NETWORK MANAGEMENT

- **Network Management** refers to the assessment, monitoring, and maintenance of all aspects of a network.
- It can include checking for hardware faults, ensuring high QoS (quality of service) for critical applications, maintaining records of network assets and software configurations, and determining what time of day is best for upgrading a router.
- Ideally, network management helps the administrator predict problems before they occur. For example, a trend in network usage could indicate when a switch will be overwhelmed with traffic. In response, the network administrator could increase the switch's processing capabilities (or replace the switch) before users begin experiencing slow or dropped connections.

Types of documentation that contribute to sound network management.

- To adequately manage your network, you should at least record the following:
  - Physical topology—Which types of LAN and WAN topologies does your network use: bus, star, ring, hybrid, mesh, or a combination of these? Which type of backbone does your network use—collapsed, distributed, parallel, serial, or a combination of these? Which type and grade of cabling does your network use?
  - Access method—Does your network use Ethernet (802.3), token ring (802.5), Wi-Fi (802.11), WiMAX (802.16), or a mix of transmission methods? What transmission speed(s) does it provide? Is it switched?

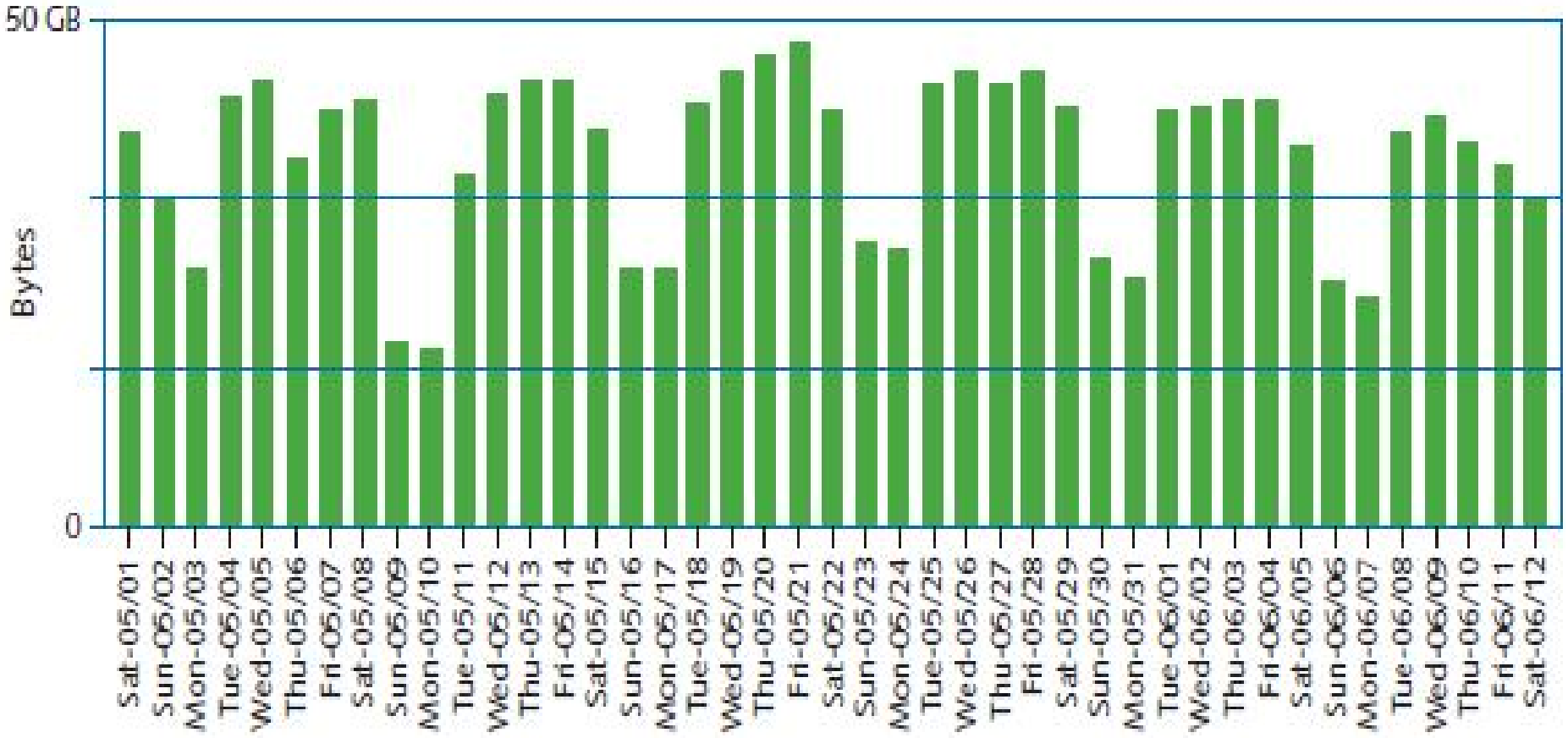
- Protocols—Which protocols are used by servers, nodes, and connectivity devices?
- Devices—How many of the following devices are connected to your network— switches, routers, hubs, gateways, firewalls, access points, servers, UPSs, printers, backup devices, and clients? Where are they physically located? What are their model numbers and vendors?
- Operating systems—Which network and desktop operating systems appear on the network? Which versions of these operating systems are used by each device? Which type and version of operating systems are used by connectivity devices such as routers?
- Applications—Which applications are used by clients and servers? Where do you store the applications? From where do they run?

