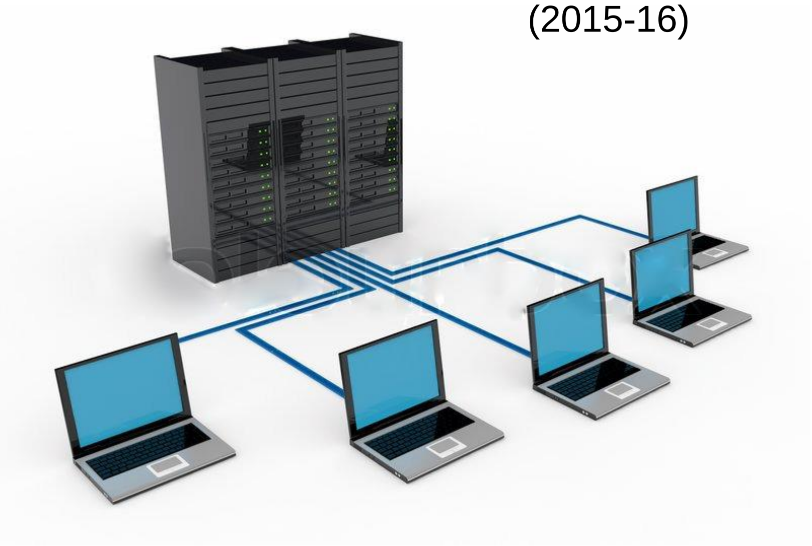
Oil & Natural Gas Corporation Ltd.

KDMIPE, 9 Kaulagarh Road, Dehradun – 248003.

Project Report on

Computer Networks

(2015-16)



Submitted By:

Amitabh Yadav
University Of Petroleum & Energy Studies,
Dehradun.

Sachin Kumar
Netaji Subhash Institute of Technology,
New Delhi.

Rishabh Kishore
Dehradun Institute of Technology,
Dehradun.

CERTIFICATE

I hereby admit that the project undertaken by me, entitled as **“COMPUTER NETWORKING”** in the partial fulfillment of the requirement of the award of certificate of summer training, submitted to the department of **GEODATA PROCESSING AND INTERPRETATION CENTER (GEOPIC), ONGC, DEHRADUN** is an authentic record of own work carried out under supervision.

This is to certify that the above statement made by the candidate is correct to the best of my knowledge. I wish him all the best for his life.

Amitabh Yadav
(8.6.2015 – 8.7.2015)

Mr. A. K. Dohare
S.E. (E&T)

Rishabh Kishore
(4.6.2015 – 4.7.2015)

Sachin Kumar
(16.6.2015 – 16.7.2015)

ACKNOWLEDGEMENTS

I am highly grateful to Shri D. Bhaumik, GM(E&T) CS(H/W) GEOPIC, ONGC DEHRADUN, for providing me the opportunity to work on this project.

With pleasure, I express my gratefulness to Mr. A. K. Dohare S.E. (E&T) CS(H/W) Division for his valuable and sustained guidance and careful supervision during the project.

I am immensely thankful to Mr. N. P. Mohanta DGM(E&T) Summer Training Co-coordinator, CS Hardware, GEOPIC, ONGC DEHRADUN for providing and arranging the required facilities.

I am also thankful to Dr. Sanjay Bhutani DGM(Chem), Summer Training Coordinator, ONGC Academy.

I express my sincere thanks to all the members of GEOPIC who have helped me directly or indirectly. Without their help and guidance I would not have been able to successfully complete the project.

Amitabh Yadav

Sachin Kumar

Rishabh Kishore

CONTENTS

ABOUT ONGC

Oil and Natural Gas Corporation Limited (**ONGC**) is an Indian multinational oil and gas company headquartered in Dehradun, India. It is a Public Sector Undertaking (PSU) of the Government of India, under the administrative control of the Ministry of Petroleum and Natural Gas. It is India's largest oil and gas exploration and production company. It produces around 69% of India's crude oil (equivalent to around 30% of the country's total demand) and around 62% of its natural gas.

