

U

# CSIT985

# Strategic Network Design

O

Autumn 2024



UNIVERSITY  
OF WOLLONGONG  
AUSTRALIA

W

# Lecture 11:

# Network Management Architecture



UNIVERSITY  
OF WOLLONGONG  
AUSTRALIA

Presented by: Dr. Shengbing Tang  
Lecturer, CCNU-UOW Joint Institute

# Overview

---

## ❖ 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

---

- 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 does 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

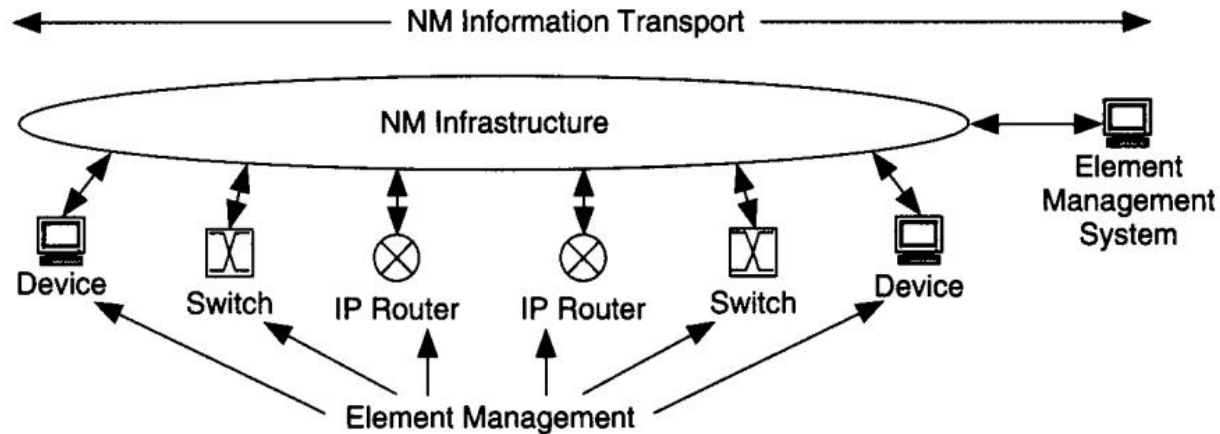
---

- 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



# 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

---

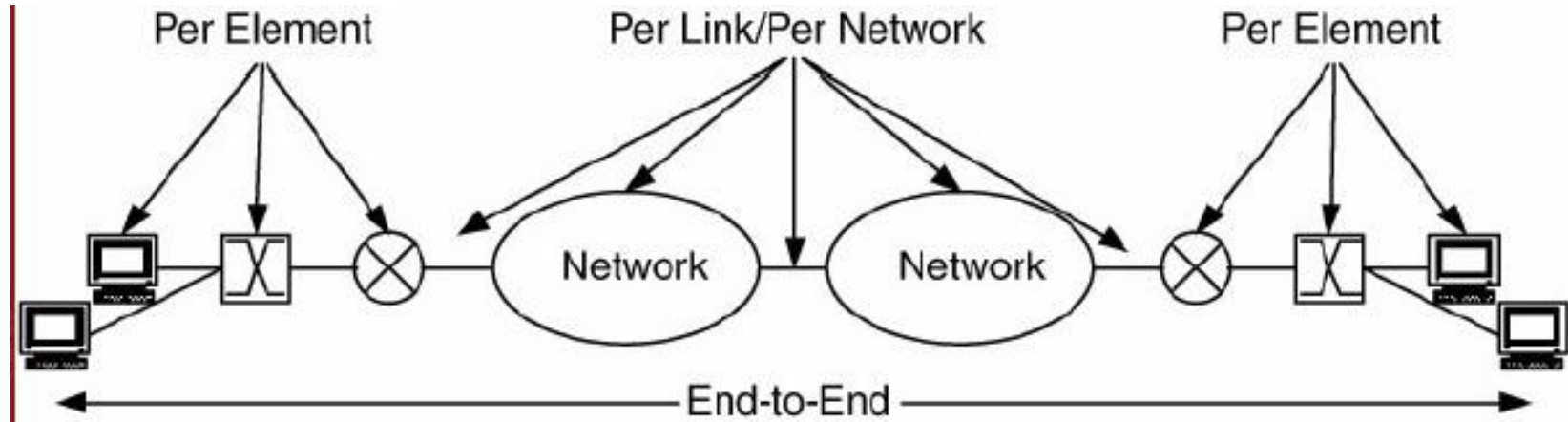
- Network device
  - An individual component of the network that participates at one or more layers of the protocol
  - End devices, routers, switches, hubs etc.

# 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.

# Network Devices and Characteristics



# 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 utilisation
  - Per element: IP forwarding rates, buffer utilisation

# Network Devices and Characteristics

---

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



# Network Devices and Characteristics

## FCAPS model

	Brief Definition	Main Practices
<b>Fault</b>	This working level aims to avoid faults in the networked systems, as well as mitigate consequences when they occur	Detection; Diagnosis/Isolation; Correlation/Aggregation; Restoration; Resolution
<b>Configuration</b>	At this working level, the networked systems are configured for properly working in their lifecycle	Inventory Update; Devices Configuration; Software Deployment and Updates
<b>Accounting</b>	Accounting tackles administrative tasks for networked systems and optimizes them for their users	Machinery Inventory Management; Generate Network Usage Statistics; Generate Client Statistics; Billing
<b>Performance</b>	This working level aims to improve the overall network performance, as well as the performance of the services running on it	Monitor Machines Overloads; Monitor Network Metrics; Monitor Quality of Service; Run Optimization Algorithms
<b>Security</b>	The working level that aims to control the access to systems' resources and keep them safe from malicious actions	Analyze incoming and outgoing traffic; Analyze running processes; Keep services available; Encrypt sensitive data

# 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

---

## What is Simple Network Management Protocol (SNMP)?

- SNMP is an Internet Standard protocol used for managing and monitoring network-connected devices in IP networks.
- SNMP is an application layer protocol that uses UDP port number 161/162.
- SNMP is used to monitor the network, detect network faults, and sometimes even to configure remote devices.

