Network Management

Course Code: CENP3104

Lecturer – Dr. S C Forbacha

Department of Computer Engineering

Level 300

COLTEC

The University of Bamenda

Chapter 1

Introduction

Networks and distributed processing systems are of critical and growing importance within enterprises of all types. The trend is toward larger, more complex networks supporting more applications and more users. As these networks grow in scale, two realities become agonizingly evident:

- The network and its associated resources and distributed applications become indispensable to the organization.
- More things can go wrong, disabling the network or a portion of the network or degrading performance to an unacceptable level.

A large network cannot be put together and managed solely by human effort. The complexity of such a system dictates the use of automated network management tools. The urgency of the need for such tools is growing, and the difficulty of supplying such tools is also increasing especially if the network includes equipment from multiple vendors. Furthermore, the increasing decentralization of network services as demonstrated by the increasing importance of workstations and client/server computing makes coherent and coordinated network management increasingly difficult. In such complex information systems, many major network assets are dispersed far from network management personnel.

So at this juncture, we are well aware that a network comprises of *many* complex, interacting pieces of hardware and software — from the links, switches, routers, hosts, and other devices that include the physical components of the network to the many protocols (in both hardware and software) that control and coordinate these devices. When hundreds or thousands of such components are put together by an organization to create a network, it is not unexpected that components will sporadically malfunction, that network elements will be misconfigured, that network resources will be over-utilized, or that network components will simply “break” (for instance, a cable will be cut or a can of coke will be spilled on top of a router). The network administrator and to some extent the network manager, whose job is to keep the network “up and running,” must be able to respond to (and better yet, avoid) such catastrophes. With potentially thousands of network components spread out over a wide area, the network administrator/manager in a network operations center (NOC) clearly needs tools to help him/her monitor, manage, and control the network.

Therefore, this course provides an overview of network management and as such, looking at the requirements for network management. This should provide you with some idea of the scope of the task to be accomplished. To manage a network, it is essential to know something about the current status and behaviour of that network.

For either LAN management alone, or for a combined LAN/WAN environment, what is required is a network management system that includes a complete set of data gathering and control tools and that is integrated with the network hardware and software. In this light, we will take a look at the general architecture of a network management system and then examine the most widely used standardized software package for supporting network management – that is the Simple Network Management Protocol (SNMP), the protocols, and information base used by a network amanger/ administrator in this task.

Thus in a nutshell, effective network management optimizes a telecommunication network's operational capabilities. The key word here is *optimizes*.

So, some of the implications that can be derived are:

- It keeps the network operating at peak performance
- It informs the operator of impending deterioration
- It provides easy alternative routing and work-arounds when deterioration and/or failure take place
- It provides the tools for pinpointing cause(s) of performance deterioration or failure
- It serves as the front-line command post for network survivability.

There are several secondary functions of network management. They are important but, in our opinion, still secondary. Among these items are:

- It informs in quasi-real time regarding network performance
- It maintains and enforces network security, such as link encryption and issuance and use of passwords
- It gathers and files data on network usage
- It performs a configuration management function
- It also performs an administrative management function

What is Network Management?

Before ploughing deep into network management itself, let us first consider a few illustrative "real-world" non-networking scenarios in which a complex system with many interacting components must be monitored, managed, and controlled by an administrator. Electrical power-generation plants have a control room where dials, gauges, and lights monitor the status (temperature, pressure, flow) of remote valves, pipes, vessels, and other plant components. These devices permit the operator to monitor the plant's numerous components, and may alert the operator (with the famous flashing red warning light) when trouble is coming up. Actions are taken by the plant operator to control these components. In the same way, an airplane cockpit is instrumented to allow a pilot to monitor and control the many components that make up an airplane. In these two examples, the "administrator/manager" *monitors* remote devices and *analyzes* their data to ensure that they are operational and operating within permitted limits (for instance, that the plane is not about to run out of fuel), *reactively controls* the system by making adjustments in response to the changes within the system or its environment, and *proactively manages* the system (for example, by detecting trends or anomalous behaviour, allowing action to be taken before serious problems crop up). In a similar sense, the network manager/administrator will actively monitor, manage, and control the system with which she or he is entrusted.