On 31 March 2013, its market capitalization was INR 2.6 trillion (US$48.98 billion), making it India's second largest publicly traded company. In a government survey for FY 2011-12, it was ranked as the largest profit making PSU in India. ONGC has been ranked 357th in the Fortune Global 500 list of the world's biggest corporations for the year 2012. It is ranked 22nd among the Top 250 Global Energy Companies by Platts.

ONGC was founded on 14 August 1956 by Government of India, which currently holds a 68.94% equity stake. It is involved in exploring for and exploiting hydrocarbons in 26 sedimentary basins of India, and owns and operates over 11,000 kilometers of pipelines in the country. Its international subsidiary ONGC Videsh currently has projects in 15 countries. ONGC has discovered 6 of the 7 commercially producing Indian Basins, in the last 50 years, adding over 7.1 billion tonnes of In-place Oil & Gas volume of hydrocarbons in Indian basins. Against a global decline of production from matured fields, ONGC has maintained production from its brownfields like Mumbai High, with the help of aggressive investments in various IOR (Improved Oil Recovery) and EOR (Enhanced Oil Recovery) schemes. ONGC has many matured fields with a current recovery factor of 25-33%. Its Reserve Replacement Ratio for between 2005 and 2013, has been more than one. During FY 2012-13, ONGC had to share the highest ever under-recovery of INR 494.2 million (an increase of INR 49.6 million over the previous financial year) towards the under-recoveries of Oil Marketing Companies (IOC, BPCL and HPCL).

History

Foundation to 1961

Before the independence of India, the Assam Oil Company in the north-eastern and Attock Oil company in north-western part of the undivided India were the only oil producing companies, with minimal exploration input. The major part of Indian sedimentary basins was deemed to be unfit for development of oil and gas resources.

After independence, the Central Government of India realized the importance of oil and gas for rapid industrial development and its strategic role in defense. Consequently, while framing the Industrial Policy Statement of 1948, the development of petroleum industry in the country was considered to be of utmost necessity.

Until 1955, private oil companies mainly carried out exploration of hydrocarbon resources of India. In Assam, the Assam Oil Company was producing oil at Digboi (discovered in 1889) and Oil India Ltd. (a 50% joint venture between Government of India and Burmah Oil Company) was engaged in developing two newly discovered large fields Naharkatiya and Moraan in Assam. In West Bengal, the Indo-Stanvac Petroleum project (a joint venture between Government of India and Standard Vacuum Oil Company of USA) was engaged in exploration work. The vast sedimentary tract in other parts of India and adjoining offshore remained largely unexplored.

In 1955, Government of India decided to develop the oil and natural gas resources in the various regions of the country as part of the Public Sector development. With this objective, an Oil and Natural Gas Directorate was set up towards the end of 1955, as a subordinate office under the then Ministry of Natural Resources and Scientific Research. The department was constituted with a nucleus of geoscientists from the Geological Survey of India.

A delegation under the leadership of the Minister of Natural Resources visited several European countries to study the status of oil industry in those countries and to facilitate the training of Indian professionals for exploring potential oil and gas reserves. Experts from Romania, the Soviet Union, the United States and West Germany subsequently visited India and helped the government with their expertise. Soviet experts later drew up a detailed plan for geological and geophysical surveys and drilling operations to be carried out in the 2nd Five Year Plan (1956-61).

In April 1956, the Government of India adopted the Industrial Policy Resolution, which placed Mineral Oil Industry among the schedule 'A' industries, the future development of which was to be the sole and exclusive responsibility of the state.