# Network Management Mechanisms

---

## Components of SNMP

- ① **SNMP Manager:** It is a centralized system used to monitor the network. It is also known as a Network Management Station (NMS). A **router** that runs the SNMP server program is called an agent, while a **host** that runs the SNMP client program is called a manager.
- ② **SNMP agent:** It is a software management software module installed on a managed device. The manager accesses the values stored in the database, whereas the agent maintains the information in the database. To ascertain if the router is congested or not, for instance, a manager can examine the relevant variables that a router stores, such as the quantity of packets received and transmitted.
- ③ **Management Information Base (MIB):** MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables. A MIB, or collection of all the objects under management by the manager, is unique to each agent. System, interface, address translation, IP, udp, and egp, icmp, tcp are the eight categories that make up MIB. The MIB object is home to these groups.

# Network Management Mechanisms

---

## SNMP Messages

- ① **GetRequest:** It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.
- ② **GetNextRequest:** To get the value of a variable, the manager sends the agent the GetNextRequest message. The values of the entries in a table are retrieved using this kind of communication. The manager won't be able to access the values if it doesn't know the entries' indices. The GetNextRequest message is used to define an object in certain circumstances.
- ③ **SetRequest:** It is used by the SNMP manager to set the value of an object instance on the SNMP agent.
- ④ **Response:** When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.
- ⑤ **Trap:** These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.
- ⑥ **InformRequest:** It was added to SNMPv2c and is used to determine if the manager has received the trap message or not. It is the same as a trap but adds an acknowledgement that the trap doesn't provide.

# Network Management Mechanisms

---

## SNMP Security Levels

- ① **noAuthNoPriv**: This (no authentication, no privacy) security level uses a community string for authentication and no encryption for privacy.
- ② **authNopriv**: This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.
- ③ **authPriv**: This security level (authentication, privacy) uses HMAC with MD5 or SHA for authentication and encryption uses the DES-56 algorithm.

# Network Management Mechanisms

---

## Versions of SNMP

- ① SNMPv1: It uses community strings for authentication and uses UDP only. SNMPv1 is the first version of the protocol. It is described in RFCs 1155 and 1157 and is simple to set up.
- ② SNMPv2c: It uses community strings for authentication. It uses UDP but can be configured to use TCP. Improved MIB structure elements, transport mappings, and protocol packet types are all included in this updated version. However, it also makes use of the current “community-based” SNMPv1 administrative structure, which is why the version is called SNMPv2c. RFC 1901, RFC 1905, and RFC 1906 all describe it.
- ③ SNMPv3: It uses Hash-based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, the conclusion is the higher the version of SNMP, the more secure it will be. NMPv3 provides the remote configuration of SNMP entities. This is the most secure version to date because it also includes authentication and encryption, which may be used alone or in combination. RFC 1905, RFC 1906, RFC 2571, RFC 2572, RFC 2574, and RFC 2575.6 are the RFCs for SNMPv3.



# Network Management Mechanisms

---

## Characteristics of SNMP

- ① SNMP is used to monitor network
- ② It detects any network faults
- ③ Can also be used to configure remote devices.
- ④ Allows a standardized way of collecting information about all kinds of devices from various manufacturers among the networking industry.

# Network Management Mechanisms

---

## Advantages of SNMP

- ① It is simple to implement.
- ② Agents are widely implemented.
- ③ Agent level overhead is minimal.
- ④ It is robust and extensible.
- ⑤ Polling approach is good for LAN based managed object.
- ⑥ It offers the best direct manager agent interface.
- ⑦ SNMP meet a critical need.

## Limitation of SNMP

- ① It is too simple and does not scale well.
- ② There is no object oriented data view.
- ③ It has no standard control definition.
- ④ It has many implementation specific (private MIB) extensions.
- ⑤ It has high communication overhead due to polling

# Network Management Mechanisms

---

- SNMP (IETF)
  - Provides facilities for collecting and configuring parameters from network devices
  - Unsolicited notification of events through traps
  - Accessible parameters are grouped into 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

---

## CMIP vs SNMP

- CMIP was designed in competition with SNMP, and has far more features than SNMP.
- For example, SNMP defines only "set" actions to alter the state of the managed device, while CMIP allows the definition of any type of action.
- CMIP was a key part of the Telecommunications Management Network, and enabled cross-organizational as well as cross-vendor network management.
- On the Internet, however, most TCP/IP devices support SNMP and not CMIP. This is because of the complexity and resource requirements of CMIP agents and management systems. CMIP is supported mainly by telecommunication devices.

# Network Management Mechanisms

---

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

# What is a MIB?

---

- A 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!
- It's an abstraction of the real world!

