Unit 6: Network Management

6GZ71004 ADVANCED COMPUTER NETWORKS & OPERATING SYSTEMS

DR MOHAMMAD HAMMOUDEH

Reading

Stevenson, D. W. (1995), Network Management What it is and what it isn't. http://www.sce.carleton.ca/netmanage/NetMngmnt/NetMngmnt.html [Accessed December 1 2016]

Cisco. How Cisco IT Outsourced Network Management Operations . www.cisco.com/web/about/ciscoitatwork/downloads/ciscoitatwork/pdf/Cisco_IT_Case_Study_CiscoROS_CS.pdf [Accessed December 1 2016]

Cisco. Capacity and Performance Management: Best Practices White Paper. www.cisco.com/c/en/us/support/docs/availability/high-availability/20769-performwp.html [Accessed December 1 2016]

Unit Outline

What is Network Management

- Platform, applications, and system
- Architecture

OSI Network Management Model

- Performance
- Availability

What is Network Management?

Network Management is the process of controlling a complex data network to maximise its efficiency and productivity.

The Network Management Platform

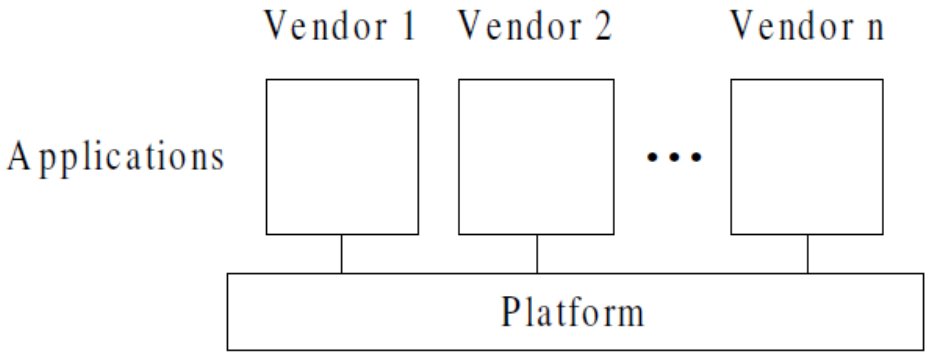
A network management platform is a software package that provides a generic functionality for managing a variety of network devices.

- A GUI
- A network map - autodiscovery, automapping
- A DBMS
- A standard method to query devices
- A event log
- A customisable menu system
- Graphing tools
- An API
- System security

Network Management Applications

Goals:

- Manage a specific set of devices
- Avoid functionality overlap with the platform
- Integrate with the platform through the API and menu system
- Reside on multiple platforms