In the early days of networking, when computer networks were research objects as opposed to a critical infrastructure used by hundreds of millions of people a day, "network management" was unheard of. If one encountered a network problem, one might run a few pings to locate the source of the problem and then modify system settings, reboot hardware or software, or call a remote colleague to do so. Since the public Internet and private intranets have grown from small networks

into a large global infrastructure, the need to manage these huge number of hardware and software components within these networks more systematically has increased in importance as well.

In order to motivate our study of network management, let us start with a simple example. Figure 1.1 depicts a small network consisting of three routers and a number of hosts and servers.

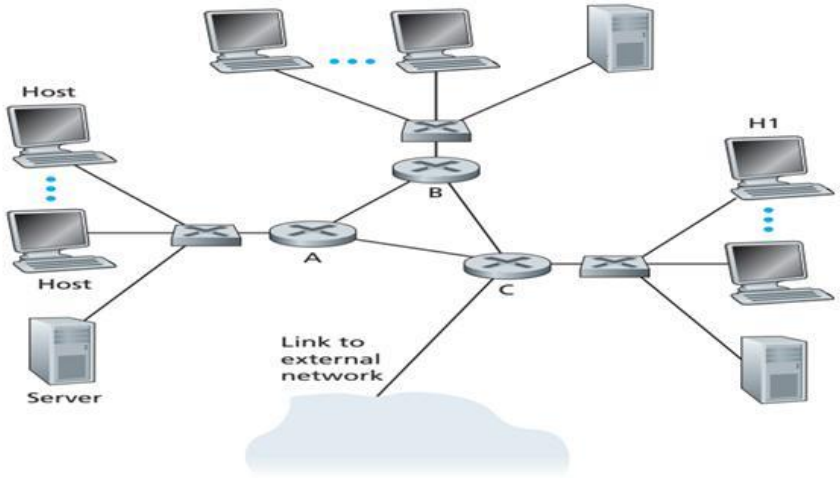


Figure 1.1: A simple scenario demonstrating the uses of network management

Even in such a simple network, there are many scenarios in which a network manager/ administrator might benefit immensely from having appropriate network management tools:

- *Detecting failure of an interface card at a host or a router.* With appropriate network management tools, a network entity (for example, router A) may report to the network manager/administrator that one of its interfaces has gone down. (This is without doubt preferable to a phone call to the NOC from a furious user who says the network connection is down!) A network manager/administrator who actively monitors and analyzes network traffic may be able to *really* impress the would-be furious user by detecting problems in the interface ahead of time and replacing the interface card before it fails. This might be done, for instance, if the manager/administrator noted an increase in checksum errors in frames being sent by the soon-to-die interface.
- *Host monitoring.* Here, the network manager/administrator might at regular intervals check to see if all network hosts are up and operational. Once again, the network manager/ administrator may really be able to impress a network user by proactively responding to a problem (host down) before it is reported by a user.
- *Monitoring traffic to aid in resource deployment.* A network manager/administrator might monitor source-to-destination traffic patterns and notice, for instance, that by switching servers between LAN segments, the amount of traffic that crosses multiple LANs could be significantly decreased. Imagine the happiness all around when better performance is achieved without new equipment costs. Similarly, by monitoring link utilization, a network manager/administrator might determine that a LAN segment or the external link to the outside world is overloaded and that a higher-bandwidth link should thus be provisioned (sadly, at an increased cost). The network manager/administrator might also want to be notified automatically when congestion levels on a link exceed a given threshold value, in order to provision a higher-bandwidth link before congestion becomes serious.
- *Detecting rapid changes in routing tables.* Route flickering - frequent changes in the routing tables - may indicate instabilities in the routing or a misconfigured router. Surely, the

network manager/administrator who has improperly configured a router would prefer to discover the error himself or herself, before the network goes down.