# 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

---

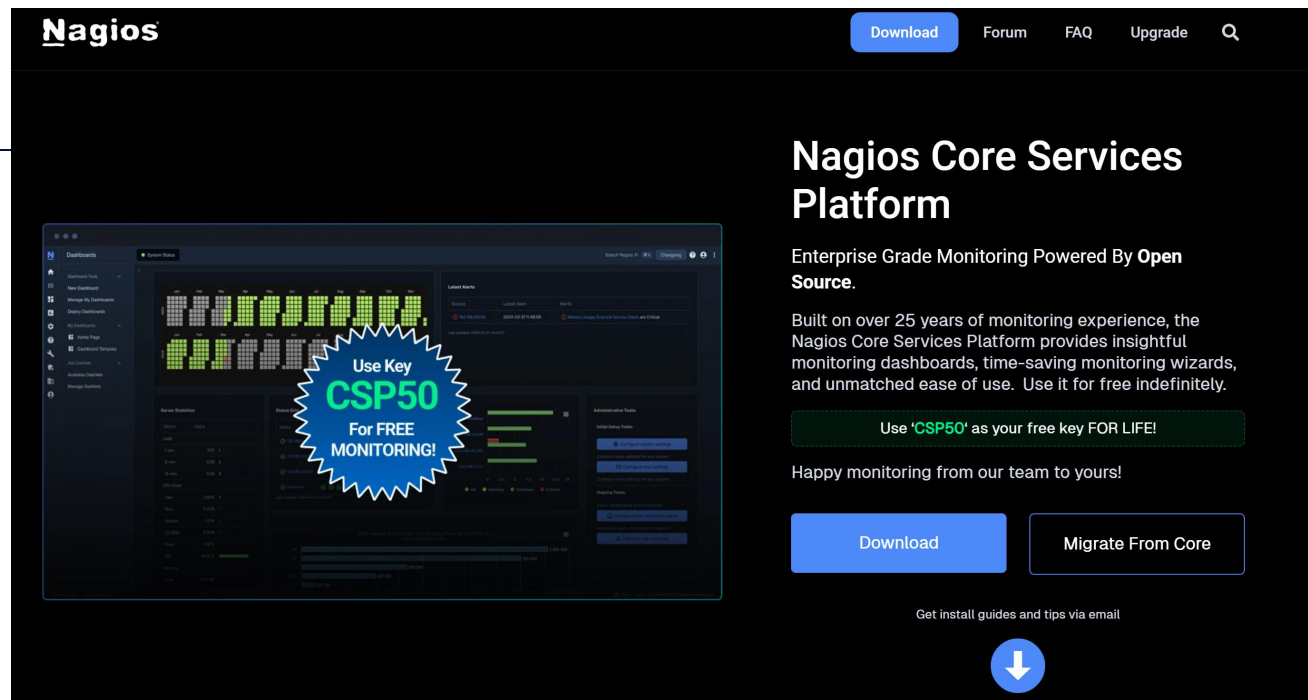
- Values for some characteristics will need to be derived from gathered data
- How and what you display about this information needs to be decided
  - Type of monitor
    - Standard VDU, Wide screen, multi-screen etc.
  - Display techniques
    - Logs, textual, graphs, charts, alarms
    - Animation, 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

# Nagios



**Nagios**

Download Forum FAQ Upgrade

## Nagios Core Services Platform

Enterprise Grade Monitoring Powered By **Open Source**.

Built on over 25 years of monitoring experience, the Nagios Core Services Platform provides insightful monitoring dashboards, time-saving monitoring wizards, and unmatched ease of use. Use it for free indefinitely.

Use 'CSP50' as your free key FOR LIFE!

Happy monitoring from our team to yours!

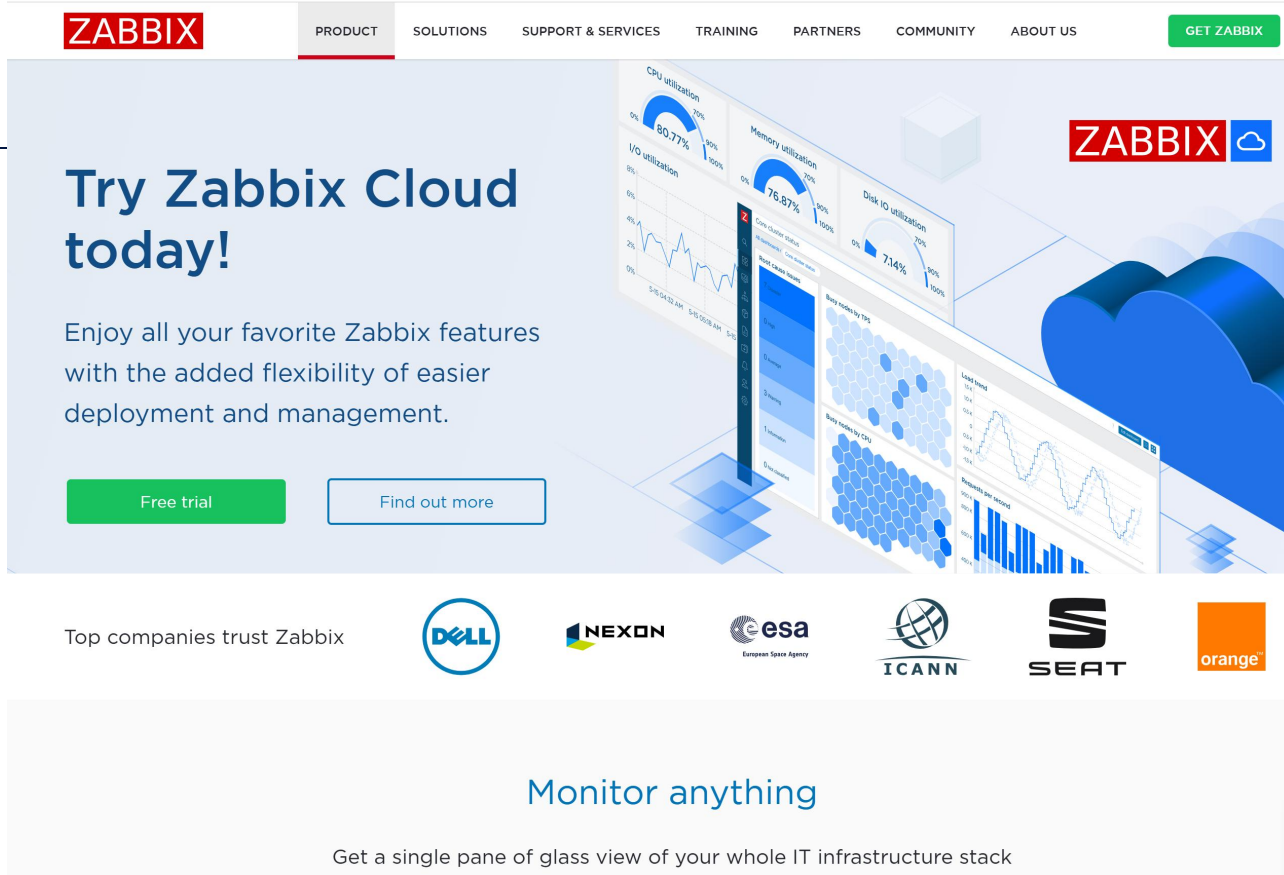
Download Migrate From Core

Get install guides and tips via email

↓

- Nagios is an event monitoring system that offers monitoring and alerting services for servers, switches, applications and services. It alerts users when things go wrong and alerts them a second time when the problem has been resolved.
- Nagios was originally designed to run under Linux, but it also runs on other Unix variants. It is free software licensed under the terms of the GNU General Public License version 2 as published by the Free Software Foundation.

