# Network Management

## Slide Set 3

# Learning Objectives

- Understand what is required to manage the day-to-day operation of networks
- Be familiar with the network management organization
- Understand configuration management
- Understand performance and fault management
- Be familiar with end users support
- Be familiar with cost management
- Understand the role and functions of network management software
- Be familiar with several types of network management hardware tools

# Outline

- **Introduction**
- **Organizing the Management Function**
  - *The Shift to LANs and the Internet*
  - *Integrating LANs, WANs and the Internet*
  - *Integrating Voice and Data Communications*
- **Configuration Management**
  - *Configuring the Network and Client Computers*
  - *Documenting the Configuration*
- **Performance and Fault Management**
  - *Network Monitoring, Failure Control Function, Performance and Failure Statistics, Improving Performance*
- **End User Support**
  - *Resolving Problems, Providing End User Training*
- **Cost Management**
  - *Sources of Costs, Reducing Costs*
- **Network Management Tools**
  - *Network Management Software*
  - *Network Management Hardware*

# Introduction

- Network management means monitoring and controlling the network so that it is working properly and providing value to its users.
- A lack of planning and organization can mean that network managers spend most of their time **firefighting** - dealing with breakdowns and immediate problems.
- The main areas of network management are:
  - Configuration Management
  - Performance and Fault Management
  - End-user support
  - Cost Management
  - Security

# The Shift to LANs and the Internet

- Since the 1980's networks have moved from using mainframes and terminals to PCs, LANs and the Internet.

- Mainframes are still important, but network management now focuses more on LANs, BNs and Internet resources.

- Currently, a critical issue is the integration of organizational networks and applications. There are two main problems.

- One integration problem is the <u>technical compatibility</u> of technologies and protocols.

- A second one is in the <u>cultural differences</u> in personalities and management styles of network managers. WAN & mainframe managers prefer more highly structured and controlled environments than do LAN and Web managers.

# Integrating Voice & Data Communications

- Traditionally, voice and data networks were separate, i.e., the telephone system and the organizational LAN, respectively.

- Separate networks mean higher network costs as well as additional staffing requirements.

- Integrating voice and data simplifies the network, and can lower network costs.

- Most organizations will likely integrate voice and data within the next 5 years.

# Configuring Network and Client Computers

- **Configuration management** means configuring the network's hardware and software and documenting that configuration.

- Two common configuration activities are
  - adding and deleting user accounts.
  - updating the software on the client computers attached to the network.

- Electronic software delivery (ESD) can be used to manage costs by eliminating the need to manually update each and every client computer.

# Documenting Hardware and Software

- Configuration documentation includes information on network hardware, software, and user and application profiles.

- Net hardware documentation uses a set of maps.

- This must be supplemented with lists of hardware details on each component such as serial number, vendor, date of purchase, warranty information, repair history, phone number for repairs, etc.

- Documenting network software is similar, but includes other information such as the network OS, software release date and site license details.

# Documenting User and Application Profiles

- The third documentation type is the user and application profiles, which must be automatically provided by the network Operating System or outside software agreements.

- Other network documentation that must be routinely developed and updated include software, standards and operations manuals, vendor contracts, and licenses.

- Documentation should include details about performance and fault management, maintenance guidelines, DRP, end-user support and cost management.

# Performance and Fault Management

- **Performance management**: ensuring the network is operating as efficiently as possible.

- **Fault management**: preventing, detecting, and correcting faults in the network circuits, hardware, and software.

- The two are interrelated. Both require **network monitoring**, i.e., tracking the operation of network circuits and devices to determine how heavily they are being used and ensure they are operating properly.

# Network Monitoring

- Most organizations use network management software to monitor and control their networks.

- The parameters monitored by a network management system fall into two distinct categories: physical network statistics and logical network information.

# Network Monitoring Parameters

- **Physical network statistics** come from monitoring the operation of modems, multiplexers, and circuits linking hardware devices.

- **Logical network parameters** include performance measurement systems that track user response times, traffic volume on a specific circuit, the destinations of network packets, and other indices showing the network's service level.

- **Performance tracking** is important since it enables network managers to be proactive and respond to problems before users complain, otherwise network management can revert to firefighting.