- *Monitoring for SLAs.* **Service Level Agreements (SLAs)** are contracts that define specific performance metrics and acceptable levels of network-provider performance with respect to these metrics to their customers. These SLAs include service availability (outage), latency, throughput, and outage notification requirements. Clearly, if performance criteria are to be part of a service agreement between a network provider and its users, then measuring and managing performance will be of great importance to the network manager/administrator.
- *Intrusion detection.* A network manager/administrator may want to be notified when network traffic arrives from, or is destined for, a suspicious source (for instance, host or port number). Similarly, a network manager/administrator may want to detect (and in many cases filter) the existence of certain types of traffic (for instance, sourcerouted packets, or a large number of SYN packets directed to a given host).

Network Management in the Early Days

The job of the network manager in the early days of the network management was mostly a local one. This was possible because connectivity of interest was mostly local, networks were not large and there were not that many networks. The network manager was predominantly concerned with attaching PCs, workstations, and a server to a LAN using Network Interface Card (NIC), installing and configuring operating systems on PCs, workstations and servers, installing protocol stacks, configuring NIC I/O addresses, Direct Memory Access (DMA) addresses and interrupts so as not to conflict with other NIC selections and configuring protocol stacks. The Ping application was usually deployed to ensure that all devices on the network could communicate with one another. Ping sends a message to a device identified by its IP address and waits for a reply from the device.

To control access to information on a network server, the manager might write a script for the server that would be executed when the user at the PC or workstation logged on. The script would provide a uniform view to all users and only provide access to drives, folders or files that the user or group of users needed. The manager would carry out coordination activities for the PCs and workstations. He/she would also install a print server application on the server or a standalone print server PC to manage print jobs from each of the PCs and workstations. After all, sharing a printer was one of the main purposes of networks in the first place.

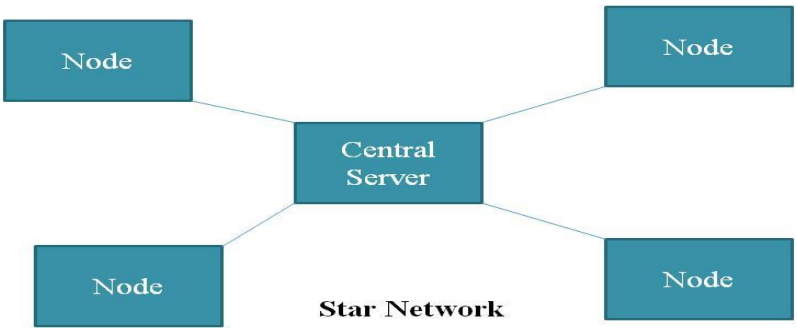
If the network was to be divided into segments or subnets, say one for each department in the organisation, a bridge or router, respectively, would be used to connect them. If a subnet, the manager would configure a router table to enable connectivity according to network address, subnet address and subnet mask. Connectivity to remote networks required more router configuration and installation and maintenance of Wide Area Network (WAN) interfaces but this was not often required.

Next, it was necessary to install user applications on PCs and workstations and to ensure that they were interfacing correctly with the operating system. Then, application support programs (APIs) appeared on the scene to support easy access to the protocol stack and thereby the server. Sometimes such support programs were an integral part of the protocol stack and sometimes not. Given all of these duties, it was still possible for the network manager to accomplish them in a timely manner since the number of devices to be managed was small by today's standards.

Physical and logical topologies

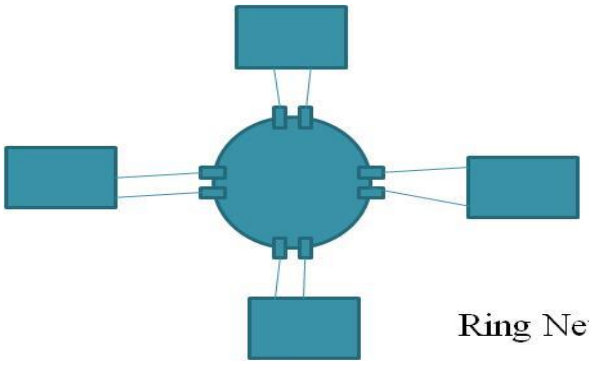
Topology is the physical and logical geometry governing the placement of nodes on a network while network topology is the physical arrangement of network nodes and media within an enterprise networking structure. Thus, the physical topology/design refers to the pattern formed by the locations of the elements of the network, as it would come into view if drawn on a sheet of paper while the logical determines how the data moves around the network from workstation to workstation. However, there are three basic topologies for LANs which are:

➢ **Star Network:** this type of network uses a central server to route data between clients or hosts



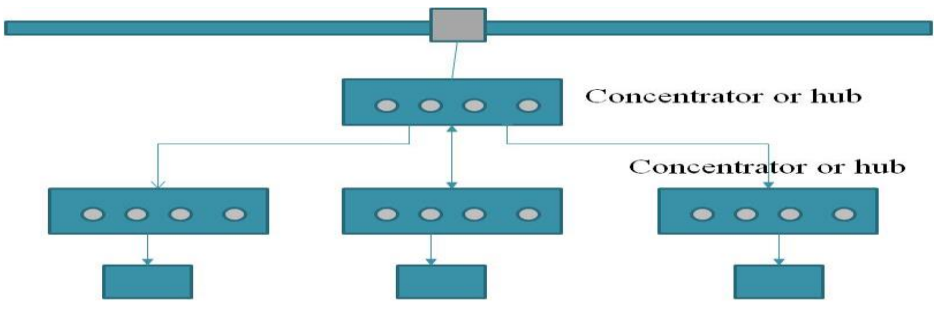
Star Network

Ring Network: It uses a ring in which data is passed from node to node, either in clockwise or anti-clockwise direction. Generally, a token is passed from node to node and a node can only transmit when it gets the token.



Ring Network

Bus Network: with this type of network, all nodes on a network segment connect to the same physical cable. Nodes must therefore contend to get access to the network. There are other topologies which are either a combination of two or more basic topologies or are derivatives of the main types. So a typical topology is a tree topology which is essentially a combined star and bus network.



Tree Topology

Star Network

With star topology, a central server (or switching hub) switches data around the network. Traffic between nodes and server will be relatively slow.

Major advantages of star topology:

➢ Since data is relatively slow between central server and nodes, low specification twisted-pair cables can be used to connect nodes to the server

➢ Fault on one of the nodes will not affect the rest of the network

➢ Typically, mainframe computers use a central server with terminals connected to it

Main disadvantages of star topology:

➢ It is highly dependent upon the operation of the server

➢ So if the server is non-operational, then the entire network could be shut down.

Therefore Ethernet hub functions as a multiport repeater (or concentrator). They are either active or passive. An active hub connects to the network media and equally regenerates signals while a passive hub simply connects devices onto networking media.

Ring Network

Computers link together to form a ring. In order to foster an orderly access to the ring, a single electronic token passes from one computer to the next around the ring. A computer can only transmit data when it captures a token. Each link between the nodes is a point-to-point link which permits the usage of any type of transmission medium. Typically, twisted-pair cables allow a bit rate of up to 16Mbps but coaxial and fibre-optic cables are generally used for extra reliability and higher data rates. A classic ring network is the IBM Token Ring.

The main advantage of a token ring network is that all nodes have an equal chance of transmitting data but unfortunately, it suffers from several problems: the most severe is that if one of the nodes goes down, then the entire network may go down **since it is not able to pass the token onto the next node.**

Bus Network

Bus network uses a multi-drop transmission medium in which all nodes on the network share a common bus and thus share communications. This permits only one device to communicate at a time. As such a distributed medium access protocol is used to determine which station is to transmit. As with ring network, data frames contain source and destination addresses in which each station monitors the bus and copies frames addressed to itself. Twisted-pair cables give data rates of up to 100Mbps whereas coaxial and fibre-optic cables give higher bit rates and longer transmission distances (Buchanan 2000). Bus network is a good compromise over the other two topologies as it allows relatively higher data rates. Again, if a node goes down, it does not normally affect the rest of the network.