Soon, after the formation of the Oil and Natural Gas Directorate, it became apparent that it would not be possible for the Directorate with its limited financial and administrative powers as subordinate office of the Government, to function efficiently. So in August, 1956, the Directorate was raised to the status of a commission with enhanced powers, although it continued to be under the government. In October 1959, the Commission was converted into a statutory body by an act of the Indian Parliament, which enhanced powers of the commission further. The main functions of the Oil and Natural Gas Commission subject to the provisions of the Act, were "to plan, promote, organize and implement programs for development of Petroleum Resources and the production and sale of petroleum and petroleum products produced by it, and to perform such other functions as the Central Government may, from time to time, assign to it ". The act further outlined the activities and steps to be taken by ONGC in fulfilling its mandate.

1961 to 2000

Since its inception, ONGC has been instrumental in transforming the country's limited upstream sector into a large viable playing field, with its activities spread throughout India and significantly in overseas territories. In the inland areas, ONGC not only found new resources in Assam but also established new oil province in Cambay basin (Gujarat), while adding new petroliferous areas in the Assam-Arakan Fold Belt and East coast basins (both onshore and offshore). ONGC went offshore in early 70's and discovered a giant oil field in the form of Bombay High, now known as Mumbai High. This discovery, along with subsequent discoveries of huge oil and gas fields in Western offshore changed the oil scenario of the country. Subsequently, over 5 billion tonnes of hydrocarbons, which were present in the country, were discovered. The most important contribution of ONGC, however, is its self-reliance and development of core competence in E&P activities at a globally competitive level.

ONGC became a publicly held company in February 1994, with 20% of its equity were sold to the public and eighty percent retained by the Indian government. At the time, ONGC employed 48,000 people and had reserves and surpluses worth ₹104.34 billion, in addition to its intangible assets. The corporation's net worth of ₹107.77 billion was the largest of any Indian company.

In 1958 the then Chairman, Keshav Dev Malaviya, held a meeting with some geologists in the Mussoorie office of the Geology Directorate where he accepted the need for ONGC to go outside India too in order to enhance Indian owned capacity for oil production. The argument in support for this step, by LP Mathur and BS Negi, was that Indian demand for crude would go up at a faster rate than discoveries by ONGC in India.

Malaviya followed this up by making ONGC apply for exploration licences in the Persian Gulf. Iran gave ONGC four blocks and Malaviya visited Milan and Bartlseville to request ENI and Phillips Petroleum to join as partners in the Iran venture. This resulted in the discovery of the Rostum oilfield in the early 'sixties, very soon after the discovery of Ankleswar in Gujarat. This was the very first investment by the Indian public sector in foreign countries and oil from Rostum and Raksh was brought to Cochin where it was refined in a refinery built with technical assistance from Phillips.

2000 to present

In 2003, ONGC Videsh Limited (OVL), the division of ONGC concerned with its foreign assets, acquired Talisman Energy's 25% stake in the Greater Nile Oil project.

In 2006, a commemorative coin set was issued to mark the 50th anniversary of the founding of ONGC, making it only the second Indian company (State Bank of India being the first) to have such a coin issued in its honor.

In 2011, ONGC applied to purchase 2000 acres of land at Dahanu to process offshore gas. ONGC Videsh, along with Statoil ASA (Norway) and Repsol SA (Spain), has been engaged in deep-water drilling off the northern coast of Cuba in 2012. On 11 August 2012, ONGC announced that it had made a large oil discovery in the D1 oilfield off the west coast of India, which will help it to raise the output of the field from around 12,500 barrels per day (bpd) to a peak output of 60,000 bpd.

In November 2012, OVL agreed to acquire ConocoPhillips' 8.4% stake in the Kashagan oilfield in Kazakhstan for around US$5 billion, in ONGC's largest acquisition to date. The acquisition is subject to the approval of the governments of Kazakhstan and India and also to other partners in the Caspian Sea field waiving their pre-emption rights.

In January 2014, OVL and Oil India completed the acquisition of Videocon Group’s ten percent stake in a Mozambican gas field for a total of $2.47 billion.