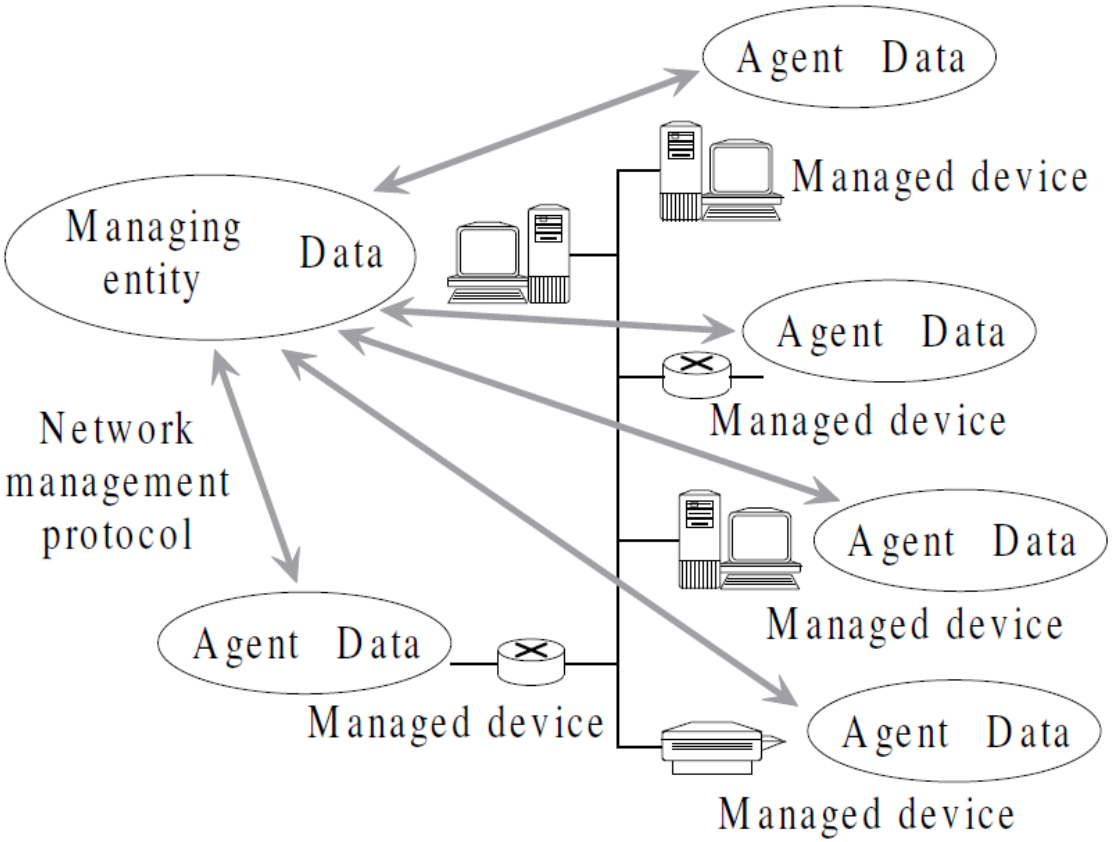


Relationship between network management platform and applications

The Network Management System

The network management system consists of the platform and the accompanying applications.

Principle Components of a Network Management Architecture



Managing entity: application running on a network

Management station: controls the collection, processing, analysis/display of network management information.

Managed device: network equipment. Within a managed device there may be several managed objects.

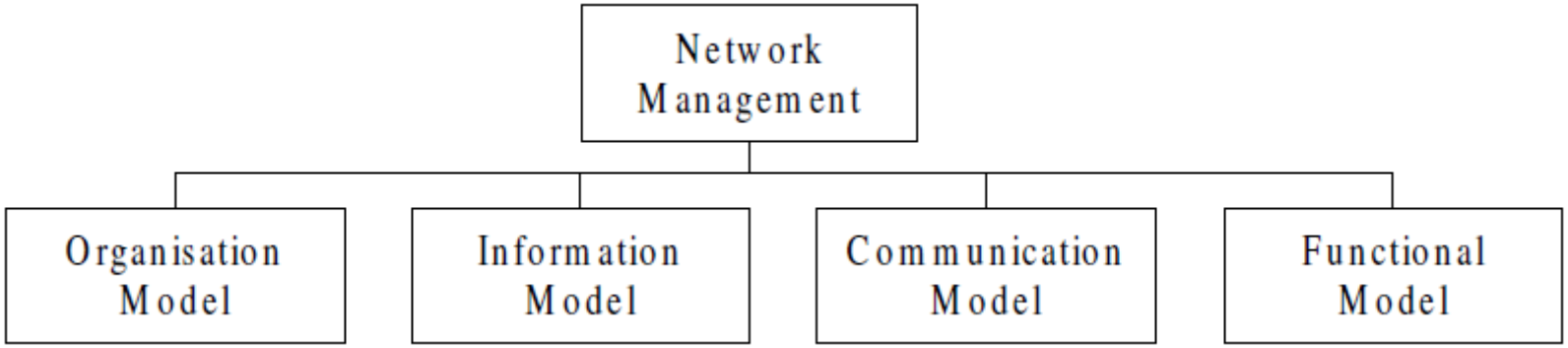
Managed objects: actual pieces of hardware within the managed device e.g. NIC and the sets of configuration parameters for the pieces of hardware and software.