# Failure Control Function

- Failure control requires problem reporting, often handled by the Help Desk.

- A central troubleshooting group should also be responsible for contacting hardware, software vendors or common carriers.

- To aid in network monitoring, **managed devices** are now being installed that record data on the messages they process and send this information back to a central management database. (see SNMP later)

- Numerous software packages are available for recording fault information. These produce reports called **trouble tickets**.

# Handling Network Problems

- Managers use trouble tickets to do **problem tracking**, enabling them to systematically address problems, tracking who is responsible for problem correction and how it's being resolved.

- This also allows **problem prioritization** ensuring critical problems get higher priority.

- Finally, maintaining a **trouble log** is helpful for reviewing problem patterns on the network and can be used to identify which network components are the most problematic.

# Performance and Failure Statistics

- The main performance statistics are the number of packets moved on a circuit and the **response time**.

- Another factor is **availability**; the percent of time the network is available. **Downtime** is the percent of time the network is not available.

- Failure statistics include:

  - **Mean time between failures (MTBF)** indicates the reliability of a network component.

  - **Mean time to repair (MTTR)** equal to the mean time to diagnose plus the mean time to respond plus the mean time to fix a problem.

  **MTTRepair** = **MTTDiagnose** + **MTTRespond** + **MTTFix**

# Availability and Reliability

Availability $= \dfrac{uptime}{uptime + downtime} = \dfrac{MTBF}{MTBF + MTTR}$

| Availability | Lost Time (hours) | Lost Time (minutes) | Lost Time (seconds) |
|---|---|---|---|
| 60.00% | 3504 | | |
| 65.00% | 3066 | | |
| 70.00% | 2628 | | |
| 75.00% | 2190 | | |
| 85.00% | 1314 | | |
| 90.00% | 876 | | |
| 95.00% | 438 | | |
| 96.00% | 350.4 | | |
| 97.00% | 262.8 | | |
| 98.00% | 175.2 | | |
| 99.00% | 87.6 | | |
| 99.50% | 43.8 | | |
| 99.90% | 8.76 | 525.6 | |
| 99.99% | 0.876 | 52.6 | 3153.6 |
| 99.999% | 0.0876 | 5.3 | 315.36 |
| 99.9999% | 0.00876 | 0.5 | 31.536 |
| 99.99999% | 0.000876 | 0.1 | 3.1536 |

1 year = 365 days/yr * 24 hrs/day = 8760 hrs/yr

Reliability $\mathrm{e}^{-T/\Phi}$

$=$

Reliability $\mathrm{e}^{-\Lambda T}$

$=$

Reliability $\mathrm{e}^{-N}$

$=$

| Reliabililty | Failures per year | Failures per 10 years | Failures per 100 years |
|---|---|---|---|
| 10.00% | 2.30 | | |
| 20.00% | 1.61 | | |
| 30.00% | 1.20 | | |
| 40.00% | 0.92 | | |
| 50.00% | 0.69 | | |
| 60.00% | 0.51 | | |
| 70.00% | 0.36 | | |
| 80.00% | 0.22 | 2.23 | |
| 90.00% | 0.11 | 1.05 | |
| 95.00% | 0.05 | 0.51 | |
| 99.00% | 0.01 | 0.10 | 1.01 |
| 99.50% | 0.005 | 0.05 | 0.50 |
| 99.90% | 0.001 | 0.01 | 0.10 |
| 99.99% | 0.0001 | 0.001 | 0.01 |
| 99.999% | 0.00001 | 0.0001 | 0.001 |
| 99.9999% | 0.0000010 | 0.00001 | 0.0001 |
| 99.99999% | 0.00000010 | 0.000001 | 0.00001 |

1 yr mission = 365 days/yr * 24 hrs/day = 8760 hrs/yr

*Where $\Phi = MTBF$, $\Lambda = $ Failure Rate*

*N = number of failures, T = mission time*

*Just as a reminde*

# Quality Control Chart used to track network performance



Circuit C had new hardware/software implemented here

Circuit B moved to a new microwave channel

Number of blocks in error

2000

1100

800

500

0

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Weeks

B

A

Circuit A is deteriorating

C

Upper control limit (1,100)

