Net Management Chapter 2

Areas of Network Management

The International Organization for Standardization (ISO) has created a network management model that is useful for placing the undependable scenarios in a more structured framework. As such, five areas of network management are defined:

- *Performance management.* The goal of performance management is to quantify, measure, report, analyze, and control the performance (for instance, utilization and throughput) of different network components. These components include individual devices (for example, links, routers, and hosts) as well as end-to-end abstractions such as a path through the network. We will see shortly that protocol standards such as the Simple Network Management Protocol (SNMP) [RFC 3410] play a central role in Internet performance management.
- *Fault management.* The goal of fault management is to log, detect, and respond to fault conditions in the network. The line between fault management and performance management is rather blurred. We can think of fault management as the immediate handling of transient network failures (for instance, link, host, or router hardware or software outages), while performance management takes the longer-term view of providing acceptable levels of performance in the face of varying traffic demands and occasional network device failures. As with performance management, the SNMP protocol plays a central role in fault management.
- *Configuration management.* Configuration management allows a network manager to track which devices are on the managed network and the hardware and software configurations of these devices. An overview of configuration management and requirements for IP-based networks can be found in [RFC 3139].
- *Accounting management.* Accounting management allows the network manager to specify, log, and control user and device access to network resources. Usage quotas, usage-based charging, and the allocation of resource-access privileges all fall under accounting management.
- *Security management.* The goal of security management is to control access to network resources according to some well-defined policy.

Structure of Computer Network

The universal computer network structure comprises of hosts (computer, terminal, telephone, or any other communicating devices) and a communication subnet (also known as a network node, a subnet, or a transport system). Each host is connected to the communication subnets. The set of network nodes defines the boundary of the network and transfers the data from a **source host** to a **destination host** via transmission media (cable system, satellite, leased telephone lines, cell phones, etc.) over communication channels across the network. The host provides various services to its users, while a subnet provides a communication environment for the transfer of data.

The communication subnet, typically consists of switching systems and transmission links (also known as channels). The transmission links carry the bits from one computer to another through networks. The switching system (high-speed dedicated processing elements with large memory) on the other end is responsible for forwarding the data to its destination over the transmission links. The switching system is connected to the host via a transmission link which carries the data from its source to the system. Transmission links connect various switching elements of subnets and define the topology (physical connection) of the subnet. The subnet defines the three lower layers (physical, data link, and network) of Open System Interconnection-Reference Model (OSI-RM).

The switching system, after receiving data from its source, searches for a free transmission link between it and the switching element which is connected to the destination host. If it finds a free link, it will forward the data on to it; otherwise, it will store the data in its memory and try other route for the data. It will send the data to another switching element, which will again look for a free link until the data is delivered to its destination. The elements of a switching system have been referred to by different names, such as **interface message processor (IMP)**, **packet-switch mode**, **intermediate system**, and **data exchange system.** These elements provide an interface between hosts and communication systems and establish a logic connection between hosts over transmission links. Different operations within communication systems are carried out in dedicated and specialized computers.

Each host is connected to one or more IMPs. All the data originating from a source host first arrives at one of these connected IMPs, from where it is then delivered to the destination host through intermediate IMPs. The IMPs of a network may be connected by lines, cables, satellite links, leased telephone lines, etc. Based on the topology of the subnet, three types of communication services (offered by IMPs to the users) have been defined:

- Point-to-point communication
- Multicast communication
- Broadcast communication

Point-to-point communication

With a point-to-point communication, data from one host is transmitted over either **direct or indirect** links between IMPs (to which these hosts are connected). In a direct link, IMPs are directly connected via a physical communication medium during data transfer. In an indirect link, the data is transferred over intermediate IMPs until it reaches the destination host. Here, the data from an incoming line arrives at the IMP, which stores it and waits for a free link between IMPs. If it finds a free link, the data is sent over it; otherwise, it sends it over intermediate IMPs, and at each intermediate IMP, data is stored and forwarded to the next available IMP. This process is repeated until the data is received by the destination host. In the case of an indirect link, the goal is to always minimize the number of hops between hosts (a hop defines a simple path of length of one between two nodes, two hops defines a simple path of length of two, and so on).

A communication system supporting point-to-point communication is defined as **point-to-point**, **store-and-forward**, or **packet-switched** subnet.