Network management agent: process running on a managed device that communicates with the management entity and takes local actions on managed device under control of management entity

Network management protocol: runs between the management entity and a managed device and allows querying of status and action to be taken on the device via the agent. Agents can use the protocol to inform the management entity of exceptional events (traps).

OSI Network Management Model

TCP/IP Internet Standard Management Framework Architecture



SNMP Framework Components

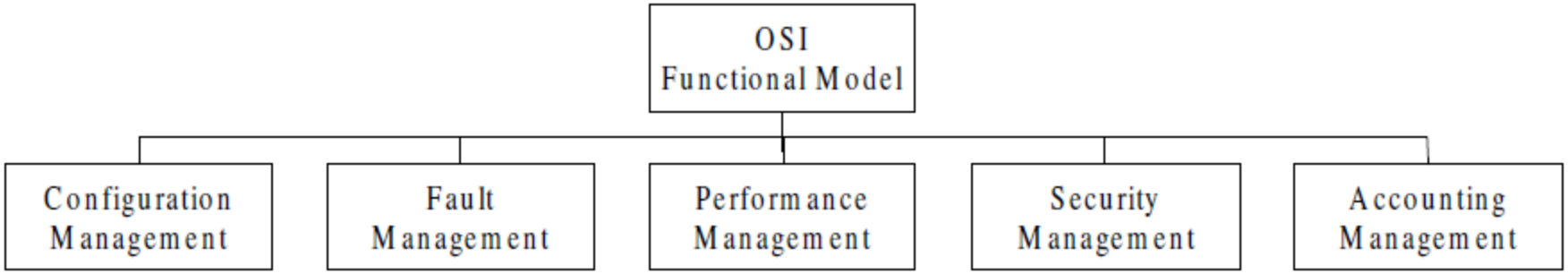
SNMP Framework Components

Structure of Management Information (SMI): is a standard that defines the structure, syntax and characteristics of management information in SNMP.

Management Information base (MIB): is the full set of these variables that describe the management characteristics of a particular type of device.

Simple Network Management Protocol (SNMP)**:** It defines how information is exchanged between SNMP agents and network management stations. [GetRequest, SetRequest, GetNextRequest, GetBulkRequest, Response, Trap, InformRequest]

Functional Model



Control Functions

Configuration management:

- Determining and setting the configuration of devices
- In a broad sense configuration management also covers network provisioning which includes network planning and design. Network provisioning is based on performance statistics and QoS requirements.

Security:

- Covers a broad range of security aspects

Monitoring Functions

Fault:

- Detection, isolation, response — correction (if possible), logging.
- Fault detection is accomplished either by polling or the generation of traps. e.g., polling – a fault management application generates a ping periodically and waits for a response. When a preset number of responses are not received connectivity is declared broken.
- The advantage of traps over polling is that failure detection is accomplished faster with less traffic overhead.

Monitoring Functions

Accounting:

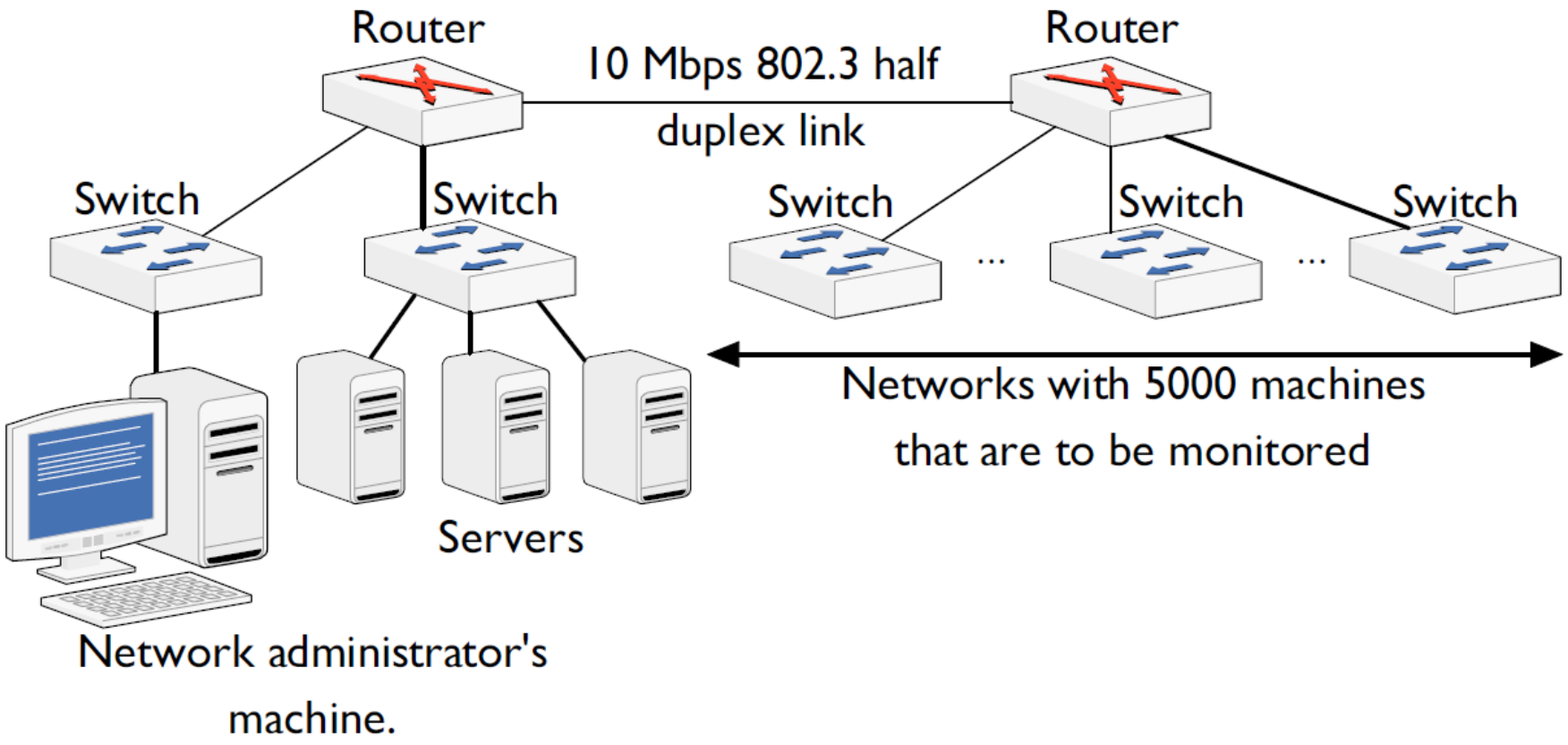
- Specifying, logging and controlling user and device access to network resources.
- Gathering statistics in order to make decisions about the allocations of network resources. e.g. querying activity logs on individual hosts or traffic counters from network devices

Performance:

- Quantify, measure, report, analyse and control the performance of different network components.
- Data traffic management.
- Involves data monitoring, problem isolation, performance tuning, statistical trend analysis and resource planning.
- Performance parameters: throughput, response time, network availability and network reliability.

Network Monitoring Calculation Example:

A network administrator wishes to monitor 5000 workstations to see whether they are switched on or not. In order to do this each machine is periodically pinged. The message size in both directions is $174\ bytes$. This **includes** $20\ bytes$ of IP. The administrator's NMS (network management station) is on a $10\ Mbps$ 802.3 switched LAN operating in half-duplex. If each machine is pinged every 50 seconds determine the maximum percentage of the capacity of the LAN connection that is being used in monitoring the workstations. The overhead of the 802.3 frame is 26 bytes.


Router
10 Mbps 802.3 half
duplex link
Router
Switch
Switch
Switch
Switch
Switch
...
...
Networks with 5000 machines
that are to be monitored
Servers
Network administrator's
machine.