# Zabbix









The image shows the Zabbix Cloud landing page. At the top is a navigation bar with links: PRODUCT, SOLUTIONS, SUPPORT & SERVICES, TRAINING, PARTNERS, COMMUNITY, ABOUT US, and a green 'GET ZABBIX' button. The main content area features the headline 'Try Zabbix Cloud today!' and a sub-headline 'Enjoy all your favorite Zabbix features with the added flexibility of easier deployment and management.' Below this are two buttons: 'Free trial' and 'Find out more'. To the right is a large graphic showing a 3D perspective of the Zabbix monitoring interface. This interface includes several widgets: 'CPU utilization' (80.77%), 'Memory utilization' (76.87%), 'I/O utilization', 'Disk I/O utilization' (73.4%), 'Load average', 'Queue per second', 'Busy nodes by IP', 'Busy nodes by CPU', and 'Queue per second'. The Zabbix logo is in the top right corner of the interface graphic. Below the main content area, there is a section titled 'Top companies trust Zabbix' with logos for Dell, NEXON, esa (European Space Agency), ICANN, SEAT, and orange.

**Try Zabbix Cloud today!**

Enjoy all your favorite Zabbix features with the added flexibility of easier deployment and management.

[Free trial](#) [Find out more](#)

Top companies trust Zabbix

**Monitor anything**

Get a single pane of glass view of your whole IT infrastructure stack

- Zabbix is an open-source software tool to monitor IT infrastructure such as networks, servers, virtual machines, and cloud services. Zabbix collects and displays basic metrics..