Major disadvantage:

- It requires a network protocol to detect when two nodes are transmitting at the same time

- It does not cope well with heavy traffic rates
- Bus networks need a termination at either end of the bus since signals require to be absorbed at the end of the bus (else it would bounce off the end of the open-circuited bus). This prevents signal from bouncing back and being received again by workstations attached to the bus

Ring and star networks do not require termination since they are automatically terminated. With star network connected, nodes automatically terminate the end of the connection. All computers have access to a common bus at the same time

Token Ring

Token ring returns were developed by several manufacturers. The most prevalent being that of the IBM Token Ring. Unlike Ethernet, they cope well with high network traffic loadings and were at one time very popular but Ethernet has since overtaken their popularity. Token Ring networks have suffered from management problems in the past and poor network tolerance.

Token Ring Operation

A Token Ring network circulates an electronic token (named control token) around a closed loop. Each node on the network reads the token and repeats it to the next node. The control token circulates around the ring even when there is no data being transmitted. Nodes on a Token Ring network intending to transmit must await a token. When they get it, the fill the frame with data and add the source and destination addresses and then send it to the next node.
This data frame then circulates around the ring until it reaches its destination node. It reads data into its local memory area (buffer) and marks an acknowledgement on the data frame which then circulates back to the source node. When it receives the frame, it tests it to determine whether it contains an acknowledgement. If it does, then the source node knows that the data frame has been received correctly else the node is not responding. And if source node has finished transmitting data, it then transmits a new token which can be used by other nodes on the ring. No nodes are allowed to transmit data unless they have received a valid control token. A distributed control protocol determines the sequence in which nodes transmit. This gives each node equal access to the ring as each node is only allowed to send one data frame. It must then give up the token to the next node and wait for the token to return before it can transmit another data frame.

Token Ring Maintenance

The Token Ring system requires a lot of maintenance – so it must perform the following functions:
Ring Initialization: when the network is started or after it is broken, it must be re-initialized. A co-operative decentralised algorithm sorts out which node starts a new token, which goes next and so on.
Adding to the Ring: if a new node is to be physically connected to the ring, then the network must be shutdown and re-initialised.
Deletion from the ring: a node can disconnect itself from the ring by joining together its predecessor or its successor. Again, the network may have to be shutdown and re-initialised.
Fault management: a typically Token Ring errors occur when two nodes think it is their turn to transmit or the ring is broken as no node thinks that it is their turn

Token Ring Multi-station Access Units (MAUs)

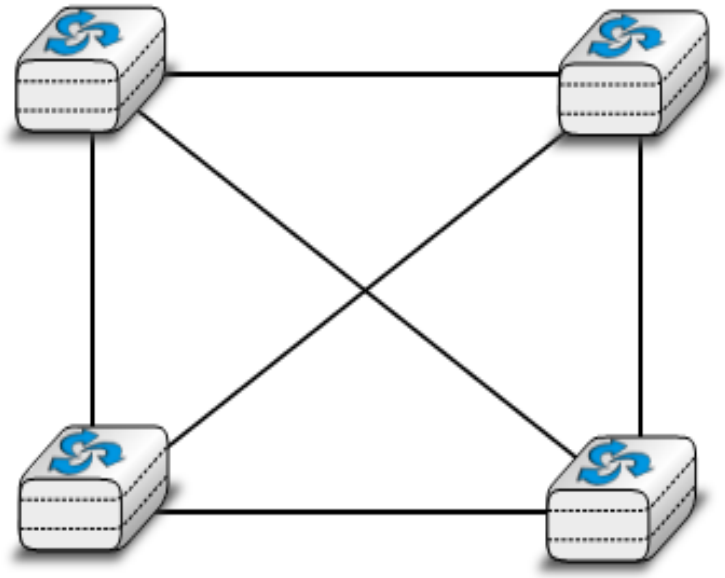
The problems of adding and deleting nodes to or from a ring network are significantly reduced with a multi-station access unit (MAU). Generally, a MAU allows nodes to be switched in and out of a network using a changeover switch or by automatic electronic switching (known as auto-loopback). This has the advantage of not switching down the network when nodes are added and deleted or when they develop faults.