– Configurations—What versions of operating systems and applications does each workstation, server, and connectivity device run? How are these programs configured? How is hardware configured? The collection, storage, and assessment of such information belongs to a category of network management known as *configuration management.* Ideally, you would rely on configuration management software to gather and store the information in a database, where those who need it can easily access and analyze the data.

Baseline Measurements

- A baseline is a report of the network's current state of operation.
- Baseline measurements might include the utilization rate for your network backbone, number of users logged on per day or per hour, number of protocols that run on your network, statistics about errors (such as runts, collisions, jabbers, or giants), frequency with which networked applications are used, or information regarding which users take up the most bandwidth.
- Baseline measurements allow you to compare future performance increases or decreases caused by network changes or events with past network performance. Obtaining baseline measurements is the only way to know for certain whether a pattern of usage has changed (and requires attention) or, later, whether a network upgrade made a difference.
- Each network requires its own approach. The elements you measure depend on which functions are most critical to your network and its users.

Figure below shows an example baseline for daily network traffic over a six-week period.



- Suppose that your network currently serves 500 users and that your backbone traffic exceeds 50% at 10:00 a.m. and 2:00 p.m. each business day. That pattern constitutes your baseline. Now suppose that your company decides to add 200 users who perform the same types of functions on the network. The added number of users equals 40% of the current number of users (200/500). Therefore, you can estimate that your backbone's capacity should increase by approximately 40% to maintain your current service levels.

How do you gather baseline data on your network?

- Although you could theoretically use a network monitor or network analyzer and record its output at regular intervals, several software applications can perform the baselining for you.
- These applications range from freeware available on the Internet to expensive, customizable hardware and software combination products.
- Before choosing a network-baselining tool, you should determine how you will use it.
- The baseline measurement tool should also be capable of collecting the statistics needed. For example, only a sophisticated tool can measure traffic generated by each node on a network, filter traffic according to types of protocols and errors, and simultaneously measure statistics from several different network segments.

Policies, procedures, and regulations that make for sound network management.

- Media installation and management—Includes designing the physical layout of a cable or wireless infrastructure, choosing and following best practices for cable management, testing the effectiveness of cable or wireless infrastructure, and documenting cable layouts.
- Network addressing policies—Includes choosing and applying an addressing scheme, determining the use and limits of subnets, integrating an internal network's addressing with an external network's, and configuring gateways for NAT.
- Resource sharing and naming conventions—Includes establishing rules for logon IDs, setting up users and groups and applying access restrictions, designing directory trees and assigning objects, and configuring resource-sharing relationships between domains and servers

- Security-related policies—Includes establishing rules for passwords, limiting access to physical spaces such as the data center, limiting access to shared resources on the network, imposing restrictions on the types of files that are saved to networked computers, monitoring computers for malware, and conducting regular security audits.
- Troubleshooting procedures—Includes following a methodology for troubleshooting network problems and documenting their solutions.
- Backup and disaster recovery procedures—Includes establishing a method and schedule for making backups, regularly testing the effectiveness of backups, assigning a disaster recovery team and defining each member's role, and choosing a disaster recovery strategy and testing it