Lower control limit (500)
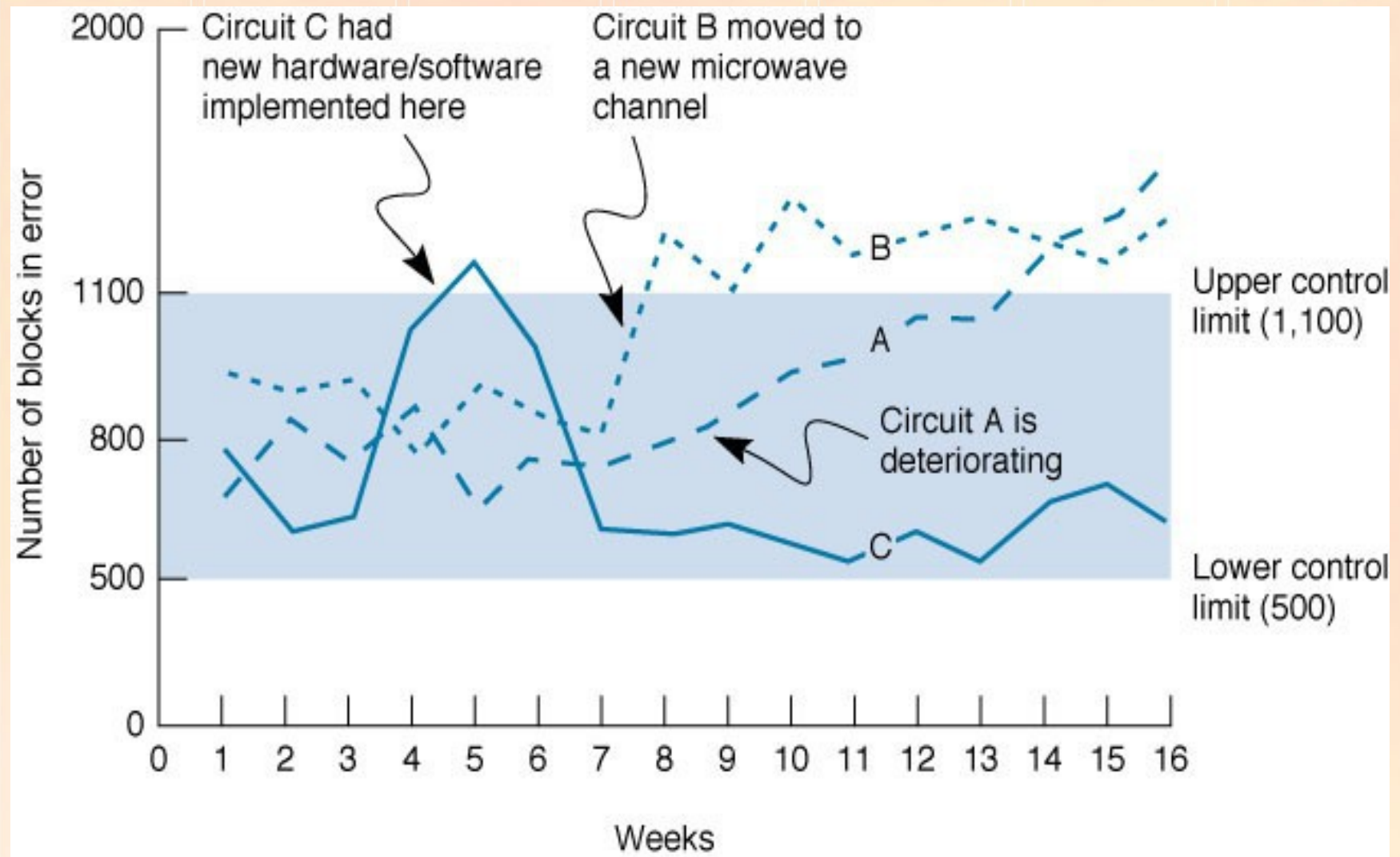
# Improving Performance

- There are three general activities related to performance management, whether on a LAN, BN or MAN/WAN:
  - Policy-based management
  - Server load balancing
  - Service-level agreements

# Policy-based Management

- In policy-based management the network manager uses special software to set priority policies for network traffic.