1. How long does it take to send a “ping”?
2. How long will it take to send 5000 pings?
3. How long does it take to monitor 5000 machines?
4. What fraction of $50s$ is used in monitoring the 5000 machines?
5. What percentage of the time is used in monitoring the 5000 machines?

Number of bytes each way in each “ping” packet

$= 174 + 26 = 200\ bytes.$

Time taken to transmit 200 bytes, including interframe gap

$= (200 \times 8)/(10 \times 10^6) + IFG = 0.16 \times 10^{-3} + 9.6 \times 10^{-6} s = 0.1696\ ms.$

So time taken to send and receive a ping

$= 0.3392\ ms.$

Time required to monitor 5000 workstations once

$= 5000 \times 0.3392 \times 10^{-3} = 1.696\ s.$

So percentage of time used in monitoring stations

$= (1.696 / 50)\ x\ 100 \sim 3.4\%.$

Service-oriented Performance Indicators

A system or activity cannot be managed or controlled unless its performance is monitored. Measures of performance can be classified as either service-oriented or efficiency-oriented.

Availability: The fraction of the time that a network system, component or an application is available to the user.

Response time: The time it takes for the system to respond to a request to perform a particular task.

Accuracy: The percentage of time that no errors appear in the transmission and delivery of information.

Availability

This is based on the reliability of the individual components of a network.

Reliability

The probability that a component will perform its specified function for a specified time under specified conditions.

For a component the availability can be expressed as

$$A = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

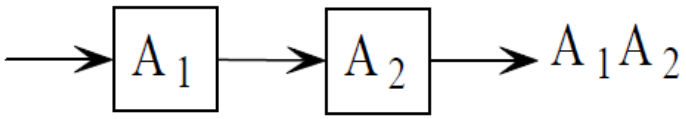
where MTBF = the mean time between failure and MTTR = the mean time to repair.

The availability of a system depends upon:

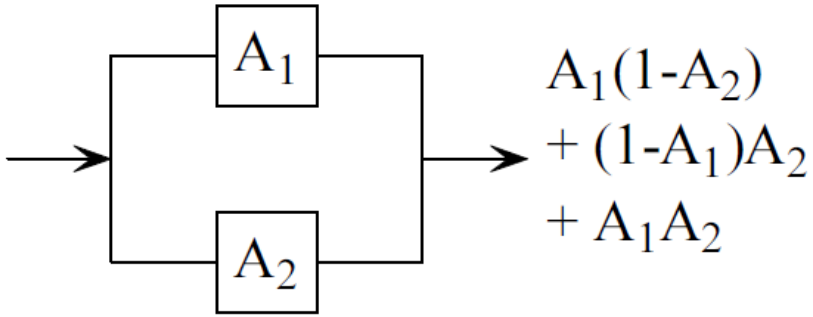
1. the availability of its individual components
2. the system organisation

For example the system may be organised to make use of redundant components in the case component failure or it may still be able to function but with reduced capabilities.

Availability of serial connections



Availability of parallel connections



A1 x A2 = the probability that link 1 is up
x the probability that link 2 is up

A1(1 - A2) = the probability that link 1 is up
x the probability that link 2 is down

(1 - A1)A2 = the probability that link 1 is down
x the probability that link 2 is up

Availability and Load

Complex configurations complicate the analysis of system availability as does taking into account the load on the system.

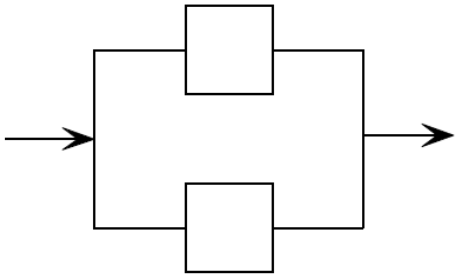
The functional availability, A_f =

(capacity of one link) x (probability one link is up)

+ (capacity of both links) x (probability both links are up)

Example

Consider a dual link system as shown below in which non-peak periods account for 30% of requests. During non-peak periods either link can handle the traffic load. During peak periods both links are required to handle the full load, but a single link can only handle 75% of the peak. If the availability of either link is 0.92, on average what percentage of requests for service can be handled by the system.