# 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

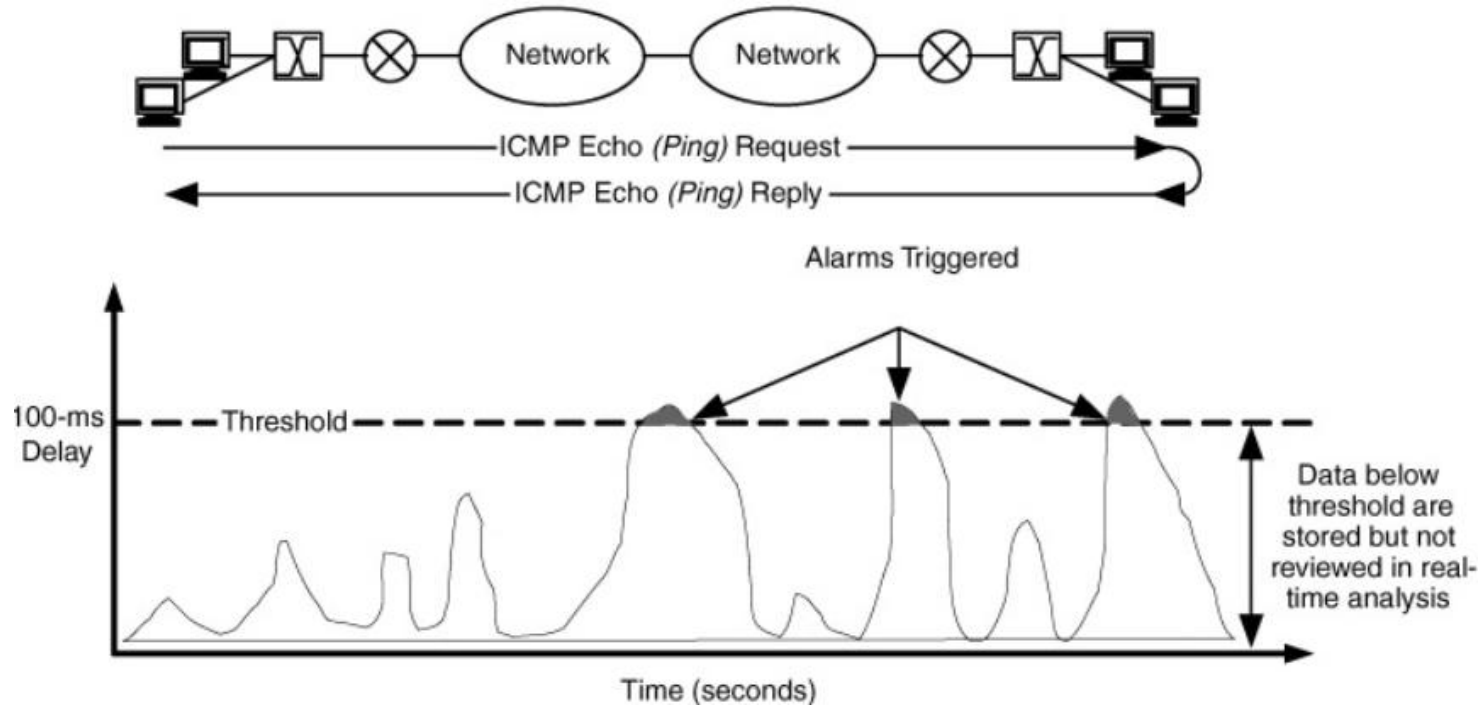
Ping statistics for 142.250.66.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 7ms, Average = 5ms
```

# 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 behavior 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



# 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
  - $(100 \text{ network devices}) \times (4 \text{ interfaces/network device}) \times (8 \text{ characteristics/interface}) = 3200 \text{ characteristics}$
- If each characteristic generates an average of 8 bytes of data and 60 bytes of protocol overhead, each polling session generates
  - $(3200 \text{ characteristics}) \times (68 \text{ bytes}) = 217600 \text{ bytes of data or } 1740800 \text{ bits/session or } 1.74 \text{ Mb of traffic}$

# 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
  - $(1,740,800 \text{ bits per polling interval}) \times (720 \text{ polling intervals/hour}) \times (24 \text{ hours/day}) = 30081024000 \text{ bits per day}$  approximate 30.2 Gb of traffic