- These take effect when the network becomes busy.

- For example, video-conferencing might be given a high priority since delays will have the highest impact on the performance of that application.

# Server Load Balancing

- Load balancing means sharing the processing load between servers.

- A separate load balancing server is usually needed to allocate the work between processors.

- The load-balancing server then allocates tasks to the other processors, using an algorithm such as a round robin formula.

# Service Level Agreements

More organizations are beginning to establish service level agreements with their common carriers and service providers, which specifies the type of performance and fault conditions that the organization will accept.

# End User Support

- Supporting end users means solving the problems users have using the network.

- End-user support can be grouped into three areas:

  - Resolving network problems
  - Resolving software problems
  - Training

# Resolving Problems

- Problems stem from three major sources:
  - **Hardware device failures**
  - **A lack of user knowledge on proper operation**
  - **Problems with software, software settings or software compatibility**
- Problem resolution in large organizations is organized at three levels:
  - **The Help Desk handles basic queries**
  - **If this is not enough, staff members with specialized skills specific to the problem at hand are brought in**
  - **If the second level specialists are still not enough, technical specialists with a higher level of training are contacted to look into the problem**

# Providing End-User Training

- End-user training needs to be an ongoing part of network management.

- Training programs are also important since employees often change jobs within an organization and so the organization can benefit from cross-training.

- Training is usually conducted using in-class or one-on-one instruction or with online training materials provided.

# Cost Management

- Because of its large and rapidly growing budget, network management must carefully monitor network costs and will likely be called upon to justify cost increases.

- This requires measuring the cost of supporting users, allocating networking department budgets between hardware, software, personnel and other costs and understanding how these costs are changing.

# Total Cost of Ownership

- The **total cost of ownership** (TCO) is a measure of how much it costs per year to keep one computer operating.

- TCO studies indicate it can cost up to five times the value of the computer to keep it operational.

- The TCO for a typical Windows computer is about $8-12,000 per computer per year !!!