The probability that both links are up is A^2, where A is the availability of either link.

The probability that exactly one link is up is

$$A(1 - A) + (1 - A)A = 2A - 2A^2.$$

So in this case the probability that both links are up is

$$0.92^2 = 0.8464$$

and the probability that exactly one link is up is

$$2 \times 0.92 - 2\ 0.92^2 = 0.1472.$$

Since one link is sufficient for nonpeak loads

$$A_f\,(nonpeak) = (1.0) \times (0.1472) + (1.0) \times (0.8464) = 0.9936$$

and, for peak periods,

$$A_f\,(peak) = (0.75) \times (0.1472) + (1.0) \times (0.8464) = 0.9567$$

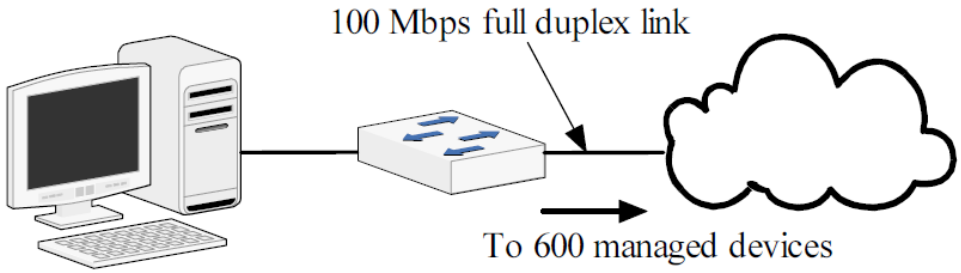
The overall functional availability is

$$\begin{aligned} A_f &= 0.7 \times Af\,(peak) + 0.3 \times Af\,(nonpeak) \\ &= 0.7 \times 0.9567 + 0.3 \times 0.9936 \\ &= 0.9678 \end{aligned}$$

So on average 97% of requests can be handled by the system.

Another Network Monitoring Calculation Example

It has been decided to remotely monitor the connectivity of 600 networked devices. The polling station connects via a $100\ Mbps$ full duplex fast Ethernet connection.



Determine the fastest rate at which a device can be polled if no more that 0.1% of the capacity of the link is to be used in polling. Hints: What is the minimum size of ICMP echo request and echo reply messages? What is the minimum size of an Ethernet frame? The inter-frame gap in $100\ Mbps$ Ethernet is $960\ ns$.

Minimum size of an ICMP echo request/reply message

$= 8\ bytes.$

IP header $= 20\ bytes.$

So minimum size ping packet $= 28\ bytes.$

```
hammoudeh@hardy:~$ ping -s 0 -c 1 149.170.13.7
PING 149.170.13.7 (149.170.13.7) 0(28) bytes of data.
8 bytes from 149.170.13.7: icmp_seq=1 ttl=64
```

Minimum size of data in Ethernet frame = 46 bytes.

Since this is more than the minimum size ping packet the packet would be padded with 18 bytes, and would be carried in a minimum size Ethernet frame of 72 bytes $(7 + 1 + 12 + 2 + 46 + 4)$.

Since communication is full duplex only transmission (or reception) need be considered.

Time taken to transmit 600 minimum size Ethernet frames on 100 Mbps Ethernet $= 600 \times \frac{72\ x\ 8}{100\ x\ 10^6} + 960 \times 10^{-9}]$

$= 4.032\ ms$

If 0.1% of the capacity is to be used in polling and T is the time between successive polls of the devices

$$\frac{4.032 \times 10^{-3}}{T} = \frac{1}{1000}$$

So T, the polling interval $= 1000 \times 4.0 \times 10^{-3} \sim 4\ s$