Full Mesh

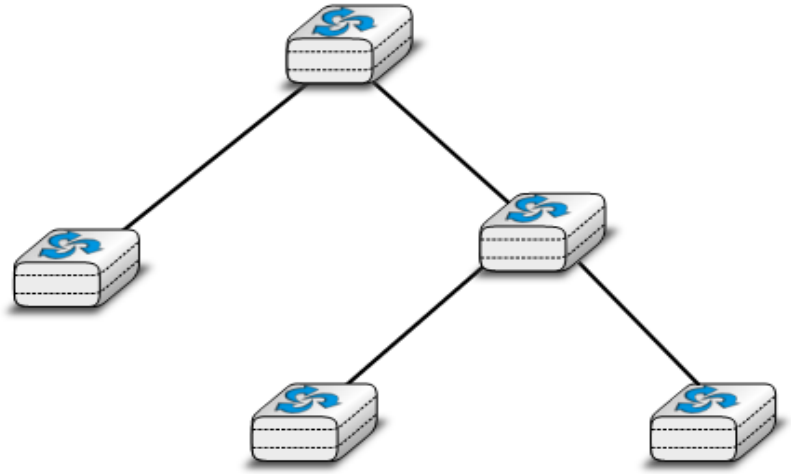
Another possible physical organisation is the mesh. To allow any host to send messages to any other host in the network, the easiest solution is to organise them as a full-mesh, with a direct and dedicated link between each pair of hosts. Such a physical topology is sometimes used, especially when high performance and high redundancy is required for a small number of hosts.

However, it has two major drawbacks:

- For a network containing *n* hosts, each host must have *n-1* physical interfaces. In practice, the number of physical interfaces on a node will limit the size of a full-mesh network that can be built
- For a network containing *n* hosts, $n \times (n-1)/2$ links are required. This is possible when there are a few nodes in the same room, but rarely when they are located several kilometers apart



Another physical organisation of a network is the tree. Such networks are typically used when a large number of customers must be connected in a very cost-effective manner. Cable TV networks are often organised as trees.



In practice, most real networks combine part of these topologies. For example, a campus network can be organised as a ring between the key buildings, while smaller buildings are attached as a tree or a star to important buildings. Or an ISP network may have a full mesh of devices in the core of its network, and trees to connect remote users as depicted in Figure 2.8 (Bonaventure, 2012).