In June 2015, Oil and Natural Gas Corporation (ONGC) given a Rs27bn ($427m) offshore contract for the Bassein development project to Larsen & Toubro (L&T).

GEOPIC

Geodata Processing & Interpretation Center (GEOPIC)
ONGC, Dehradun.

INTRODUCTION

Each of the past three centuries was dominated by a single new technology. The 18th century was the era of the great mechanical systems accompanying the Industrial Revolution. The 19th century was the age of the steam engine. During the 20th century, the key technology was information gathering, processing, and distribution. It was the same time that computer first came into picture. Among other developments, we saw the installation of worldwide telephone networks, the invention of radio and television, the birth and unprecedented growth of the computer industry, the launching of communication satellites, and, of course, the Internet.

During the first two decades of their existence, computer systems were highly centralized, usually within a single large room. Not infrequently, this room had glass walls, through which visitors could gawk at the great electronic wonder inside. A medium-sized company or university might have had one or two computers, while very large institutions had at most a few dozen.

The merging of computers and communications has had a profound influence on the way computer systems are organized. The once-dominant concept of the "computer center" as a room with a large computer to which users bring their work for processing is now totally obsolete (although data centers holding thousands of Internet servers are becoming common). The old model of a single computer serving all of the organization's computational needs has been replaced by one in which a large number of separate but interconnected computers do the job. These systems are called **computer networks**.

In simple terms, "Computer Network" means a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information. The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used. Networks come in many sizes, shapes and forms, as we will see later. They are usually connected together to make larger networks, with the **Internet** being the most well-known example of a network of networks.

History of Computer Networks

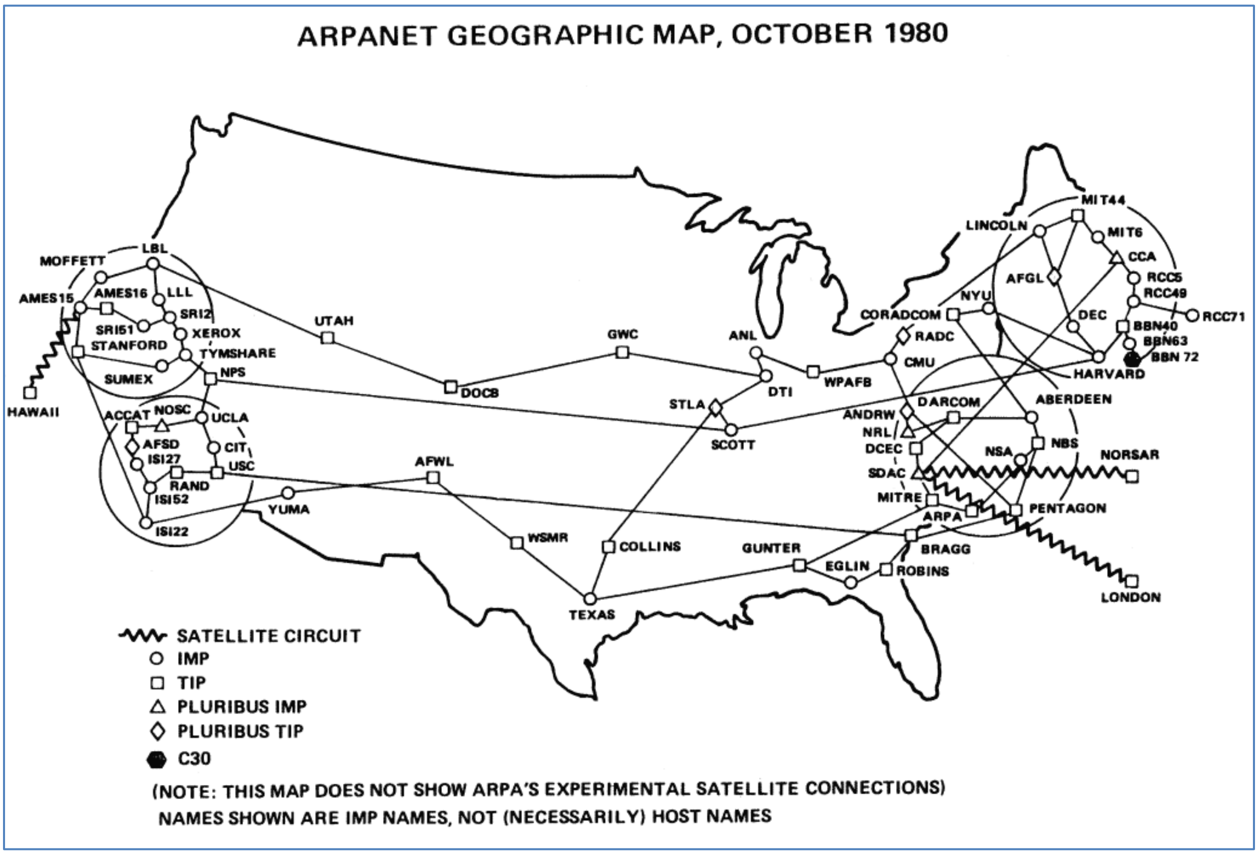
A computer network, or simply a network, is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information. As of 2015 computer networks are the core of modern communication.

