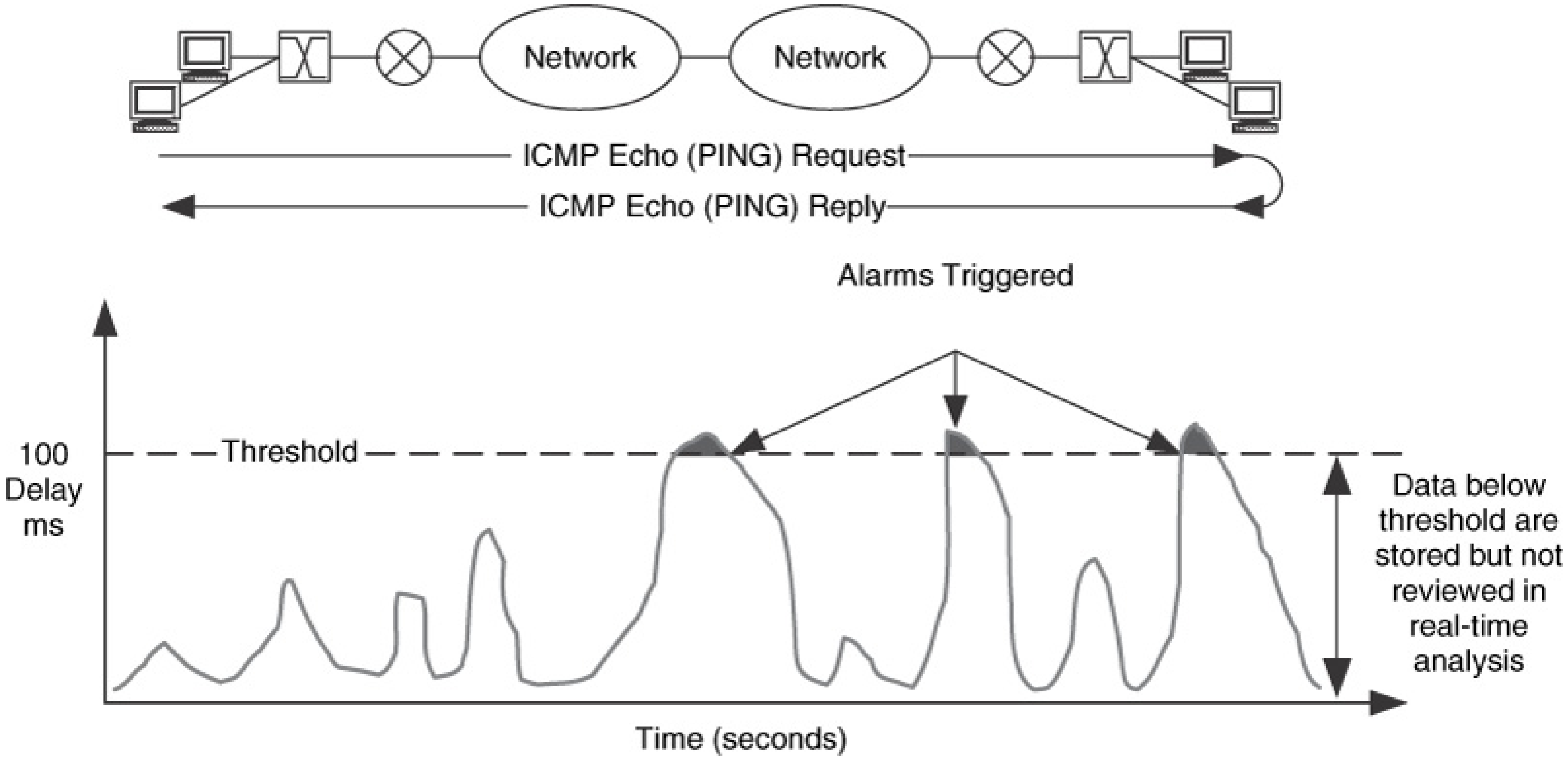


Data collection

Data processing and display

Data storage

Monitoring Parameters

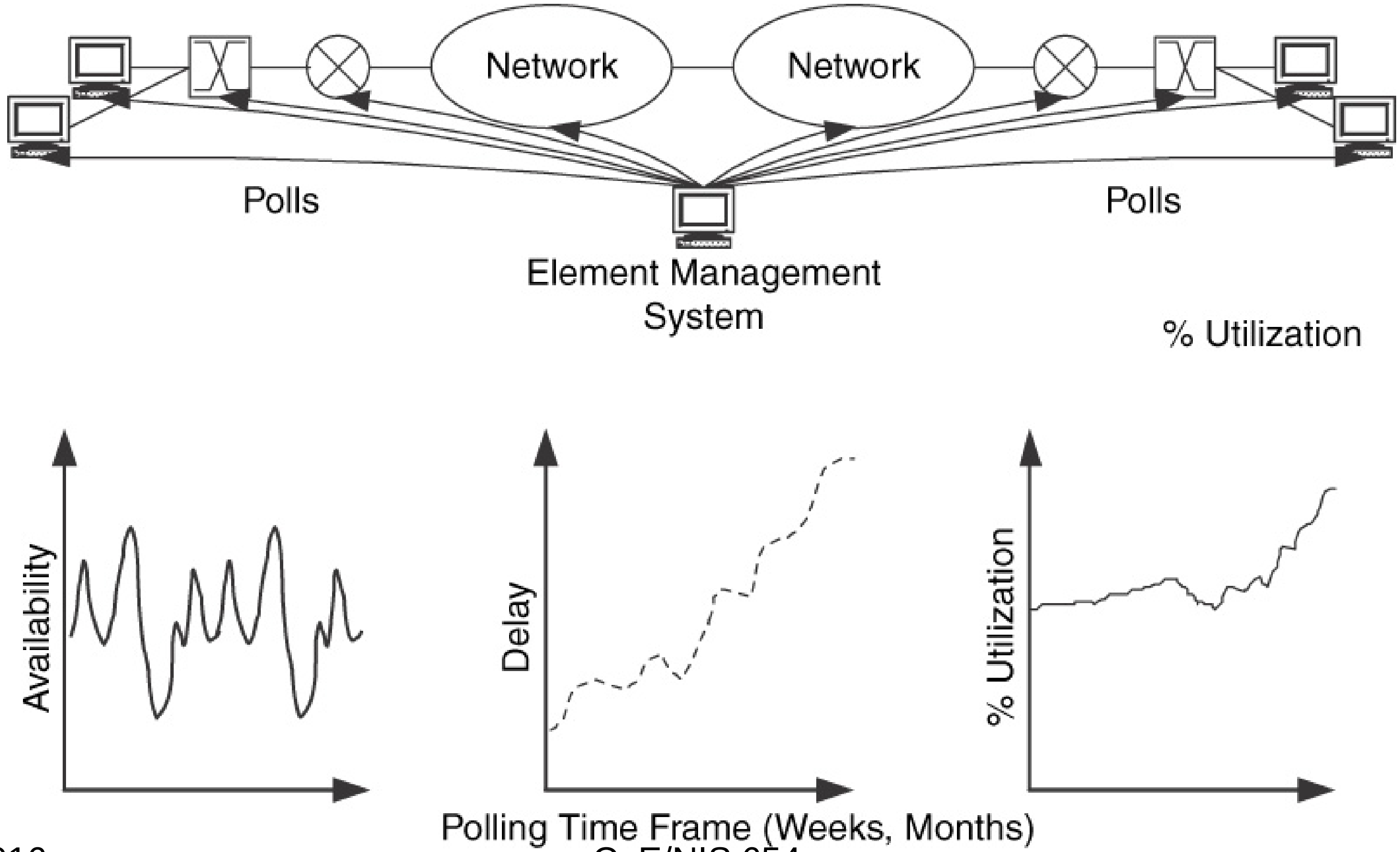


Trend Analysis

Using network management data to determine long-term network behaviors, or trends.