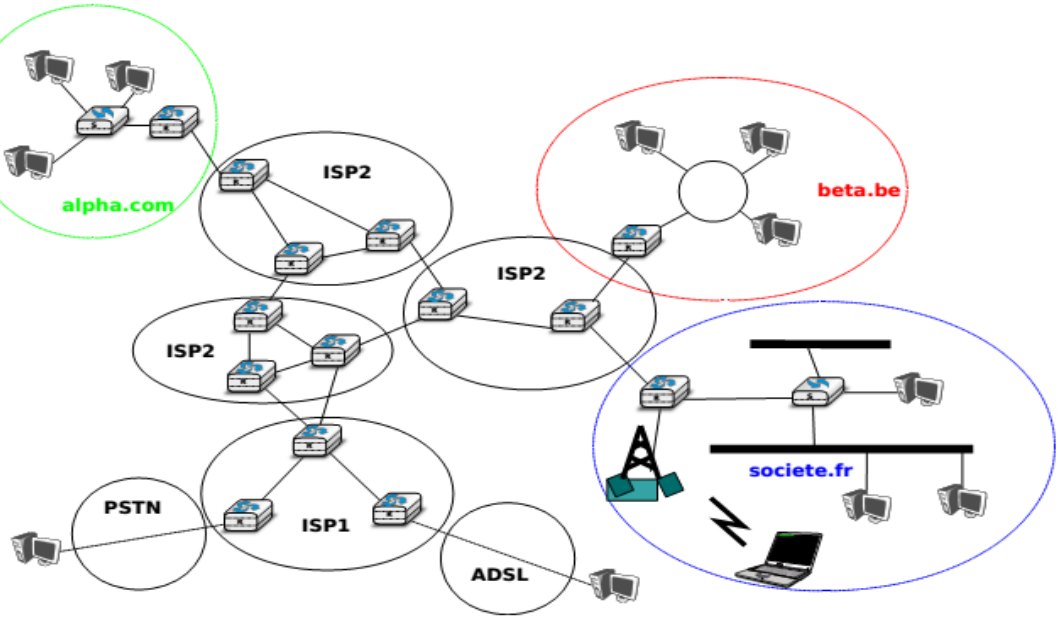


Figure 2.8: A simple internetwork

Advantages of Tree Topology

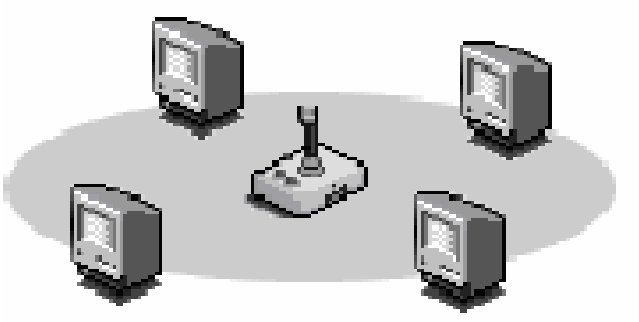
- Installation and configuration of network is easy.
- Less expensive when compared to mesh topology.
- Faults in the network can be detected traced.
- The addition of the secondary hub allows more devices to be attached to the central hub.
- Supports multiple cable types like shielded twisted pair cable, unshielded twisted pair cable, ordinary telephone cable etc.

Disadvantages of Tree Topology

- Failure in the central hub brings the entire network to a halt.
- More cabling is required when compared to bus topology because each node is connected to the central hub.

Cellular Topology

Cellular topology, divides the area being serviced into cells. In wireless media each point transmits in a certain geographical area called a cell, each cell represents a portion of the total network area. Figure below shows computers using Cellular Topology.



Devices that are present within the cell, communicate through a central hub. Hubs in different cells are interconnected and hubs are responsible for routing data across the network. They provide a complete network infrastructure.

Cellular topology is applicable only in case of wireless media that does not require cable connection.

Advantages of Cellular Topology

- If the hubs maintain a point-to-point link with devices, trouble shooting is easy.
- Hub-to-hub fault tracking is more complicated, but allows simple fault isolation.

Disadvantages of Cellular Topology

- When a hub fails, all devices serviced by the hub lose service (are affected).

Network protocols and standards

Starting with simple e-mail to the complexities of the web, several networks have deployed numerous network protocols and standards over the years to exchange data between two or more nodes. Many services are available on the Internet

- What enables these varied services to work?
- What enables the Internet itself to work?

The response to all these questions is Internet protocols

Despite the fact that the operation of the Internet relies on many protocols, several stand out as the most commonly used: the Internet Protocol (IP), Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), Address Recognition Protocol (ARP), and

Network Address Translation (NAT) which are but a few to be stated. We are not going to look at each of them in details.

Internet Protocol (IP) provides a connectionless data transfer service over heterogeneous networks by passing and routing IP datagrams or data packets. There are two versions – IP version 4 (IPv4) and version 6 (IPv6). Perhaps one of the most common examples of a transport layer protocol is the other half of the popular TCP/IP protocol. The principal function of the **Transmission Control Protocol (TCP)** is to turn an unreliable network (such as the one created by IP) into a reliable network that is free from lost and duplicate packets. Thus, TCP essentially fills in some holes created by IP. The **Internet Control Message Protocol (ICMP)**, which is used by routers and nodes, carries out error reporting for the Internet Protocol since IP does not report these errors.
User Datagram Protocol (UDP) is a transport protocol that does not establish connections plus does not attempt to keep data packets in sequence, and does not watch for datagrams that have existed for too long. The Address Resolution Protocol is another small but essential protocol that is used to support TCP/IP networks. The **Address Resolution Protocol (ARP)** takes an IP address in an IP datagram and translates it into the appropriate medium access control layer address for delivery on a local area network since every workstation having a connection to the Internet is assigned an IP address. This IP address is what a packet deploys to find its way to its intended destination.