The chronology of significant computer-network developments includes:

- In the late 1950s early networks of communicating computers included the military radar system Semi-Automatic Ground Environment (SAGE).
- In 1959 Anatolii Ivanovich Kitov proposed to the Central Committee of the Communist Party of the Soviet Union a detailed plan for the re-organization of the control of the Soviet armed forces and of the Soviet economy on the basis of a network of computing centres.
- In 1960 the commercial airline reservation system semi-automatic business research environment (SABRE) went online with two connected mainframes.
- In 1962 J.C.R. Licklider developed a working group he called the "Intergalactic Computer Network", a precursor to the ARPANET, at the Advanced Research Projects Agency (ARPA).
- In 1964 researchers at Dartmouth College developed the Dartmouth Time Sharing System for distributed users of large computer systems. The same year, at Massachusetts Institute of Technology, a research group supported by General Electric and Bell Labs used a computer to route and manage telephone connections.
- Throughout the 1960s, Leonard Kleinrock, Paul Baran, and Donald Davies independently developed network systems that used packets to transfer information between computers over a network.
- In 1965, Thomas Marill and Lawrence G. Roberts created the first wide area network (WAN). This was an immediate precursor to the ARPANET, of which Roberts became program manager.
- Also in 1965, Western Electric introduced the first widely used telephone switch that implemented true computer control.

- In 1969 the University of California at Los Angeles, the Stanford Research Institute, the University of California at Santa Barbara, and the University of Utah became connected as the beginning of the ARPANET network using 50 kbit/s circuits.

ARPANET GEOGRAPHIC MAP, OCTOBER 1980



(NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

- In 1972 commercial services using X.25 were deployed, and later used as an underlying infrastructure for expanding TCP/IP networks.
- In 1973, Robert Metcalfe wrote a formal memo at Xerox PARC describing Ethernet, a networking system that was based on the Aloha network, developed in the 1960s by Norman Abramson and colleagues at the University of Hawaii. In July 1976, Robert Metcalfe and David Boggs published their paper "Ethernet: Distributed Packet Switching for Local Computer Networks" and collaborated on several patents received in 1977 and 1978. In 1979 Robert Metcalfe pursued making Ethernet an open standard.
- In 1976 John Murphy of Datapoint Corporation created ARCNET, a token-passing network first used to share storage devices.

- In 1995 the transmission speed capacity for Ethernet increased from 10 Mbit/s to 100 Mbit/s. By 1998, Ethernet supported transmission speeds of a Gigabit. The ability of Ethernet to scale easily (such as quickly adapting to support new fiber optic cable speeds) is a contributing factor to its continued use as of 2015.