- Although TCO has been widely accepted, many organizations disagree with the practice of including user "waste" time in the measure and prefer to focus on costing methods that examine only the direct costs of operating the computer.
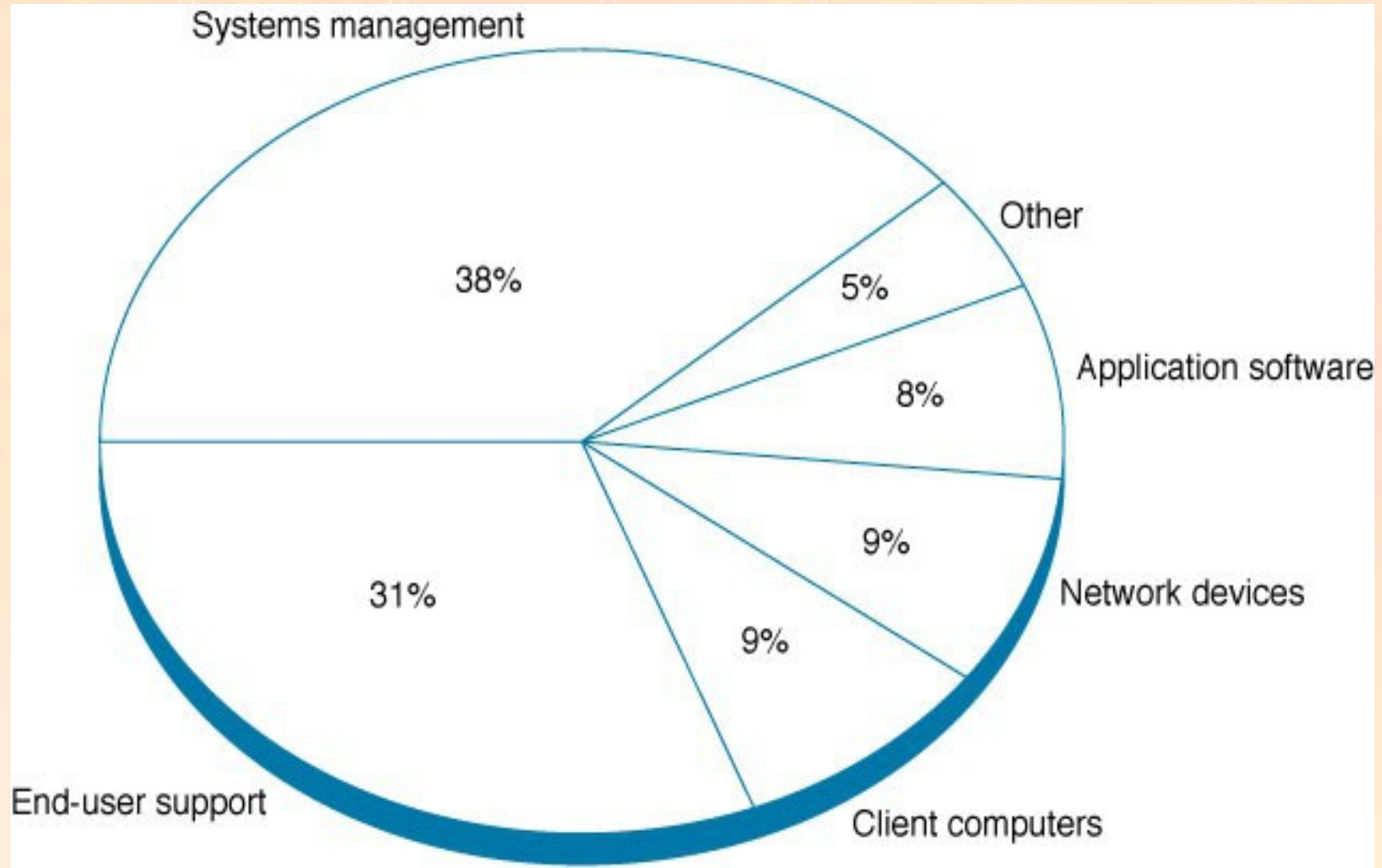
# Net Cost of Ownership

- **Net Cost of Ownership (NCO)** is an alternative to TCO that measures only direct costs, leaving out so-called "wasted" time.

- NCO costs per computer are between $1500-$3500, so management for a 100-user network require an annual budget of between $150,000-$350,000.

- Using NCO, the largest network budget items are:
  - **Personnel cost, accounting for 50-70% of costs**
  - **WAN circuits**
  - **Hardware upgrades and replacement parts**

# Network Personnel Costs

- Since the largest item in any network budget today is **personnel time**, cost management needs to focus on ways to reduce personnel time, not hardware costs.

- The largest use of personnel time is in **System management**.

- The second largest source is **User Support**.

# Network management personnel costs



Systems management — 38%
End-user support — 31%
Client computers — 9%
Network devices — 9%
Application software — 8%
Other — 5%

# Reducing Network Costs

**Five Steps to Reducing Network Costs:**

1. Develop standard hardware and software configurations for client computers and servers.

2. Automate as much of the network management function as possible by deploying a solid set of network management tools.

3. Reduce the costs of installing new hardware and software by working with vendors.

4. Centralize Help Desks.

5. Move to thin-client architectures.

# Network Management Software

- Network management software is designed to provide automated support for some or all of the network management functions.

- There are three fundamentally different types of network management software:
  - Device management software
  - System management software
  - Application management software