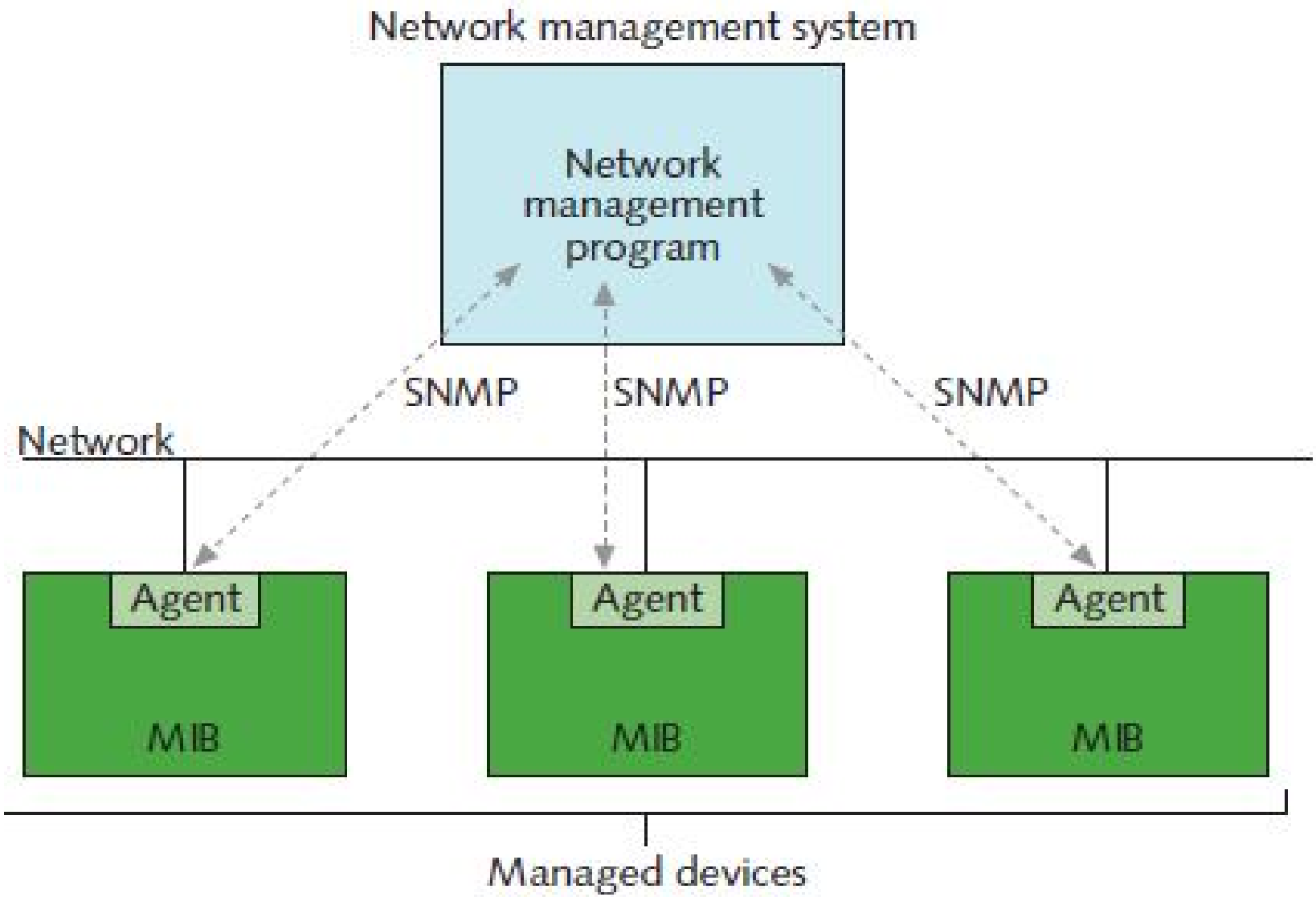
Fault and Performance Management

- Fault management,-Refers to detection and signaling of device, link, or component faults.
- Performance management-Refers to monitoring how well links and devices are keeping up with the demands placed on them.
- To accomplish both fault and performance management, organizations often use enterprise-wide network management software. Some popular applications include IBM's Tivoli NetView and Cisco's CiscoWorks, but hundreds of other such tools exist.
- All rely on a similar architecture, in which at least one network management console (which may be a server or workstation, depending on the size of the network) collects data from multiple networked devices at regular intervals, in a process called polling.
- Each managed device runs a network management agent, a software routine that collects information about the device's operation and provides it to the network management application running on the console.