Packets

Most of the information in computer networks is carried in *packets*. A network packet is a formatted unit of data (a list of bits or bytes, usually a few tens of bytes to a few kilobytes long) carried by a packet-switched network. Computer communication links that do not support packets, such as traditional point-to-point telecommunication links, simply transmit data as a bit stream.

In packet networks, the data is formatted into packets that are sent through the network to their destination. Once the packets arrive they are reassembled into their original message. With packets, the bandwidth of the transmission medium can be better shared among users than if the network were circuit switched. When one user is not sending packets, the link can be filled with packets from others users, and so the cost can be shared, with relatively little interference, provided the link isn't overused.

Packets consist of two kinds of data: control information and user data (also known as payload). The control information provides data the network needs to deliver the user data, for example: source and destination network addresses, error detection codes, and sequencing information. Typically, control information is found in packet headers and trailers, with payload data in between.

Often the route a packet needs to take through a network is not immediately available. In that case the packet is queued and waits until a link is free.

Applications of Computer Networks

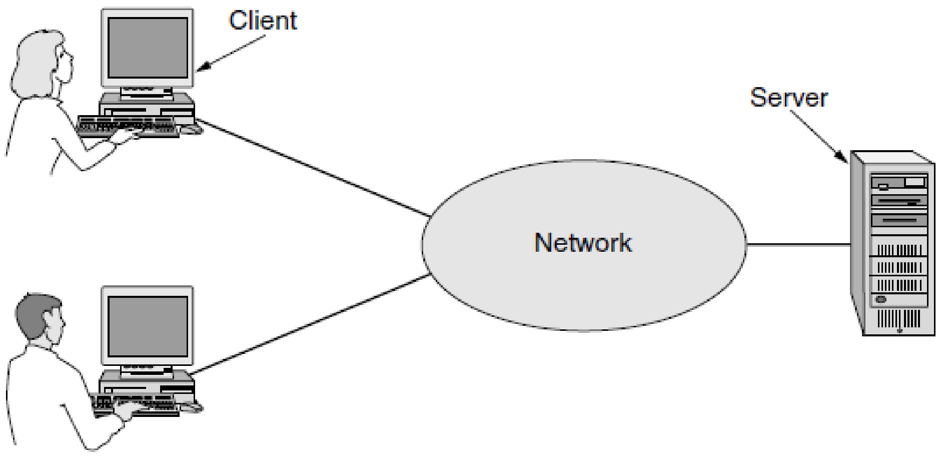
A computer network facilitates interpersonal communications allowing people to communicate efficiently and easily providing access to information on shared storage devices is an important feature of many networks. A network allows sharing of files, data, and other types of information giving authorized users the ability to access information stored on other computers on the network. It is worth devoting some time to pointing out why people are interested in computer networks and what they can be used for. Some of the major areas of applications of Computer Networks are stated, as follows:

1. Business Applications

Most companies have a substantial number of computers. The issue here is **resource sharing**. The goal is to make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource or the user. An obvious and widespread example is having a group of office workers share a common printer. For smaller companies, all the computers are likely to be in a single office or perhaps a single building, but for larger ones, the computers and employees may be scattered over dozens of offices and plants in many countries.

Networks called **VPNs** (**Virtual Private Networks**) may be used to join the individual networks at different sites into one extended network. In other words, the mere fact that a user happens to be 15,000 km away from his data should not prevent him from using the data as though they were local.

In the simplest of terms, one can imagine a company's information system as consisting of one or more databases with company information and some number of employees who need to access them remotely. In this model, the data are stored on powerful computers called **servers**. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simpler machines, called **clients**, on their desks, with which they access remote data, for example, to include in spreadsheets they are constructing. This whole arrangement is called the **client-server model**. It is widely used and forms the basis of much network usage. The most popular realization is that of a **Web application**, in which the server generates Web pages based on its database in response to client requests that may update the database.