Multicast communication

With a multicast communication, data can be sent to users of a selected group. The usual way of implementing this communication is to set the high-order bit in the address field (of data) to 1. The data will then be delivered to all the users whose high-order bit in the address field is set to 1. There exists only one channel or circuit which can be shared by all connected users' (of the selected group) hosts/IMPs. This type of communication suffers from the problem of **contention**. The problem of contention can be resolved either by using a centralized dedicated processor (which will decide as to which host can send the data next) or by using a distributed system (where each IMP resolves the problem independently). This apparently requires a complex protocol at each IMP.

Broadcast communication

A more general form of multicast communication is broadcast communication, whereby data is delivered to all hosts/IMPs connected to the network. A special code in the address field of the data is used to distinguish between point-to-point and multicasting communications. The data is sent on the network circuit and is received by every host/IMP connected to it. If the address of any connected host/IMP matches the address contained in the data, it can copy the data into its buffer. This type of shared communication typically defines the following network topologies: bus, satellite, radio, and televsion.

Data Communications Basics

Data communications or data networking is the exchange of digital information between computers and other digital devices via telecommunications nodes and wired or wireless links. But in order to have a better appreciation of the evolution of networking services/network management, it is vital to first understand the general computing architectures and traffic types, both of which have changed significantly over time. Thus, it is very crucial to have a good grasp of these basics.

Data Communications or Network Architectures

In a fairly brief history of data networking, a variety of architectures have arisen and each of them has had distinctive impacts on network characteristics. Table 5.1 (Goleniewski, 2006) depicts an essential time line of architectures that have prevailed during different periods.

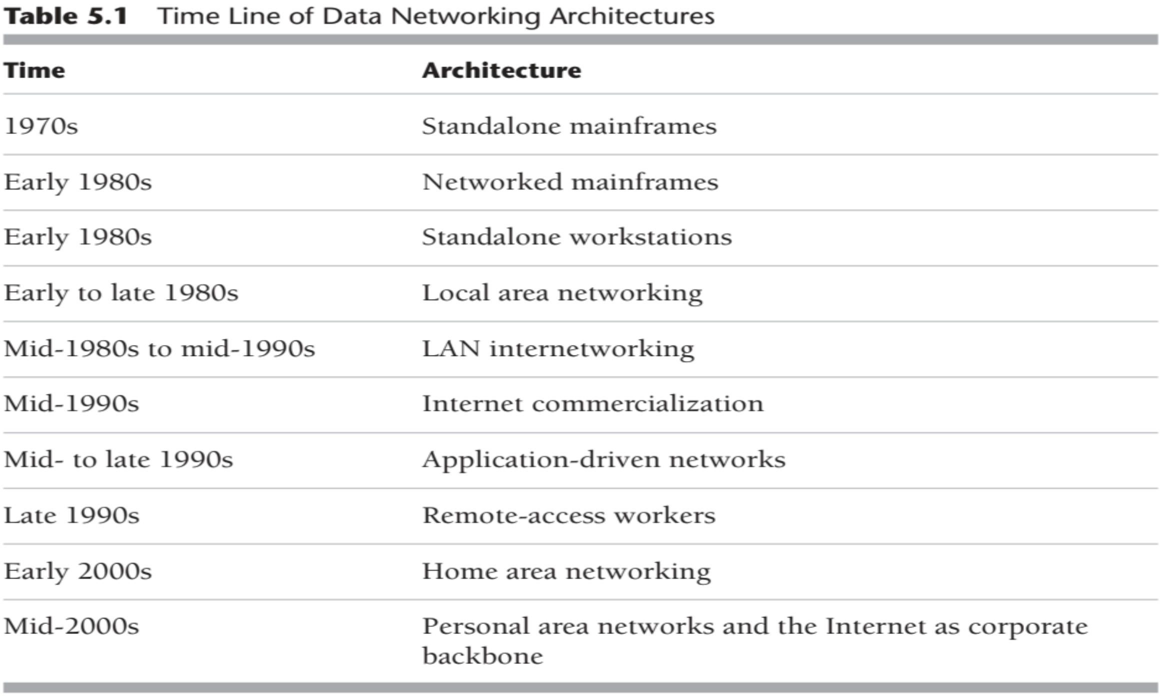


Table 5.1 Time Line of Data Networking Architectures

Time	Architecture
1970s	Standalone mainframes
Early 1980s	Networked mainframes
Early 1980s	Standalone workstations
Early to late 1980s	Local area networking
Mid-1980s to mid-1990s	LAN internetworking
Mid-1990s	Internet commercialization
Mid- to late 1990s	Application-driven networks
Late 1990s	Remote-access workers
Early 2000s	Home area networking
Mid-2000s	Personal area networks and the Internet as corporate backbone