- Useful in planning for future network growth.
- Polling intervals are long (minutes or hours instead of seconds).

Monitoring for Trends



Two monitoring mechanisms

- Monitoring by polling (e.g. using the *get* command)
- Monitoring by event notifications (e.g. using the *trap* command).

Monitoring Overhead

Real-time analysis for a network usually requires short polling intervals. This can generate some overhead on the network.

There is a trade-off between the number of characteristics and network devices polled for real-time analysis versus the amount of resources (capacity, CPU, memory, storage) needed to support such analysis (overhead).

Example

Consider a network that has 100 network devices. Each device or element has an average of four interfaces and each interface is monitored for eight characteristics:

(100 network devices) x (4 interfaces/network devices) x (8 characteristic /interface) = 3200 characteristics

If each of the 3200 characteristics generate an average of 8 bytes of data and an estimated 60 bytes of protocol overhead, the amount of data generated per polling session is as follows:

(3200 characteristic) x (8 bytes + 60 bytes) = 217.6 KB* = 1.74Mb* of traffic.

If we plan to poll with a polling interval 5 seconds, then in each second an average of 348 Kb* (1.74 Mb/5) will be generated and transferred. The total amount of traffic for a period of 1 day is 30.2 Gb* of traffic.

The amount of data stored would be:

(3200 characteristic/polling interval) x (8 bytes) x (720 polling intervals/hour) x (24 hours/day) = 442 MB** data stored per day.

(Note: * when traffic bps is calculated the raw # of bits is given, but ** when storage bytes (B) is given we use 1K = 1024, 1M =$(1024)^2$ is used for conversion)

Instrumentation Mechanisms

Instrumentation is the set of tools and utilities needed to monitor and probe the network for management data. Instrumentation mechanisms include access to network management data via SNMP, monitoring tools, and direct access.

- Access to network for management data via SNMP.
- Monitoring tools include utilities such as *ping*, *traceroute*, etc.
- Direct access mechanisms include telnet, FTP, and connections via a console port.

You have to ensure that the instrumentation is accurate.

Configuration Mechanisms

Configuration is setting parameters in a network device for operations and control of that element.

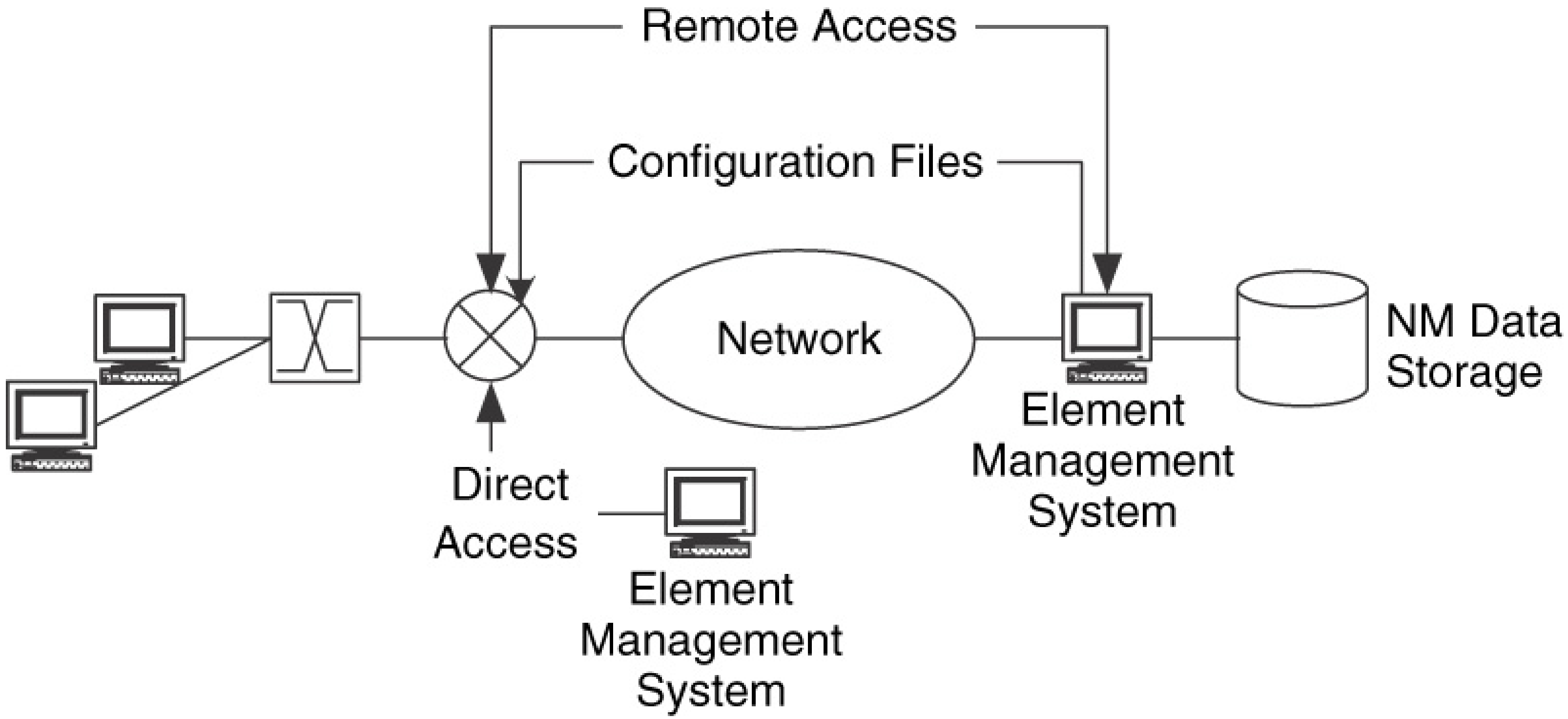
Different types of configurations:

- SNMP SET commands
- Telnet and Command Line Lnterface (CLI) access
- Access via HTTP
- Access via common object request broker architecture (CORBA)

To enable SW written in multiple languages and running on multiple computers to work together

- Use of FTP to download configuration files

Configuration Mechanisms



Architectural Considerations

Network management touches all other aspects of management - FCAPS:

- Fault management
- Configuration management
- Account management
- Performance management
- Security management

Network Management Architecture Considerations

- In-band and out-of band management
- Centralized, distributed, and hierarchical management
- Scaling of network management traffic
- Checks and balances
- Managing NM data
- Parameters (MIB) selection
- Integration with Operations Support Systems (OSS)