A network with two clients and one server.

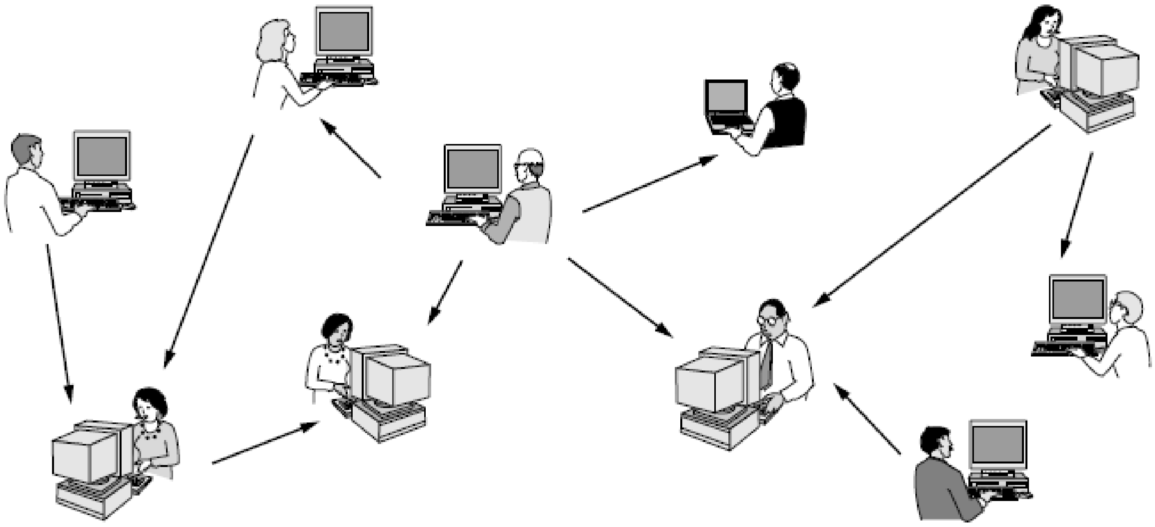
Communication takes the form of the client process sending a message over the network to the server process. The client process then waits for a reply message. When the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply.

A computer network can provide a powerful **communication medium** among employees. Virtually every company that has two or more computers now has **email** (**electronic mail**), which employees generally use for a great deal of daily communication. Telephone calls between employees may be carried by the computer network instead of by the phone company. This technology is called **IP telephony** or **Voice over IP** (**VoIP**) when Internet technology is used. A third goal for many companies is doing business electronically, especially with customers and suppliers. This new model is called **e-commerce** (**electronic commerce**) and it has grown rapidly in recent years.

2. Home Applications

Internet access provides home users with connectivity to remote computers. As with companies, home users can access information, communicate with other people, and buy products and services with e-commerce. The main benefit now comes from connecting outside of the home. Bob Metcalfe, the inventor of Ethernet, hypothesized that the value of a network is proportional to the square of the number of users because this is roughly the number of different connections that may be made (Gilder, 1993). This hypothesis is known as “Metcalfe’s law”. It helps to explain how the tremendous popularity of the Internet comes from its size.

Much of the information is accessed using the client-server model, but there is different, popular model for accessing information that goes by the name of **peer-to-peer communication** (Parameswaran et al., 2001). In this form, individuals who form a loose group can communicate with others in the group. Every person can, in principle, communicate with one or more other people; there is no fixed division into clients and servers.



In a peer-to-peer system there are no fixed clients and servers.

Peer-to-peer communication is often used to share music and videos. It really hit the big time around 2000 with a music sharing service called Napster that was shut down after what was probably the biggest copyright infringement case in all of recorded history (Lam and Tan, 2001; and Macedonia, 2000).