Each architecture has slightly different traffic characteristics plus requirements in terms of security and access control and each has presented a different volume and consistency of traffic to network. So as we will see, each new computing architecture has brought about a demand for new generations of network services.

Standalone Mainframes

The 1970s was the era of standalone mainframes. These networks were very hierarchical in which certain paths needed to be taken. It was an era of terminal-to-host connectivity. At the bottom of the stack were smart terminals. A group of terminals would report to an upper-level manager which is frequently referred to as a cluster controller. The cluster controller was responsible for managing traffic flows in and out of its underlying terminals plus scheduling resources upstream from those terminals. In turn, a number of cluster controllers would be managed by yet another level of managers known as the front-end processors which served as the interface between the underlying communications network and the applications stored in the host.

So during that era, a given terminal could have access only to the host upstream from it. To make use of the applications that resided on another host, a user either required a different terminal or had the pleasure of working with a variety of cables under his desk changing the connection as needed.

Networked Mainframes

A major change took place in the early 1980s. People began networking the mainframes. This was called multidomain networking which enabled one terminal device on a desktop to access numerous hosts that were networked together. Also, in the early 1980s, standalone workstations (WSs) started appearing within the enterprise. This did not usually take place because data-processing department had decided that it would migrate to workstations. Rather, it took place because technically shrewd users began to bring their WSs into the firm plus would then ask data-processing department or management information services (MIS) department to allow connectivity into the corporate resources from WSs which was usually accommodated through dialup modem or X.25.

Local Area Networks (LANs)

As independent WSs started penetrating the corporate environment, people started to study how data was actually being used. They found out that 80% of information used in a business came from within that location while only 20% was exchanged with other locations or other entities. This permitted businesses to be aware that for majority of their communications, they needed networks that had limited geographical span and hence developed the local area network (LAN).

LANs were defined as serving a business address:

- ✓ A particular building or at most a campus environment
- ✓ A shift began to take place in how networks had to accommodate data

In mainframe environment, with its single-to-terminal-to-host communications, traffic volumes were predictable. Traffic levels between a given terminal and its host were known. So it was possible to make some fairly adequate assumptions about the amount of capacity to provision between those two points. However, traffic patterns in the LAN environment were very unpredictable e.g. in a business with 100 PCs on LAN and 50 PCs on another LAN, the level of traffic on each LAN might change throughout the day. Sometimes it was exceedingly high volume, sometimes there was nothing going on and other times, it was steady stream. This unpredictability introduced a requirement for network services that could be flexible in how they addressed bandwidth requirements i.e. services that could introduce bandwidth on demand.

Frame Relay has the capacity to provide more bandwidth than the user subscribes to. But since traffic patterns fluctuate, the overall usage should balance out at the end of the day. Throughout the mid to late 1980s, major design emphasis was on deploying LANs which was to speed up corporate communications to make work more productive plus to reduce costs associated with sharing software and hardware resources.

LAN Internetworking

As LANs were springing up in enterprises all over, it became vital to come up with a tool for internetworking them otherwise, islands of knowledge existed on a particular LAN. But those islands could not communicate with other departments, clusters, or divisions located elsewhere within the enterprise. LAN internetworking therefore took place throughout the late 1980s and early to mid-1990s bringing with it the evolution, introduction and rapid penetration of devices such as: Hubs, bridges, routers and brouters whose purpose is to internet between separate networks.

Internet Commercialization

In the mid-1990s, however, another alternative of data networking came about with the commercialization of the Internet. Before about 1995, the Internet was mainly available to the academic, research plus government communities since it offered a very cost-effective means for data networking chiefly with text-based busty data flows. It held significant appeal for academic and research community.