In-Band and Out-of-Band Management

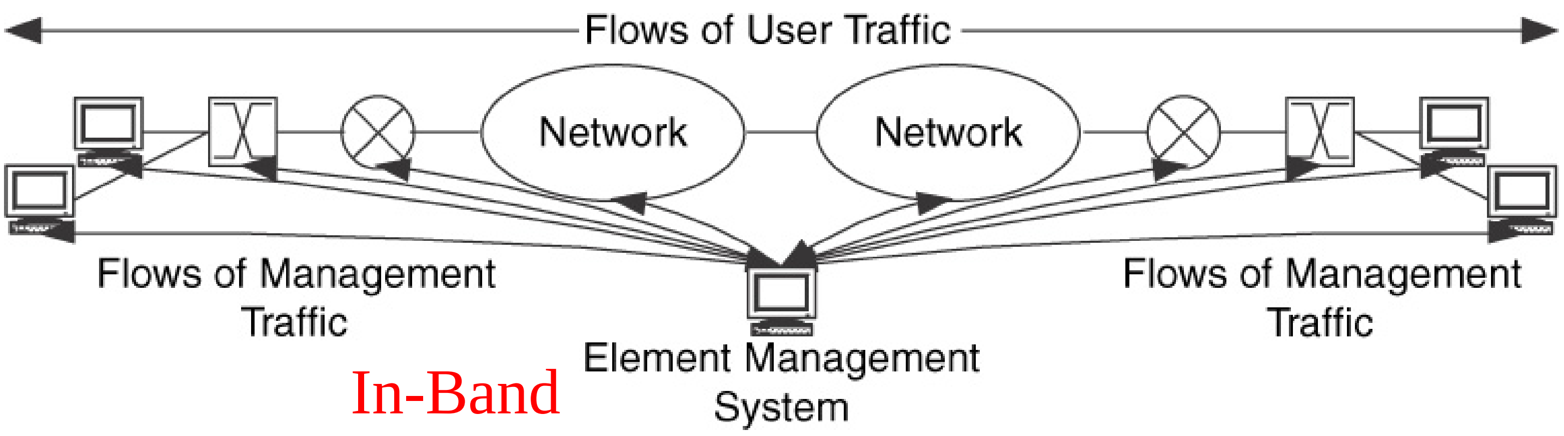
Trade-offs between in-band and out-of-band management:

- Out-of-band is costly and complex. This is an extra network to manage with issues impacting traffic and synchronization between the management and user networks.

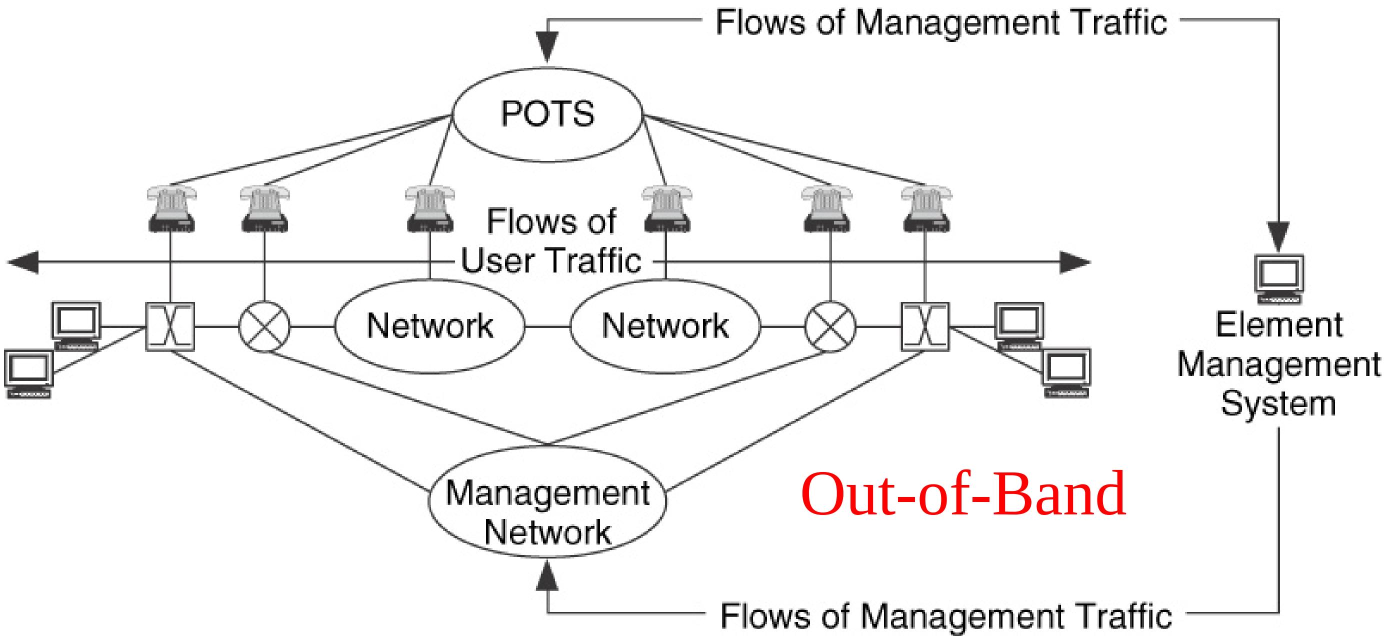
  However, for out-of-band management, management data flows will not be affected by user data flows or problems in the user traffic bearing network.

- Having a separate network for network management allows to integrate additional security features into this management network.
- For in-band management, management data flows can be affected by the same problems that impact user traffic flows.

In-Band Versus Out-of-Band NM Traffic


Flows of User Traffic
Network
Network
Flows of Management Traffic
Flows of Management Traffic
Element Management System