# Network management software (Source: HP OpenView)
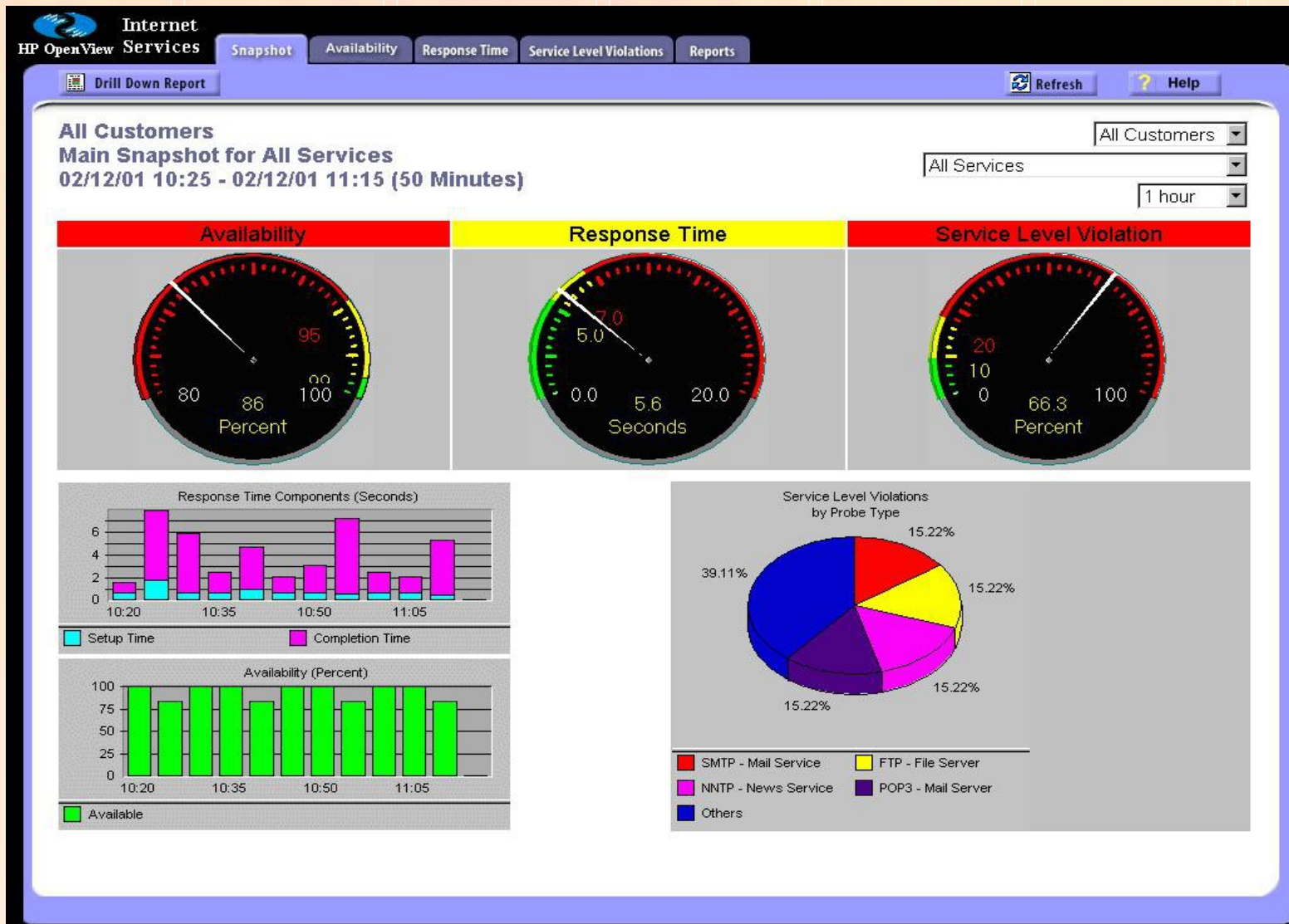
# Network Management Software

- One major problem is ensuring that hardware devices from different vendors can understand and respond to the messages sent by the network management software of other vendors.

- The two most commonly used network management protocols are:

  - Simple Network Management Protocol (SNMP, part of the TCP/IP protocol suite)

  - Common Management Interface Protocol (CMIP, developed by ISO)

# Simple Network Management Protocol

- **SNMP**: TCP/IP suite protocol for network management that allows agents to communicate with each other and other network devices

- **Agents**: programs residing on network devices that gather and share network status information

- **Management Information Bases (MIBs)**: databases of network status statistics such as traffic levels, error rates & data rates

- **Network Management Console**: when requested, data from the MIBs is sent to a Network Management Console.