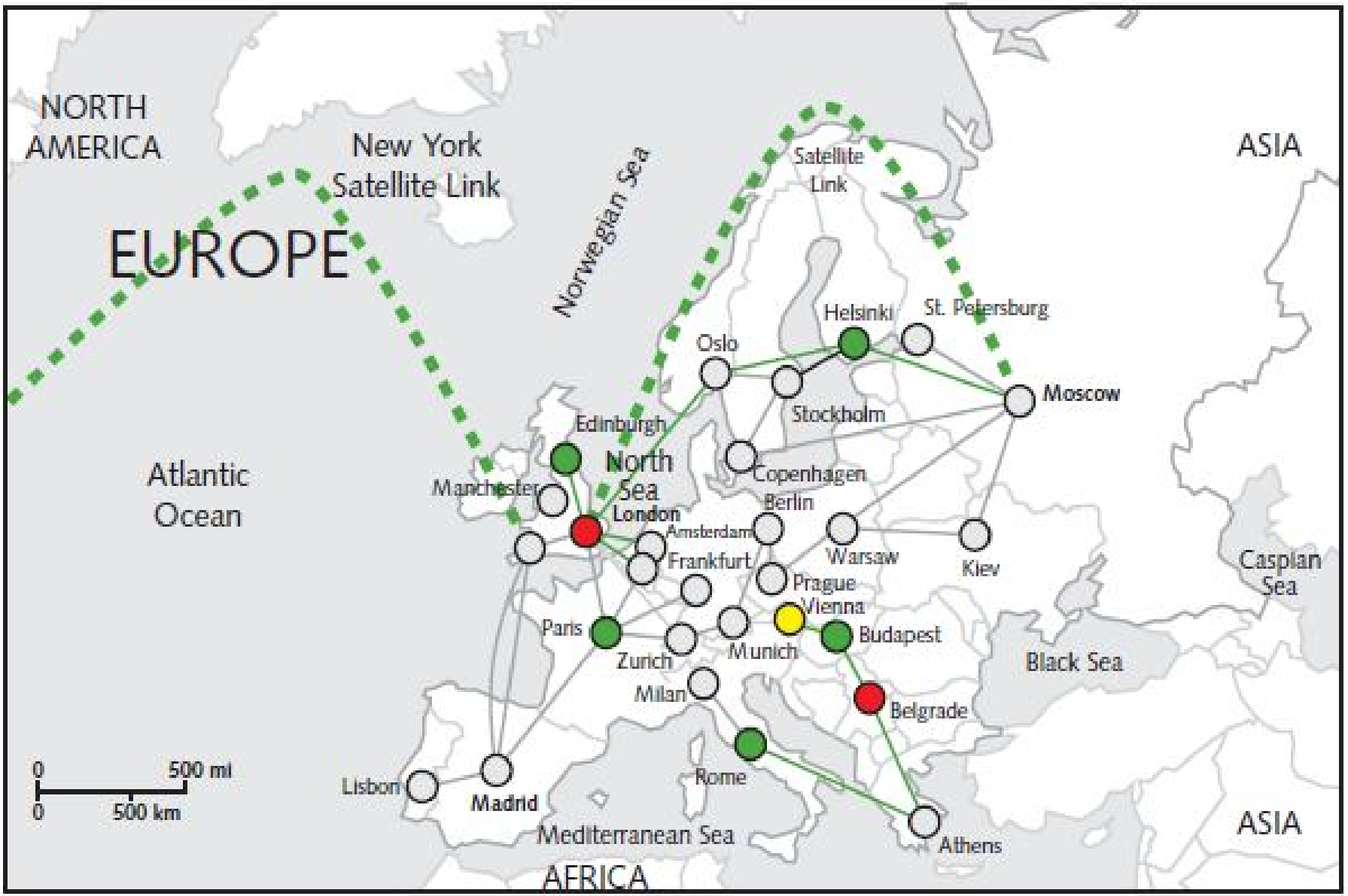
- A managed device may contain several objects that can be managed, including components such as processor, memory, hard disk, NIC, or intangibles such as performance or utilization.
- For example, on a server, an agent can measure how many users are connected to the server or what percentage of the processor's resources are used at any time.
- The definition of managed devices and their data are collected in a **MIB (Management Information Base).**