The most popular protocol that deals with dynamic assignment is the **Dynamic Host Configuration Protocol (DHCP)**. When a workstation running the DHCP client software needs to connect to the Internet, the protocol issues an IP request, which prompts the DHCP server to look in a static table of IP addresses. If this particular workstation has an entry, then that IP address is assigned to that workstation. But if there is no entry in the static table, the DHCP server selects an IP address from an available pool of addresses and assigns it to that workstation. Another protocol that is used to assign IP addresses is **Network Address Translation (NAT)**. NAT allows a router represent an entire local area network to the Internet as a single IP address. When a user workstation on a company local area network sends a packet out to the Internet, NAT replaces the IP address of the user workstation with a corporate global IP address. Thus, all packets that leave the corporate network contain this global IP address. As such, the only IP address that anyone sees outside of the corporate network is the one global IP address.

Standards

It has long been accepted in the telecommunications industry that standards are essential to govern the physical, electrical, and procedural characteristics of communication equipment. In the past, this view has not been embraced by the computer industry. Whereas communication equipment vendors recognize that their equipment will usually interface to and communicate with other vendors' equipment, computer vendors have conventionally attempted to monopolize their customers.

However, the proliferation of computers and distributed processing has made that an unsustainable position. Computers from different vendors must communicate with each other and, with the ongoing evolution of protocol standards, customers will no longer accept special-purpose protocol conversion software development. There are a number of advantages and disadvantages to the standards-making process. We list here the most striking ones. The principal advantages of standards are as follows as noted by Stallings (2007):

- A standard assures that there will be a large market for a particular piece of equipment or software. This encourages mass production and, in some cases, the use of large-scale-integration (LSI) or very-large-scale-integration (VLSI) techniques, resulting in lower costs.
- A standard allows products from multiple vendors to communicate, giving the purchaser more flexibility in equipment selection and use.

The principal disadvantages are as follows:

- A standard tends to freeze the technology. By the time a standard is developed, subjected to review and compromise, and promulgated, more efficient techniques are possible.
- There are multiple standards for the same thing. This is not a disadvantage of standards per se, but of the current way things are done. Fortunately, in recent years the various standards-making organizations have begun to cooperate more closely. Nevertheless, there are still areas where multiple conflicting standards exist.

Different organizations have been involved in the development or promotion of these standards. The following are the most important (in the current context) of these organizations:

• **Internet Society**: The Internet SOCiety (ISOC) is a professional membership society with more than 150 organizational and 6000 individual members in over 100 countries. It provides leadership in addressing issues that confront the future of the Internet and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). All of the RFCs and Internet standards are developed through these organizations.

• **IEEE 802**: The IEEE (Institute of Electrical and Electronics Engineers) 802 LAN/MAN Standards Committee develops local area network standards and metropolitan area network standards. The most widely used standards are for the Ethernet family, wireless LAN, bridging, and virtual bridged LANs. An individual working group provides the focus for each area.

• **ITU-T**: The International Telecommunication Union (ITU) is an international organization within the United Nations System where governments and the private sector coordinate global telecom networks and services. The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors of the ITU. ITU-T's mission is the production of standards covering all fields of telecommunications.

• **ATM Forum**: The ATM Forum is an international non-profit organization formed with the objective of accelerating the use of ATM (asynchronous transfer mode) products and services through a rapid convergence of interoperability specifications. In addition, the Forum promotes industry cooperation and awareness.

• **ISO**: The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from more than 140 countries, one from each country. ISO is a nongovernmental organization that promotes the development of standardization and related activities with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity. ISO's work results in international agreements that are published as International Standards.