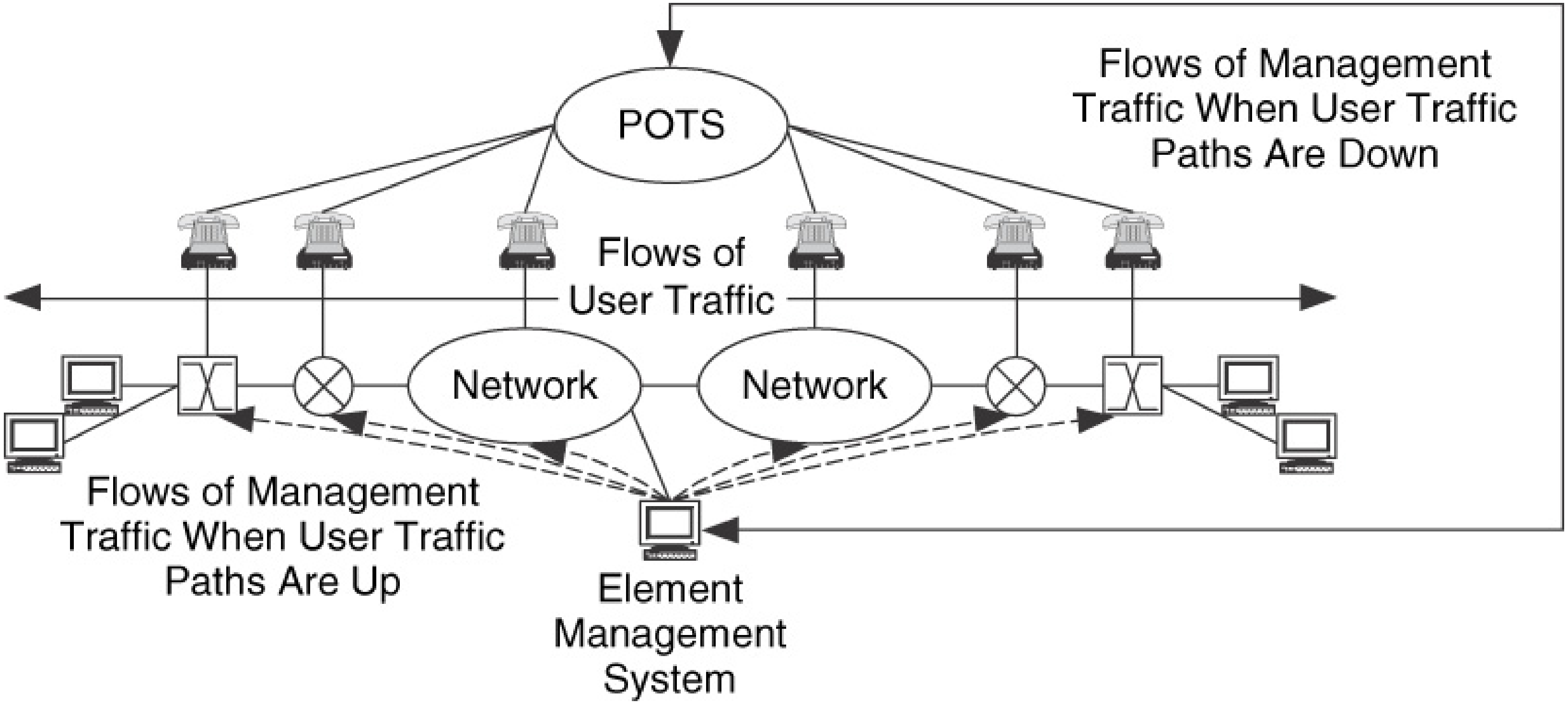
In-Band


Flows of Management Traffic
POTS
Flows of User Traffic
Network
Network
Element Management System
Management Network
Flows of Management Traffic

Out-of-Band

Combination of In-Band Out-of-Band NM Traffic

For some networks a combination of in-band and out-of-band management is optimal. In such applications, out-of-band network is used when user data network is down.


POTS
Flows of Management Traffic When User Traffic Paths Are Down
Flows of User Traffic
Network
Network
Flows of Management Traffic When User Traffic Paths Are Up
Element Management System

Centralized, Distributed and Hierarchical Management

Centralized Management occurs when all management data radiate from a single central management system. The management data flows behave like the client-server flows.

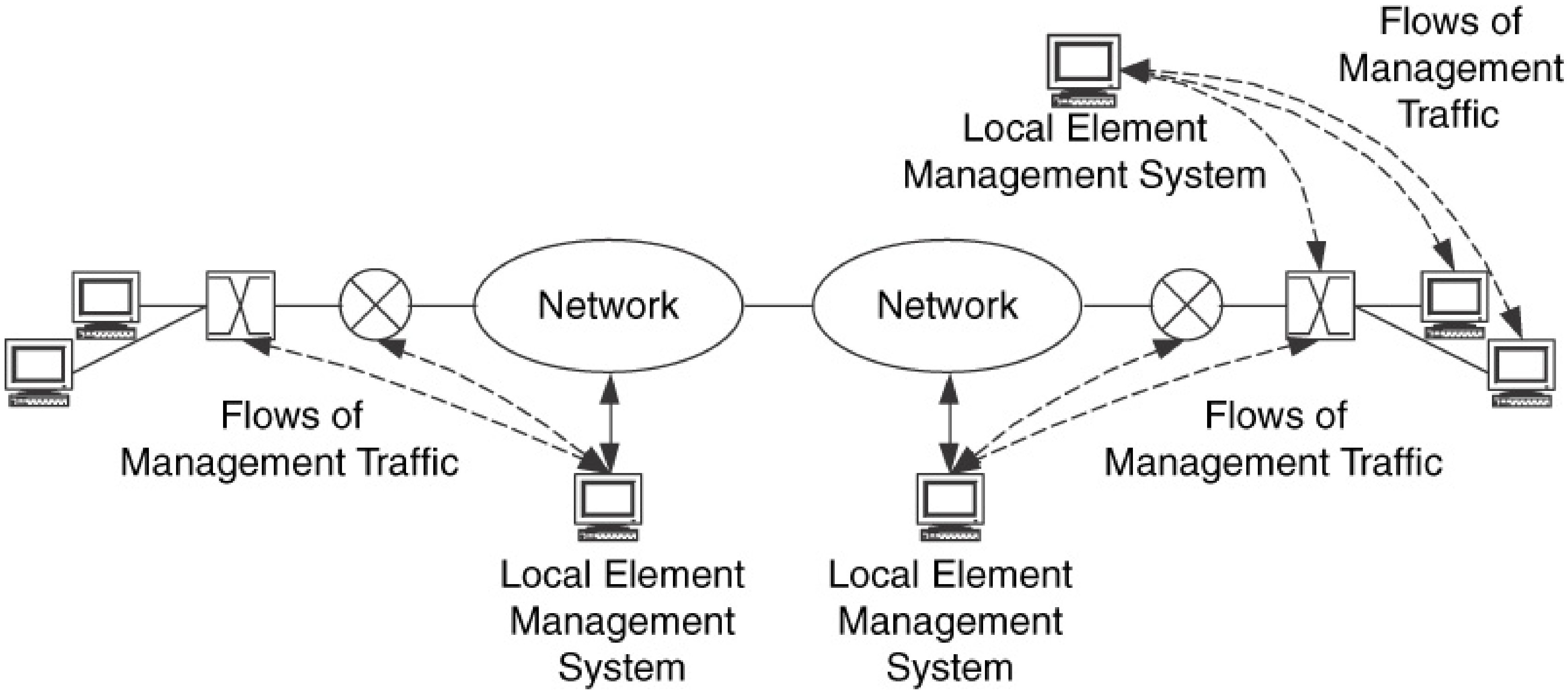
Distributed Management occurs when there are multiple separate components to the management system and theses components are placed across the network.

In **Hierarchical Management**, localized monitoring device collect management data and either pass these data directly to display and storage devices or process them.