- Data stored
  - $(3200 \text{ characteristics/polling interval}) \times (8 \text{ bytes}) \times (720 \text{ polling intervals/day}) \times (24 \text{ hours/day}) = 442368000$  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

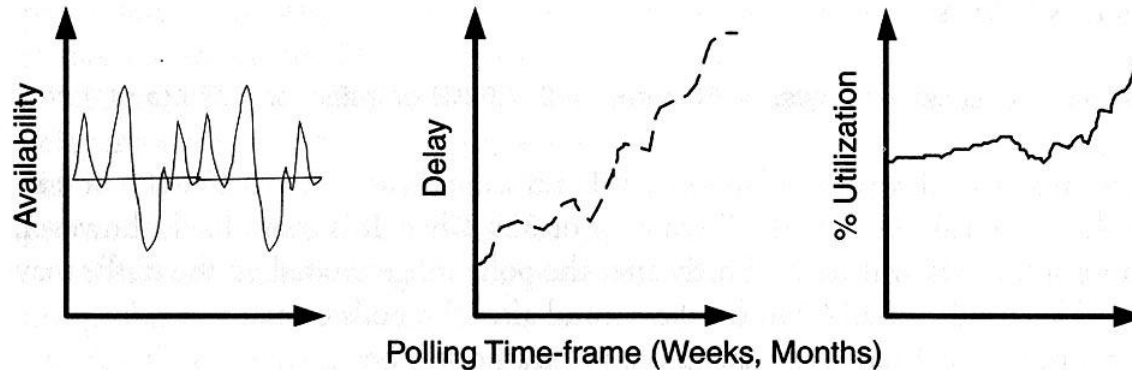
---

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

# Monitoring for Trend Analysis

---

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



**FIGURE 7.6** Monitoring for metrics and planning.

# 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

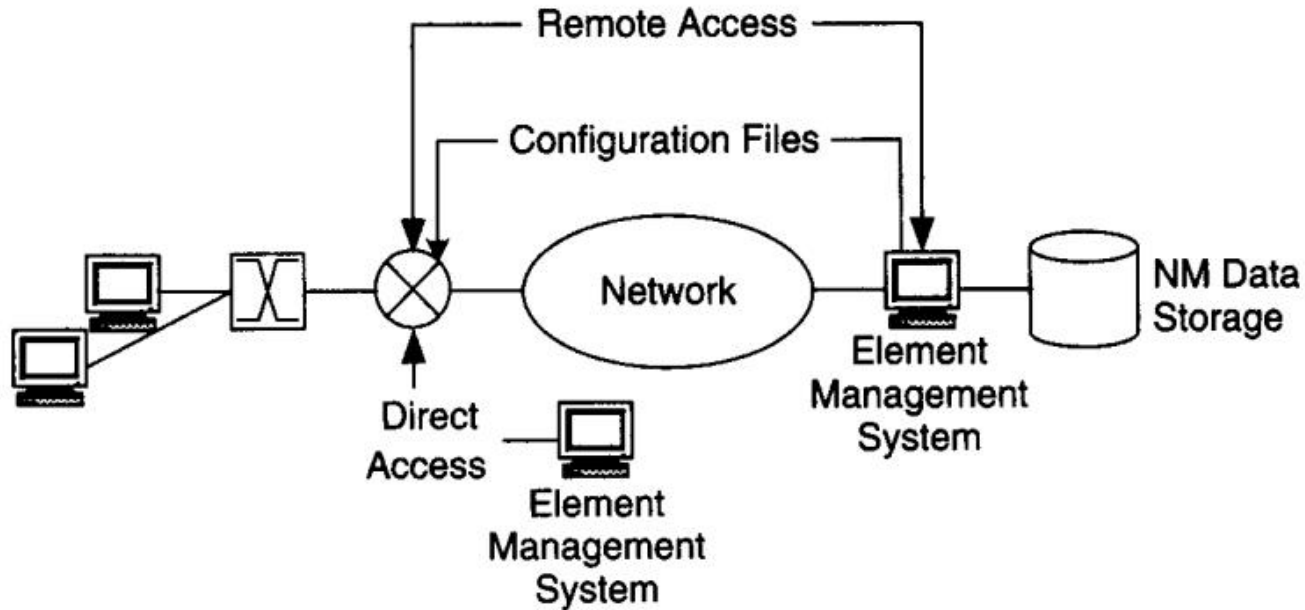
---

- 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

# 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
  - Centralised, 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

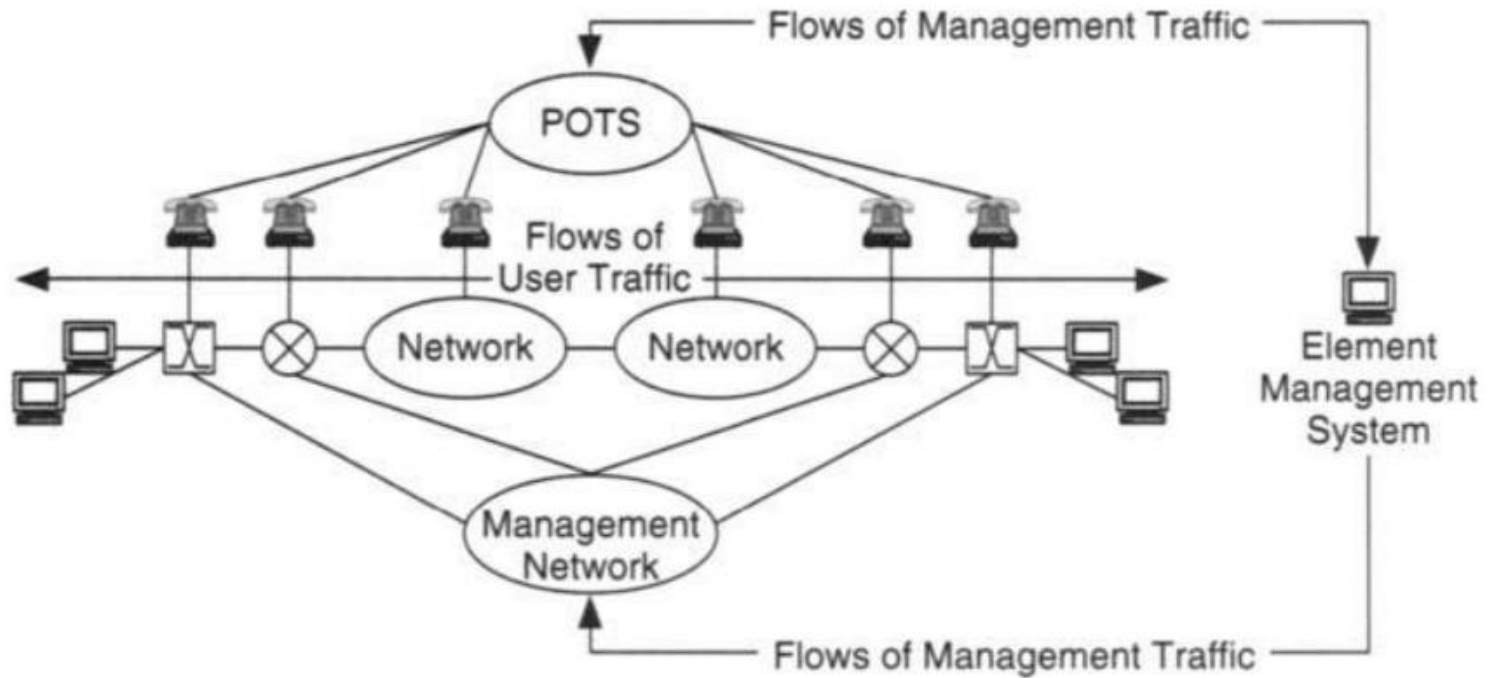
---

- 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