Nevertheless, until the introduction of the World Wide Web (WWW), the Internet remained largely an academic platform. Intuitive graphical interface and navigational control of the WWW made it of curiosity to those without UNIX skills; that is, anyone with a PC running some version of Windows plus precipitated the demise of just about every other form of Internet communications. Internet was mainly useful for applications such as e-mail, for which there was finally one standard that was open sufficiently to facilitate messaging exchanges between various businesses that deploy different systems.

Application-Driven Networks

The mid to late 1990s began to see the development of advanced bandwidth-hungry applications such as videoconferencing, collaboration, multimedia, and media conferencing. This resulted in another shift in how people thought about deploying networks. During the era of hierarchical networks, decisions about network resources were based on the number of devices and their distance from one another. But when advanced applications –which had a great capacity demands and could not tolerate delays or congestions began to be developed, these applications too also started to dictate the type of network required. Thus, the architecture shifted from being devices driven to being application driven.

Remote-Access Workers

In the late 1990s, following the downsizing of IT departments, both in terms of physical size and cost, it became much easier to deploy IT resources to the worker than to require worker to come to IT resources. Remote access or teleworking became a commonly used personnel approach that had advantages in terms of enhanced employee productivity, better morale, and savings in transportation costs.

Equally, as several large corporations downsized, workers became self-employed plus worked from small offices or home offices. This architecture featuring remote-access workers focused on providing appropriate data networking capabilities to people in their homes, hotels, airports, and in any other place where they might require to access the network. Facilities were designed specifically to authenticate plus authorise remote users and to grant them access to corporate LANs and their underlying resources.

Home Area Networks (HANs)

Individuals are increasingly using their residences as places to carry out professional duties today. As such, they need to network intelligent devices used for work, educational, or leisure activities. Thus, HANs are quickly becoming a new network domain that needs to be addressed since we are now bringing LAN technology into the homes with the likes of Wi-Fi being extremely popular at this time. PAN is a network that serves a single person or small group and is characterised by limited distance, limited throughput and low volume. PANs are deployed to transfer data between a laptop or PDA and a desktop machine or server and a printer. They frequently support virtual docking stations, peripheral sharing and ad hoc infrared links.

A Growing number of machine-to-machine applications are emerging as are applications involving wearables and even implants; their key benefits cannot be realised without PANs. In the case of wearable and implant, PAN exists on or even in the person.

Internet as Corporate Backbone

Another trend just starting to emerge is the disappearance of corporate LAN in some parts of the world where bandwidth is in surplus and cheap, some forward thinking organisations have begun shrinking their LANs and relying on Internet to play the role of the corporate backbone. These companies have migrated many of their applications to web-based service housed in (often outsourced) data centres.

These applications are owned and maintained by the corporation, all access is via Internet-connected Web browser plus is authenticated against a corporate directory server. These organisations no longer face the burden and expense of maintaining complicated corporate networks spreading out with various “extranets” and multilevel demilitarized zones (DMZs). So the rise of high-speed ubiquitous Internet connections, and reliable authentication has finally made such “demilitarization” feasible

Network Hardware

In designing and implementing a network, the following network hardware are required:

Workstations – which are personal computers/microcomputers (desktops, laptops, notebooks, handhelds, etc.) where user reside.

Servers - which are the computers that store network software and shared or private user files.

Switches – which are the collection points for wires that interconnect the workstations.

Routers – which are the connecting devices between local area networks and wide area networks.

Hubs – which are a multiport repeater and can be thought of as being the central point of a star topology network

Nodes – which are computing devices that allow workstation to connect to the network plus make decisions about where to route a piece od data.