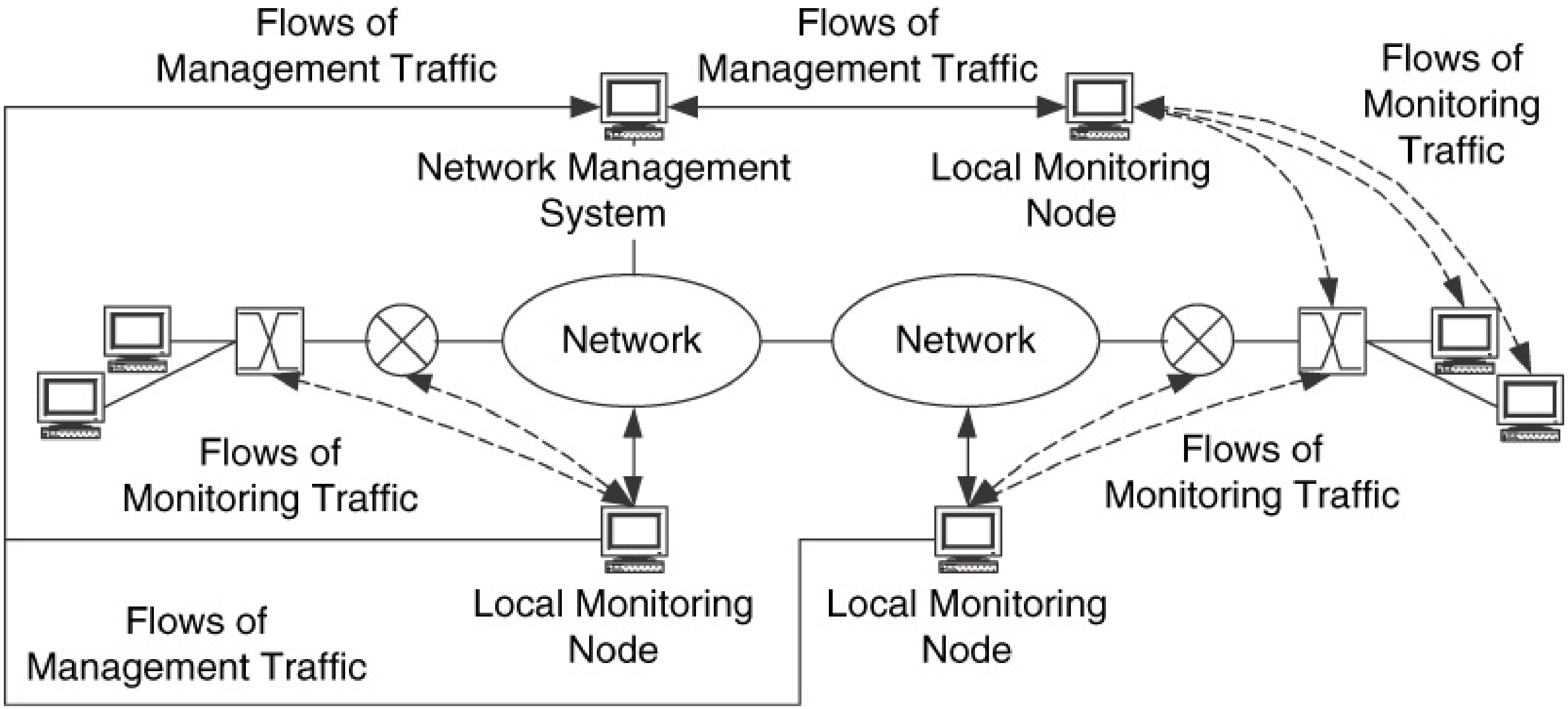
Trade-Offs
in
Centralized, Distributed and Hierarchical Management

- Centralized management is a single point of failure while distributed management provides redundant monitoring.
- Distributed management reduces the amount of management data that transit the network.
- Distributed and hierarchical managements are costly and complex.

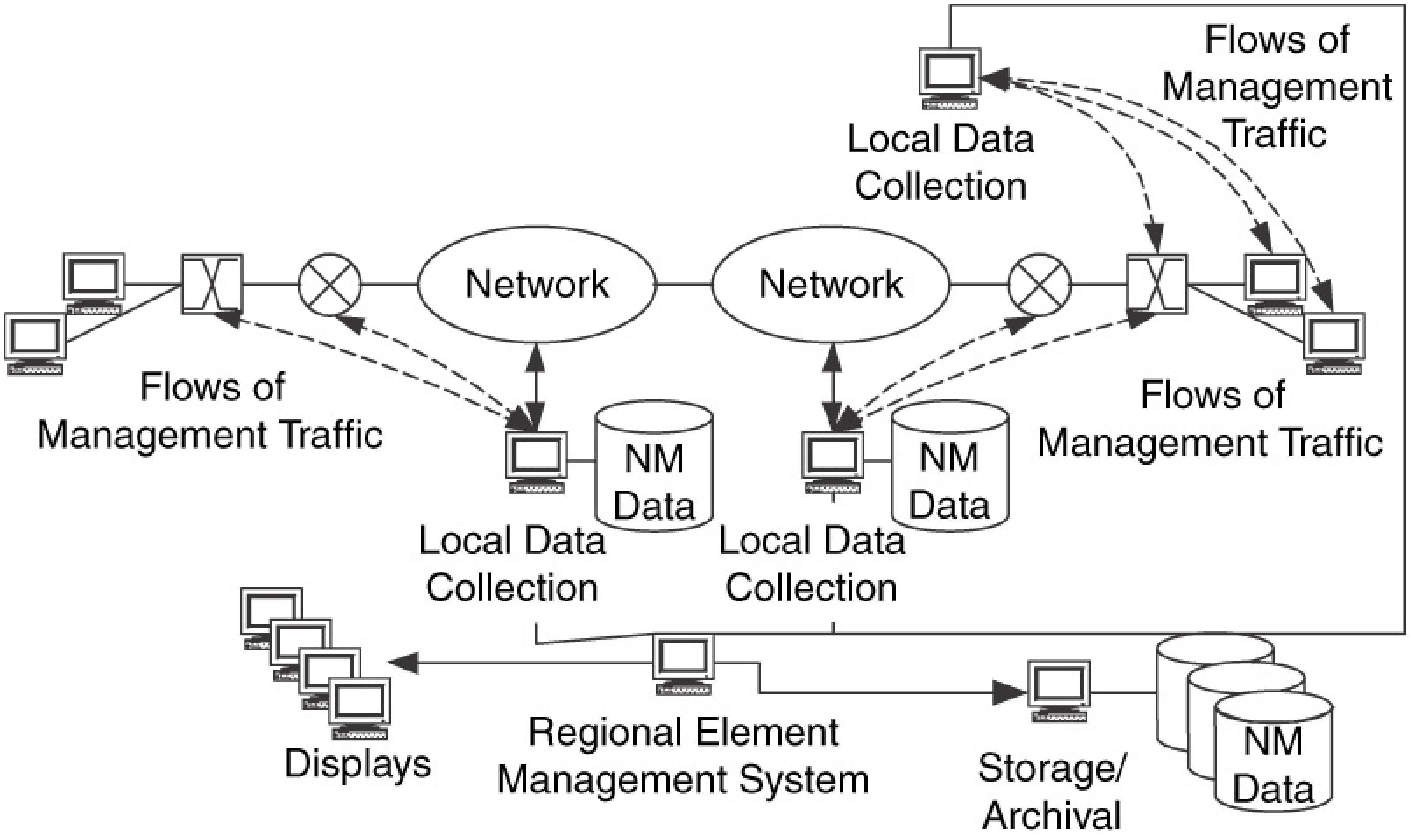
Fully Distributed Network Management Systems