# 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.

# Centralised, Distributed and Hierarchical Management

---

## Centralised

- 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 localise traffic
  - Redundancy of monitoring
  
- Trade offs
  - Increased costs

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

---

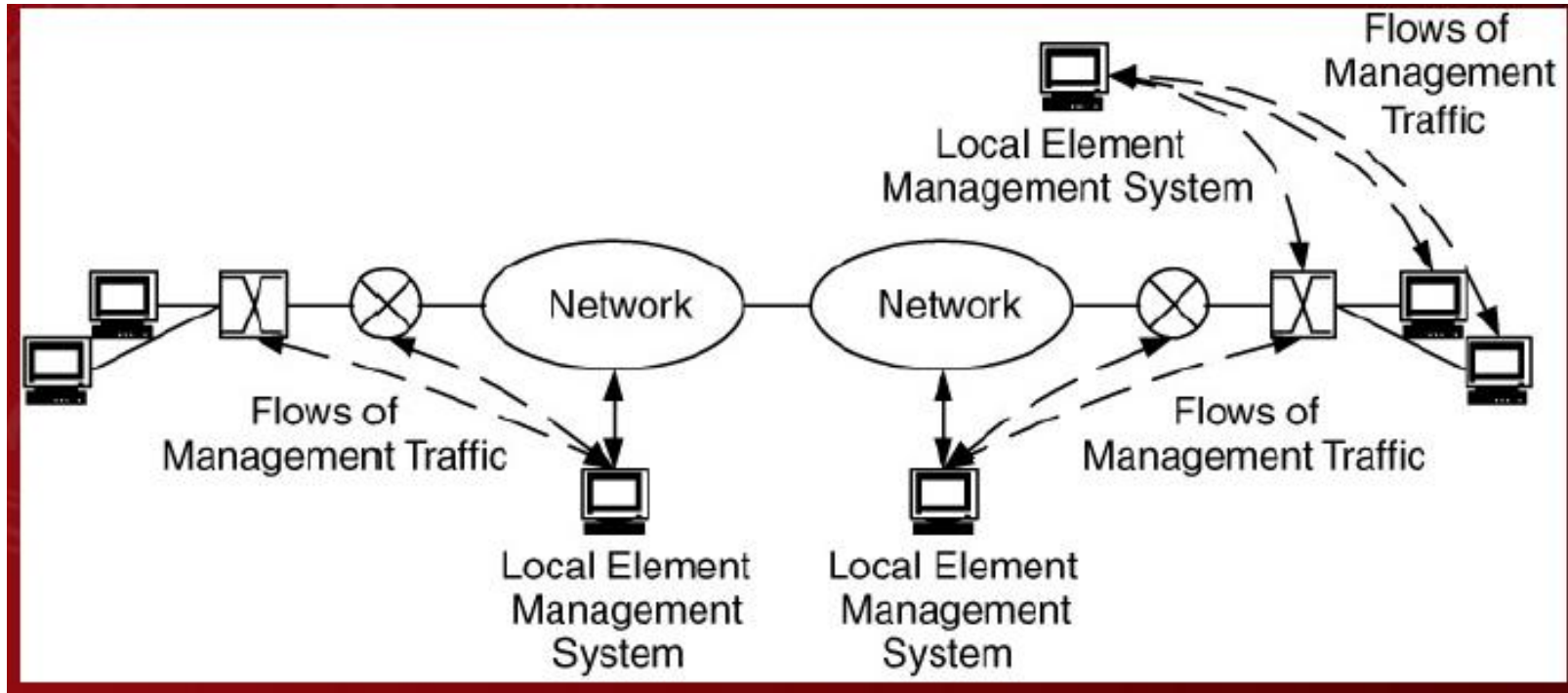
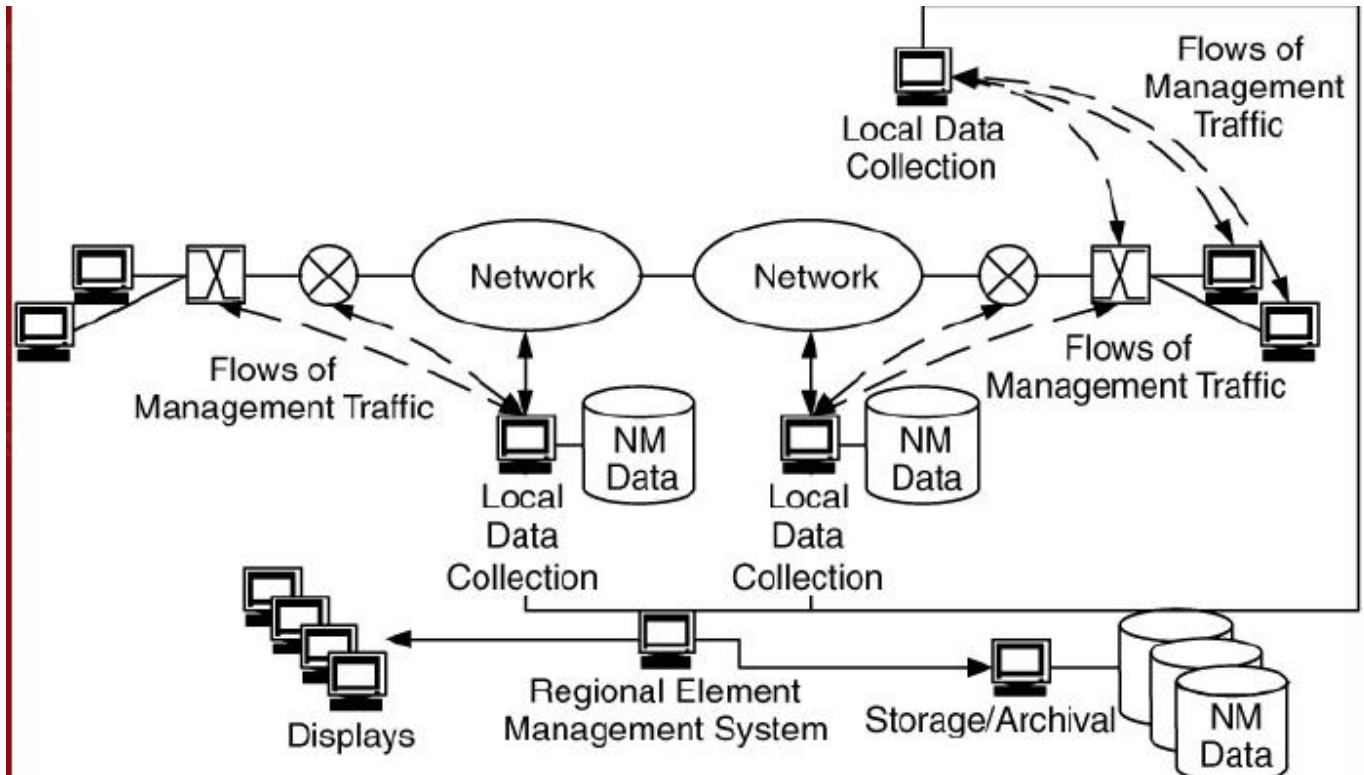


Figure: Hierarchical management separates management into distinct functions that are distributed across multiple platforms.



# 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

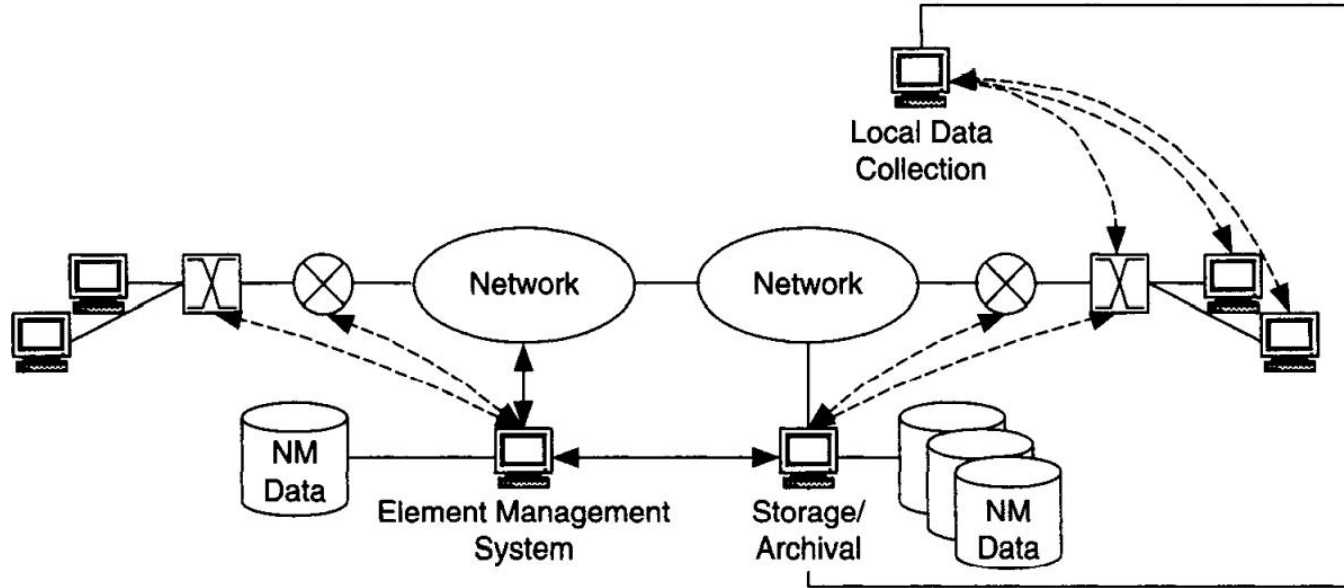


# Management of Network Management Data

---

- 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.

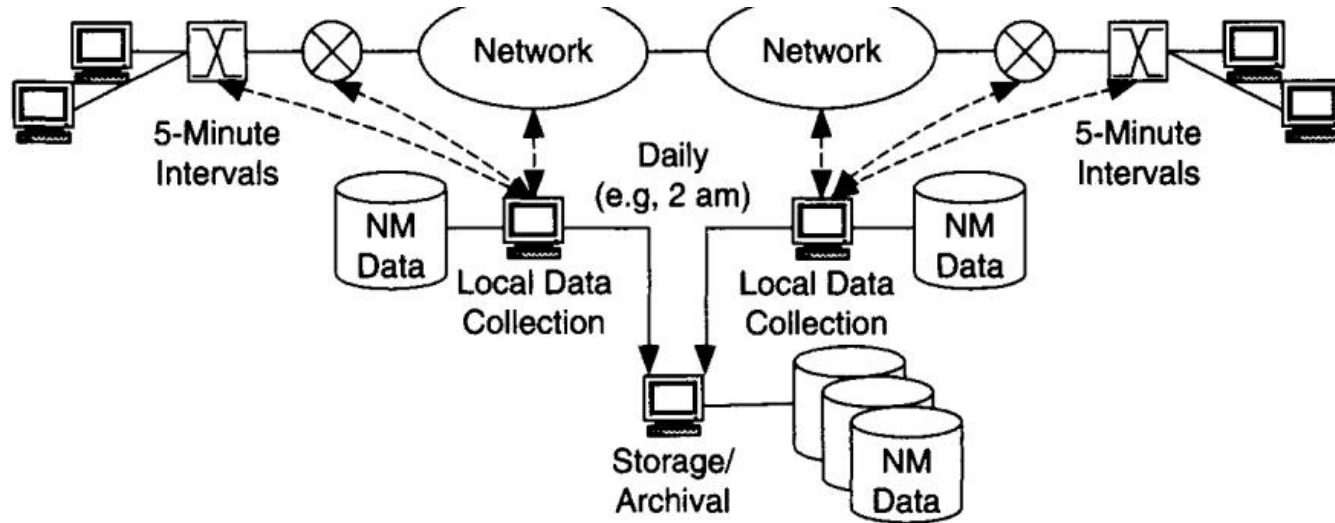
# Management of Network Management Data



**FIGURE 7.15** Local and Archival Storage for Management Data

# 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

# 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.

# Internal Relationship – Interactions

---