# Network Management with SNMP (More Later)
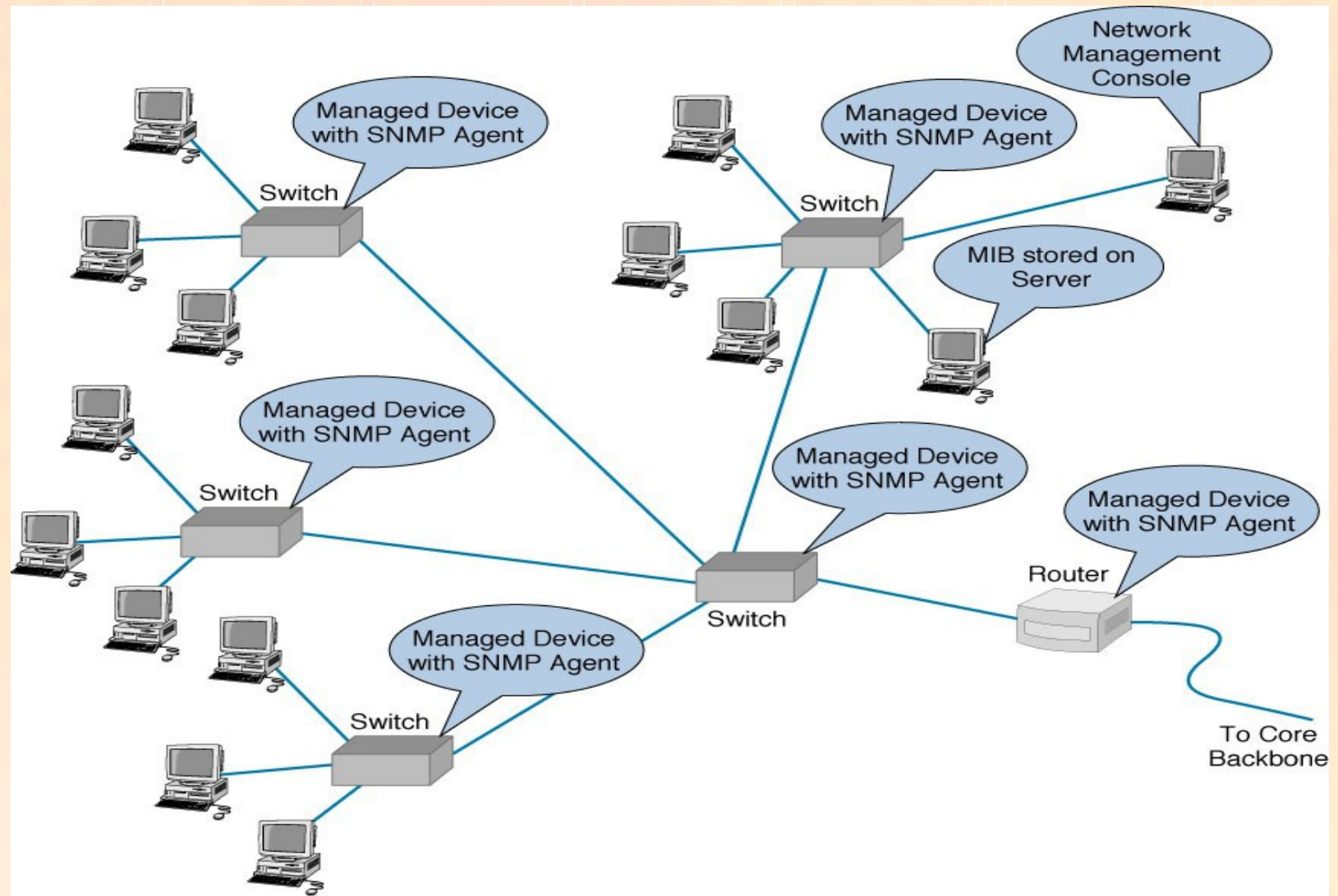
# Network Management Hardware

- Most network management hardware is used to test circuits. Circuit testing can be divided into three areas:

- **Analogue testing** involves troubleshooting the communications circuits on the analog side of the modem supplied by common carriers.

- **Digital testing** involves testing digital communication circuits.

- **Protocol testing** involves testing the sign-on/sign-off procedures, checking the contents of packets, and examining message transmission times.