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

Hierarchical Where Monitoring is Distributed



Fully Hierarchical Network Management System



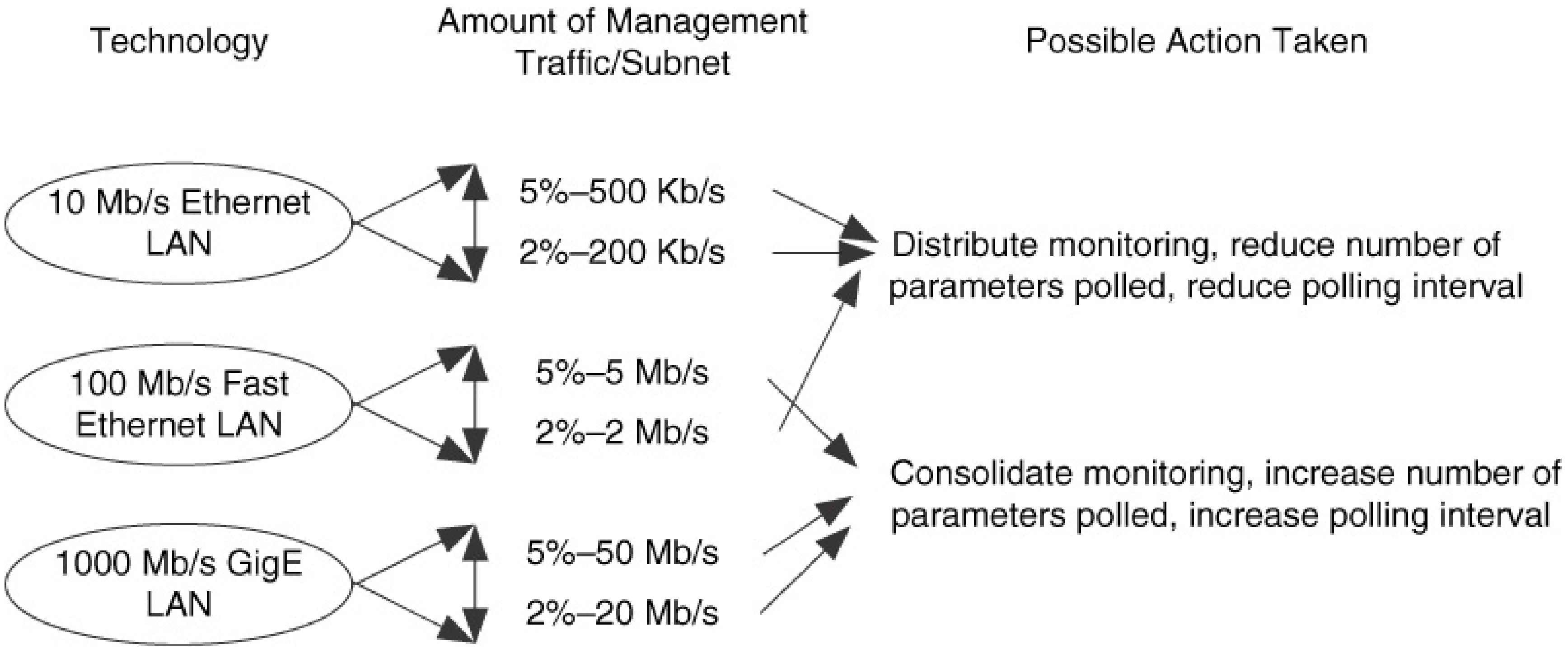
Scaling of Network Management Traffic

The estimated size of management traffic is based on:

- Number of network devices
- An average number of interfaces per device
- Number of parameters to be collected
- Frequency of polling (polling interval)

The management traffic rate should be targeted at 2% to 5% of the LAN capacity

Scaling of Network Management Traffic


Technology
Amount of Management Traffic/Subnet
Possible Action Taken
10 Mb/s Ethernet LAN
5%–500 Kb/s
2%–200 Kb/s
Distribute monitoring, reduce number of parameters polled, reduce polling interval
100 Mb/s Fast Ethernet LAN
5%–5 Mb/s
2%–2 Mb/s
Consolidate monitoring, increase number of parameters polled, increase polling interval
1000 Mb/s GigE LAN
5%–50 Mb/s
2%–20 Mb/s

Checks and Balances

Checks and Balances are methods to duplicate measurements to verify and validate NM data. The objectives are to locate and identify:

- Errors in recording and presentation of data
- Rollover of counters (e.g., returning zero value without proper notification)
- Changes in MIB variables from one software version to another

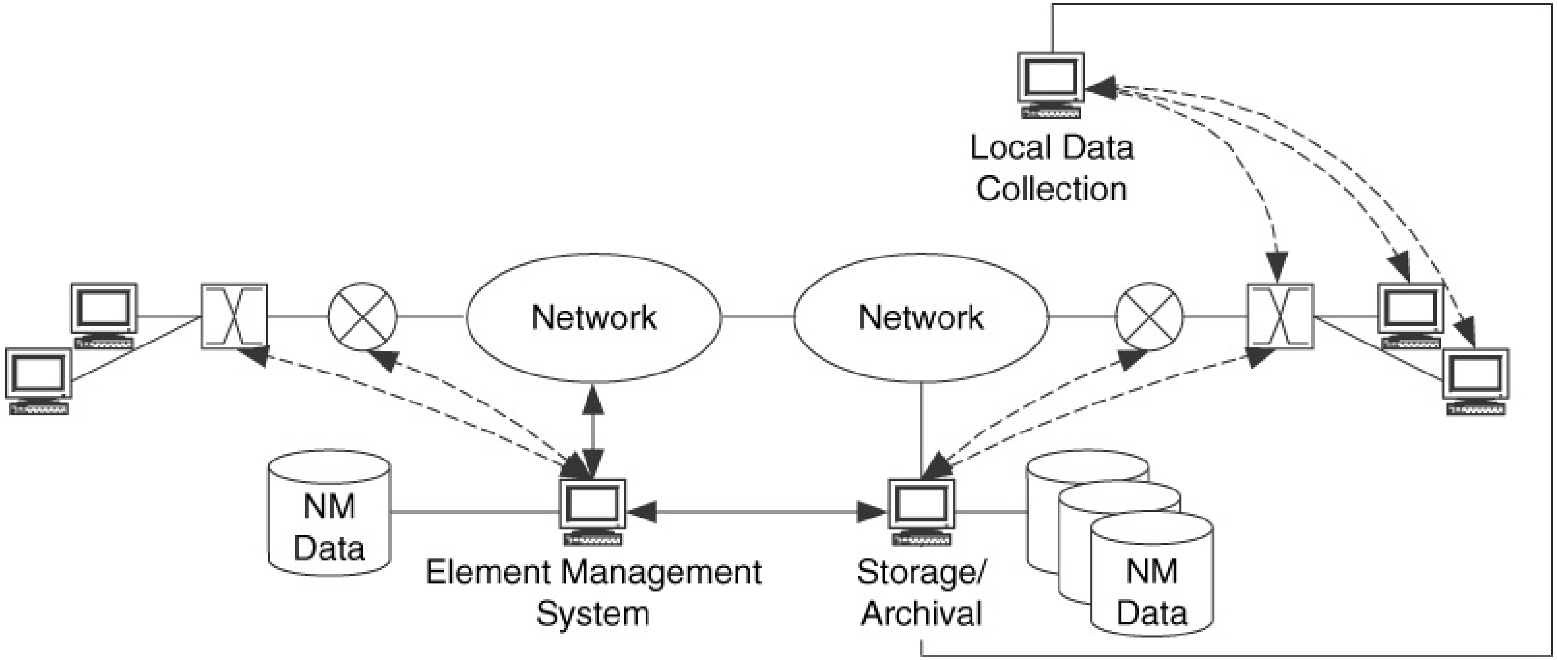
Collected data should always be verified for accuracy