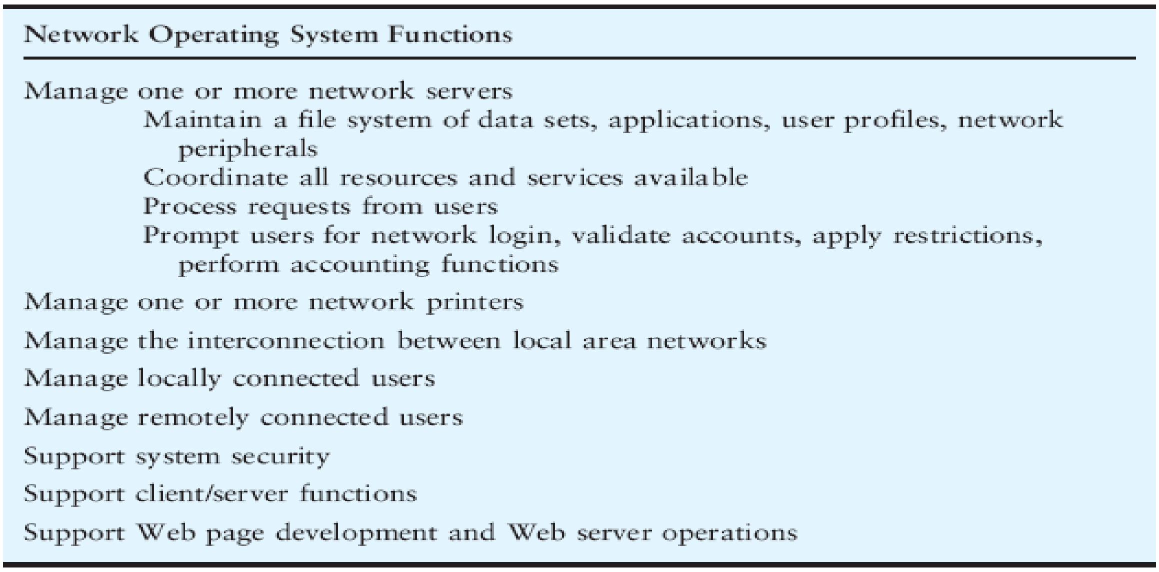
Network interface card (NIC) cards – which are devices that connect workstations or file server to the network and it is where the physical or MAC address is located.

Networking media - this is the media that connects the parts of the network. There are four main types of the media: unshielded twisted-pair cable, shielded twisted-pair cable, coaxial cable and fibre-optic cable.

Network operating systems

A network operating system (NOS) is a large, complex program that can manage the common resources on most local area networks, in addition to carrying out the standard operating system services. Table 8-1 (White, 2013) summarizes the functions of a network operating system. The resources that a network operating system must manage normally include one or more servers, multiple network printers, one or more physical networks, and a potentially large number of users who are directly, and sometimes remotely, connected to the network. Amongst these resources, the server is crucial. The server is typically a high-powered workstation that maintains a large file system of data sets, user profiles, and access information about all the network peripherals.

Table 8-1 Summary of network operating system functions



Network Operating System Functions
Manage one or more network servers
Maintain a file system of data sets, applications, user profiles, network peripherals
Coordinate all resources and services available
Process requests from users
Prompt users for network login, validate accounts, apply restrictions, perform accounting functions
Manage one or more network printers
Manage the interconnection between local area networks
Manage locally connected users
Manage remotely connected users
Support system security
Support client/server functions
Support Web page development and Web server operations

Some examples of networking operating systems include: Novell NetWare**,** windows Server, Linux, UNIX and Mac OS X Server.

Network mapping

Network mapping deals with the study/understanding of networks' physical connectivity while Internet mapping deals with the physical connectivity of the Internet. Network mapping results in the discovery of networked devices and their connectivity. Care needs to be taken not to get confused or mixed up with network discovery which involves discoverying devices on the network and their characteristics such as open ports, listening network services, operating system, etc. Thus, since networks are becoming very complex and dynamic, the automated mapping arena is increasingly becoming crucial.

Organisations and enterprises are increasingly creating maps of their network systems today. These maps can be created manually through the deployment of basic tools such as Microsoft Visio or it could be made effortless by using tools that integrate auto network discovery with Network mapping. There are several of these products being offered by various vendors which can enable individuals to customise plus deploy their personal labels and adding non-discoverable items and background images. Sophisticated mapping can be delpoyed to aid visualise the network plus understand the relationships between end devices and transport layers that offer services required. As such, matters such as bottlenecks and root cause analysis can be easily detected usinig these tools.

The 3 major approaches deployed in network mapping include:

- Simple Network Management Protocol (SNMP) based approaches
- Active probing based approaches
- Route analytics

SNMP based approach retrieves data from router and switch managment information bases (MIBs) in order to construct the network map. The active probing approach is reliant on a string of tracer-route like probe packets which would enable it to build a network map while the route analytics approach depends on information from the routing protocols to construct a network map. It is therefore worth noting that each of these 3 approaches have their strengths as well as their weaknesses.