What is OSS (Operations Support System)?

- A OSS is a set of programs that helps a communications service provider monitor, control, analyze and manage a telephone or computer network.
- OSS supports management functions such as network inventory, service provisioning, network configuration and fault management.



# Internal Relationship – Interactions

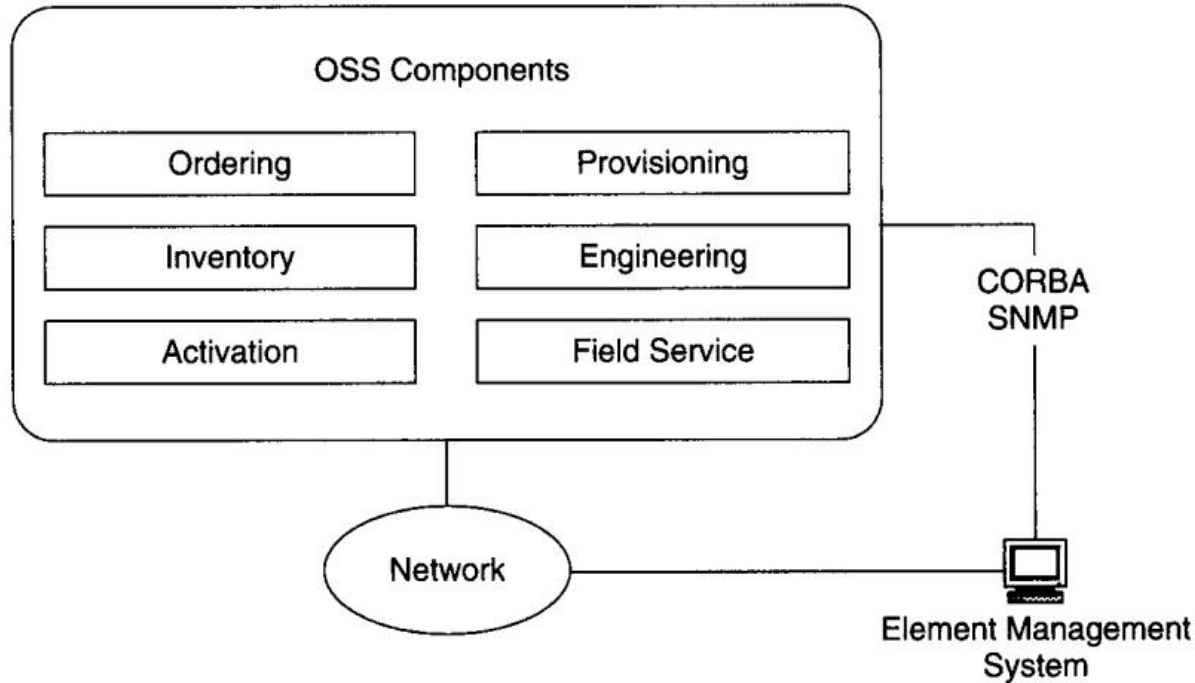
---

## What is OSS (Operations Support System)?

In general, an OSS covers at least the following five functions:

- ① Network management systems
- ② Service delivery
- ③ Service fulfillment, including the network inventory, activation and provisioning
- ④ Service assurance
- ⑤ Customer care

# Internal Relationship – Interactions



**FIGURE 7.18** The Integration of Network Management with OSS

# 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
  - Centralised
  - 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.



U

Thank you  
Q&A ?

O



UNIVERSITY  
OF WOLLONGONG  
AUSTRALIA

W