Managing NM Data

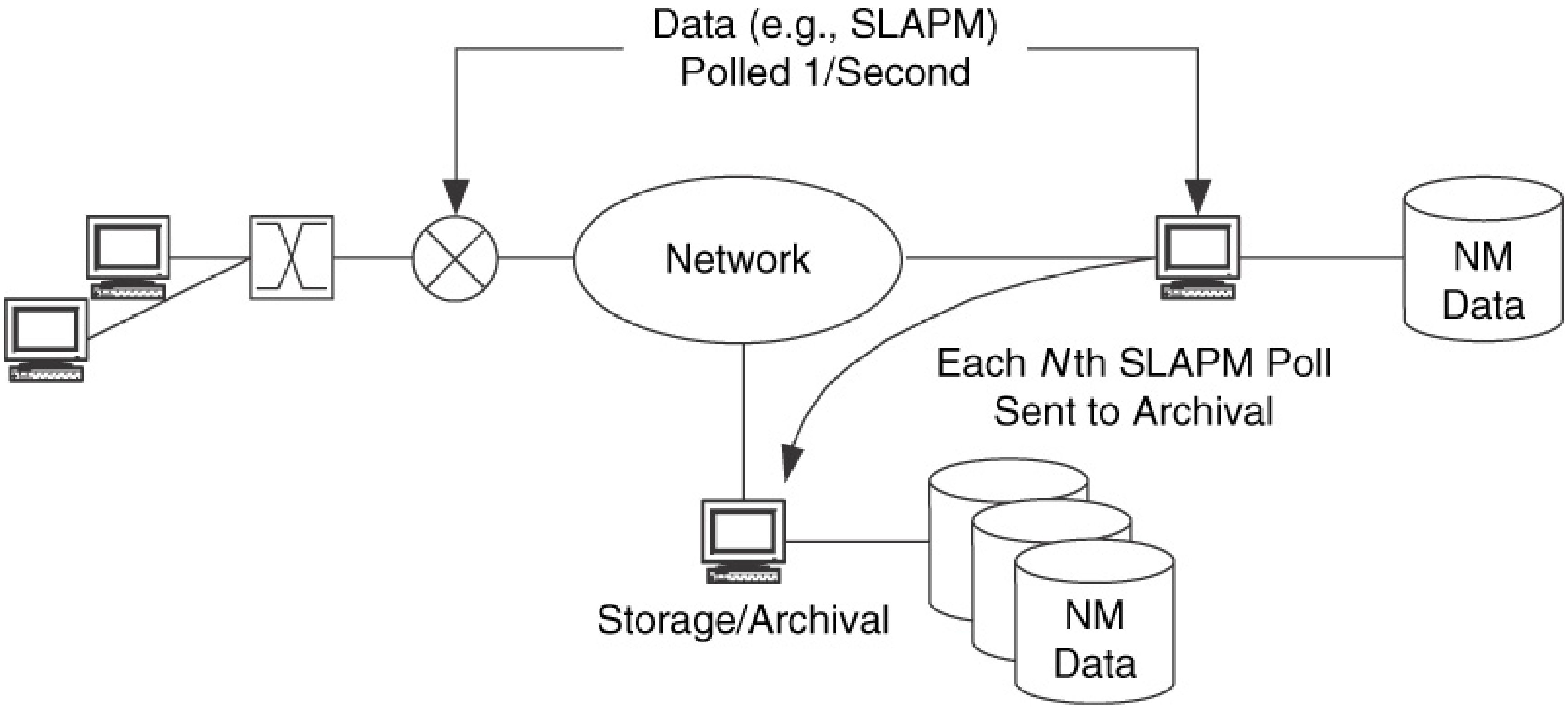
NM data may be generated by query/response (stateless) mode or by SNMP traps in response to set of threshold trigger conditions (stateful). Following items should be carefully considered:

- Local storage vs. archival based on data utility
- Selective copying of data based on storage capacities, need for trend analysis, data protection
- Data migration
- Metadata (data about data content or additional information about collected data), e.g., references to data types, time stamps, linkages to other data, etc.

Managing NM Data
Local Storage Versus Archiving



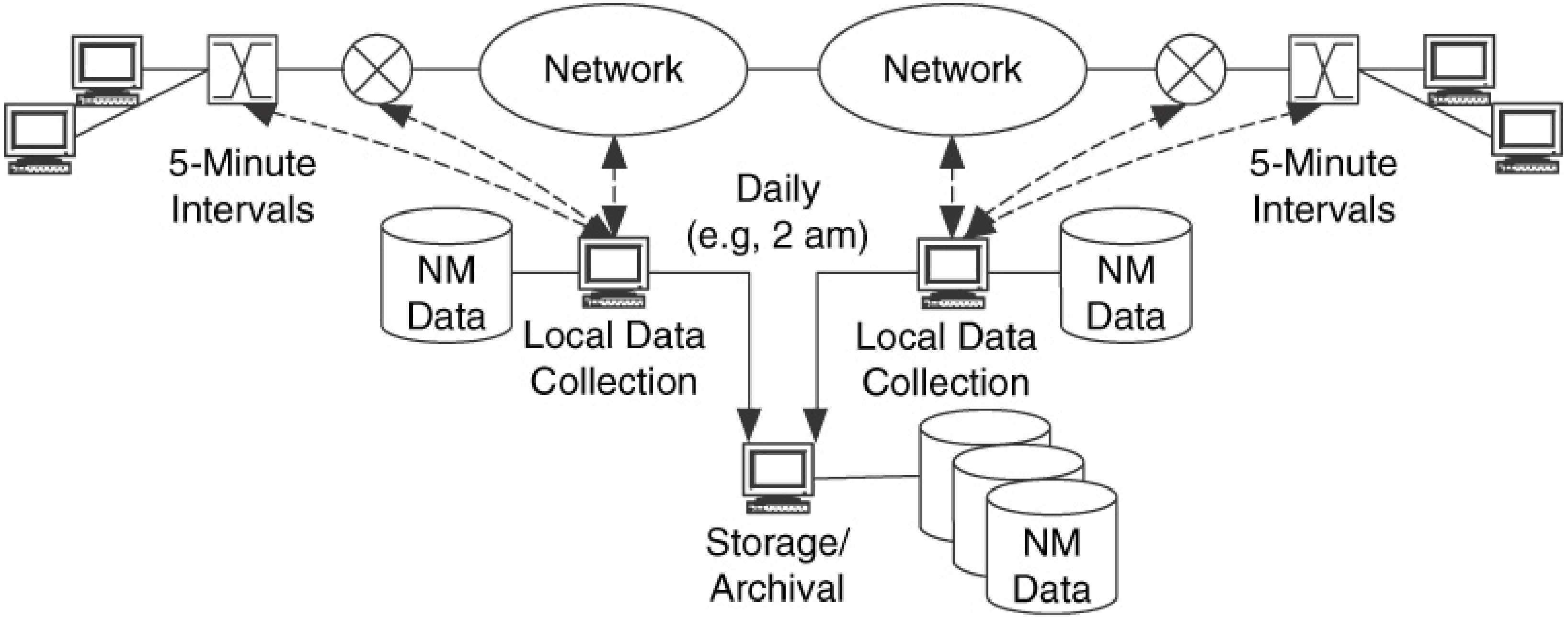
Managing NM Data
Selective Copying and Archiving for Long Term Storage



SLA Polled per second for monitoring and Nth polled saved for long term archival and analysis

SLAPM: SLA Performance Metrics

Managing NM Data
Data Migration



Polls of NM data every five minutes for local storage and then they are downloaded for archival one or twice a day

MIB Selection

MIB selection is about determining which MIBs to use and apply and which variables in each MIB are appropriate.