- Agents communicate information about managed devices via any one of several Application layer protocols. On modern networks, most agents use SNMP (Simple Network Management Protocol). SNMP is part of the TCP/IP suite of protocols and typically runs over UDP on port 161 (though it can be configured to run over TCP).
- After data is collected, the network management application can present an administrator with several ways to view and analyze the data. For example, a popular way to view data is in the form of a map that shows fully functional links or devices in green, partially (or less than optimally) functioning links or devices in yellow, and failed links or devices in red.

Network management architecture



Map showing network status



- Performance and fault management monitoring does not necessarily require a complex application.
- One of the most common network management tools used on WANs is MRTG (Multi Router Traffic Grapher). MRTG is a command-line utility that uses SNMP to poll devices, collects data in a log file, then generates HTML-based views of the data. MRTG is freely distributed software

Asset Management

- Another key component in managing networks is identifying and tracking its hardware and software through asset management.
- The first step in asset management is to take an inventory of each node on the network. This inventory should include the total number of components on the network, and also each device's configuration files, model number, serial number, location on the network, and technical support contact.
- You will also want to keep records of every piece of software purchased by your organization, its version number, vendor, licensing, and technical support contact.
- The asset management tool you choose depends on your organization's needs. You might purchase an application that can automatically discover all devices on the network and then save that information in a database, or you might use a simple spreadsheet to save the data.
- Asset management simplifies maintaining and upgrading the network chiefly because you know what the system includes.
- In addition, asset management provides network administrators with information about the costs and benefits of certain types of hardware or software. For example, if you conclude that 50% of your staff's troubleshooting time is spent on one flawed brand of NIC, an asset management system can reveal how many NICs you would need to replace if you chose to replace those cards, and whether it would make sense to replace the entire installed base.

Change Management

- Technology advances, vendors come and go, and users' needs change. Managing change while maintaining your network's efficiency and availability requires good planning.
- Software Changes-You are most likely to implement the following types of software changes on your network: patches (improvements or enhancements to a particular piece of a software application), upgrades (major changes to the existing code), and revisions (a general term for minor or major changes to the existing code).
- Hardware and Physical Plant Changes-This involves adding or upgrading equipment,Cabling upgrades(you can upgrade in phases),Backbone upgrades

NETWORK PERFORMANCE

- **Network performance metrics**
  - Channel capacity
  - Channel utilization
  - Delay and *jitter*
  - Packet loss and errors

Channel Capacity

- The maximum number of bits that can be transmitted for a unit of time (eg: bits per second)
- Depends on:

  - Bandwidth of the physical medium
    - Cable
    - Electromagnetic waves

  -Processing capacity for each transmission element

  -Efficiency of algorithms in use to access medium

  - Channel encoding and compression

Channel Utilization

- What fraction of the channel capacity is actually in use.
- How is this Important?
  - Future planning
    - What utilization growth rate am I seeing?
    - For when should I plan on buying additional capacity?
    - Where should I invest for my updates?
  - Problem resolution
    - Where are my bottlenecks, etc.

Delay and Jitter

- **Delay**- This is the time required to transmit a packet along its entire path.
- **Jitter-**Jitter is the uneven arrival of packets. For example, imagine a VoIP conversation where packet 1 arrives at a destination router. Then, 20 ms later, packet 2 arrives. After another 70 ms, packet 3 arrives, and then packet 4 arrives 20 ms behind packet 3. This variation in arrival times (that is, variable delay) is not dropping packets, but this jitter might be interpreted by the listener as dropped packets.

Packet Loss and Errors

- Occurs due to the fact that buffers are not infinite in size.

  -When a packet arrives to a buffer that is full the packet is discarded.

  - Packet loss, if it must be corrected, is resolved at higher levels in the network stack (transport or application layers)

  - Loss correction using retransmission of packets can cause yet more congestion if some type of (flow) control is not used (to inform the source that it's pointless to keep sending more packets at the present time)