One may use a full MIB, a conformance subset of the MIB, user-defined subset of MIBs, or enterprise-specific MIBs

MIB variables can be classified into a common set pertaining to network health and a set to monitor and manage network devices and network parameters like SLA, policies, etc.

Integration of Network Management with OSS

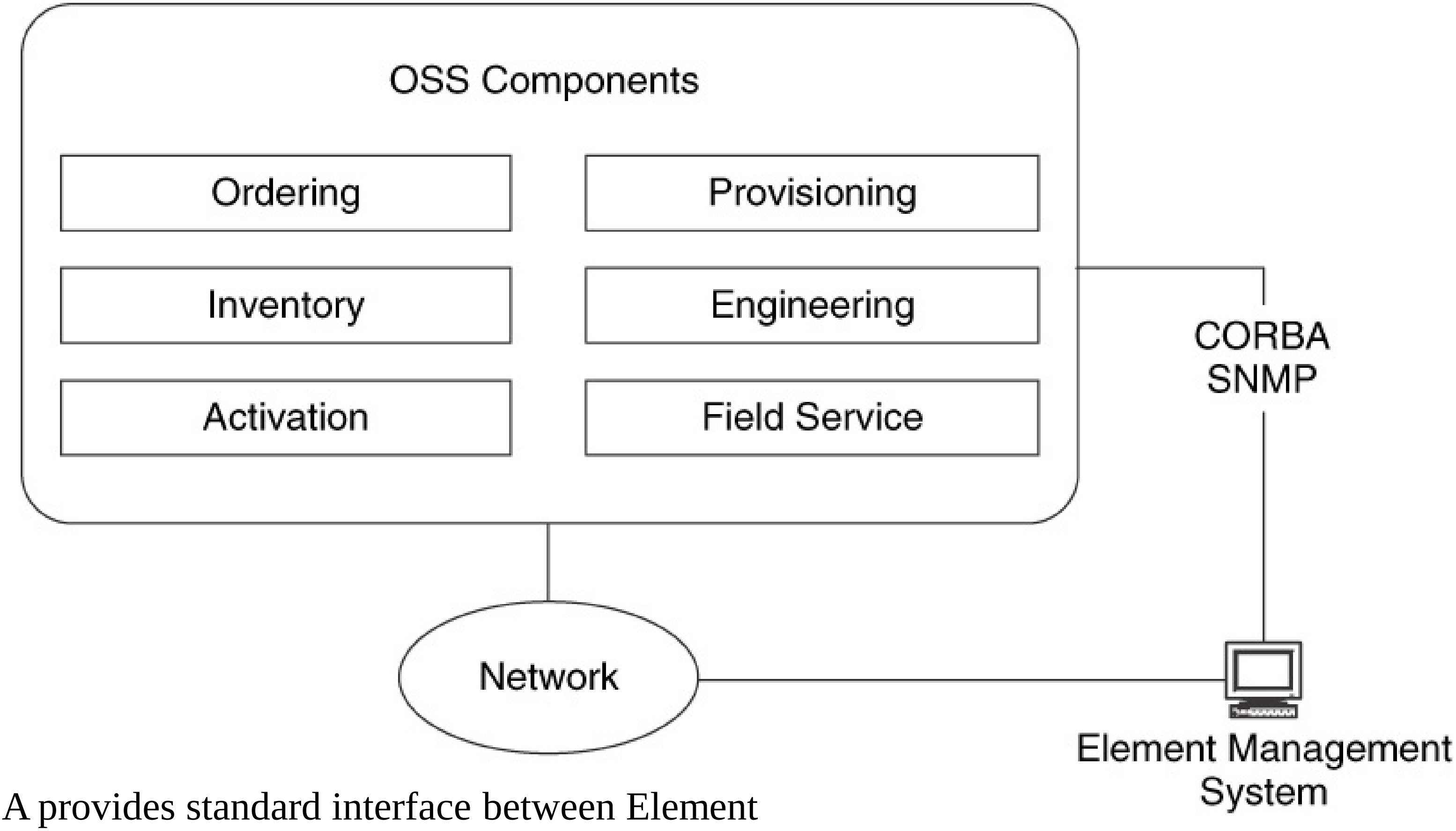
It is extremely important to consider how NM is to be integrated with OSS when the network includes an interface to the OSSs.

The interface from NM to OSS is often called the northbound interface. OSSs generally support service and business management.

The northbound interface protocol is typically SNMP.

CORBA is another protocol that is now less and less used. (defined by Object Management Group (OMG), an international, open membership, not-for-profit computer industry standards consortium developing integration standards for a wide range of technologies, platform and languages for communication)

Integration of Network Management with OSS



CORBA provides standard interface between Element Management System and OSS

Integration with OSS

TMForum (TeleManagement Forum) is a consortium to define OSS interface specifications. TMForum defining OSS interfaces through Frameworx

Frameworx: formerly known as New Generation Operations Systems and Software (NGOSS) is a set of technical specifications to help communication providers manage their business.

The TM Forum Frameworx consists of four frameworks:

–Application Framework (sometimes referred to as the Telecom Application Map (TAM))

–Business Process Framework (sometimes referred to as the enhanced Telecom Operations Map (eTOM))

–Information Framework (sometimes referred to as the Shared Information/Data (SID) model)

–Integration Frameworks (which is developed in the TM Forum Integration Program (TIP))

Frameworx is based around 5 key principles:

–Separation of Business Process from Component Implementation

–Loosely Coupled Distributed System

–Shared Information Model

–Common Communications Infrastructure

–Contract defined interfaces

Technology Trends

Home is the Network!

- Home LAN Network – IPTV, Internet, Mobile devices, WiMAX terminals, IP enabled appliances, Gaming
- Mobile devices is the growth Opportunity Areas
- Technology that make it happen
    - FiOS/G-PON
    - Femto Cell
    - Cable Networks, VoIP
    - IPTV
    - Cellular Networks
    - Wifi Networks

Home Network Management

Service Providers Manage Home Networks

- Automated Provisioning
- Network Monitoring of all devices at Home
- Remote Troubleshooting/Diagnostics
- Software Upgrade
- Braodband Forum (formerly DSL Forum) developed Standards that evolved to manage CPEs at home TR 069 (CPE WAN Management Protocol (CWMN) defines application layer protocol for remote management of end-user devices.

Home Network Management

Advantages

- Integrated Triple play services from single Service Provider
- Single Billing for end customers
- Single point of contact for all problems
- Reduced Truck roll and prevention of problems due to continuous monitoring
- Access to the end users

New Applications

New Applications using Home LAN Network

- Energy Management using IP enabled appliances
- Security Management
- Wellness Monitoring and healthcare applications
- To be invented

Next Class!

Performance Architecture

McCabe Chapter 8