Instant Messaging is derived from the UNIX *talk* program in use since around 1970, allows two people to type messages at each other in real time. There are multi-person messaging services too, such as the **Twitter** service that lets people send short text messages called ‘‘tweets’’ to their circle of friends or other willing audiences.

TV shows now reach many homes via **IPTV** (**IPTeleVision**) systems that are based on IP technology instead of cable TV or radio transmissions. Another form of entertainment is game playing. Another category is **ubiquitous computing**, in which computing is embedded into everyday life, as in the vision of Mark Weiser (1991).

3. Mobile Users

Mobile computers, such as laptop and handheld computers, are one of the fastest-growing segments of the computer industry. Cellular networks operated by the telephone companies are one familiar kind of wireless network that blankets us with coverage for mobile phones. **Wireless hotspots** based on the **IEEE 802.11** standard are another kind of wireless network for mobile computers. They have sprung up everywhere that people go, resulting in a patchwork of coverage at cafes, hotels, airports, schools, trains and planes. Anyone with a laptop computer and a wireless modem can just turn on their computer on and be connected to the Internet through the hotspot, as though the computer were plugged into a wired network.

Wireless Hotspots

An area in which mobile phones are now starting to be used is **m-commerce** (**mobile-commerce**) (Senn, 2000).When equipped with **NFC** (**Near Field Communication**) technology the mobile can act as an RFID smartcard and interact with a nearby reader for payment. **Wearable computers** are another promising application.

4. Social Issues

Computer networks, like the printing press 500 years ago, allow ordinary citizens to distribute and view content in ways that were not previously possible. But along with the good comes the bad, as this new-found freedom brings with it many unsolved social, political, and ethical issues.

Social networks, message boards, content sharing sites, and a host of other applications allow people to share their views with like-minded individuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise. The trouble comes with topics that people actually care about, like politics, religion, or human rights. Views that are publicly posted may be deeply offensive to some people. Worse yet, they may not be politically correct. In the past, people have sued network operators, claiming that they are responsible for the contents of what they carry, just as newspapers and magazines are.

Some network operators block content for their own reasons. Some users of peer-to-peer applications had their network service cut off because the network operators did not find it profitable to carry the large amounts of traffic sent by those applications. Those same operators would probably like to treat different companies differently. Opponents of this practice argue that peer-to-peer and other content should be treated in the same way because they are all just bits to the network. This argument for communications that are not differentiated by their content or source or who is providing the content is known as **network neutrality** (Wu, 2003).

A lot of these problems could be solved if the computer industry took computer security seriously. If all messages were encrypted and authenticated, it would be harder to commit mischief. Such technology is well established.

NETWORK TOPOLOGIES

Communication Components

A data communications system has five components:
1. **Message**: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

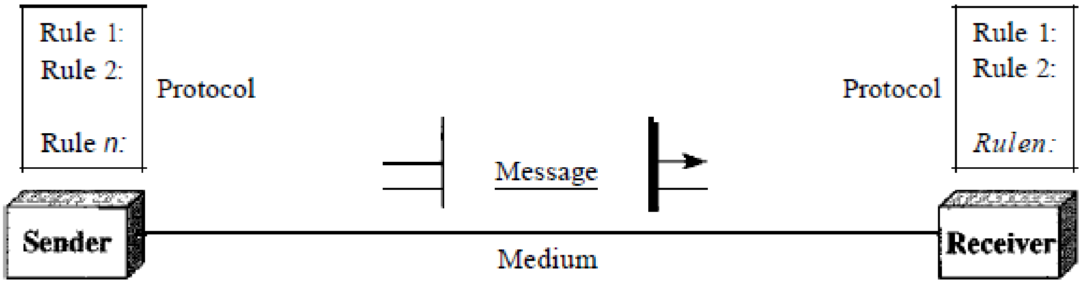
2 **Sender**: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. **Receiver**: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. **Transmission medium**: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5. **Protocol**: A protocol is a set of rules that govern data communications.

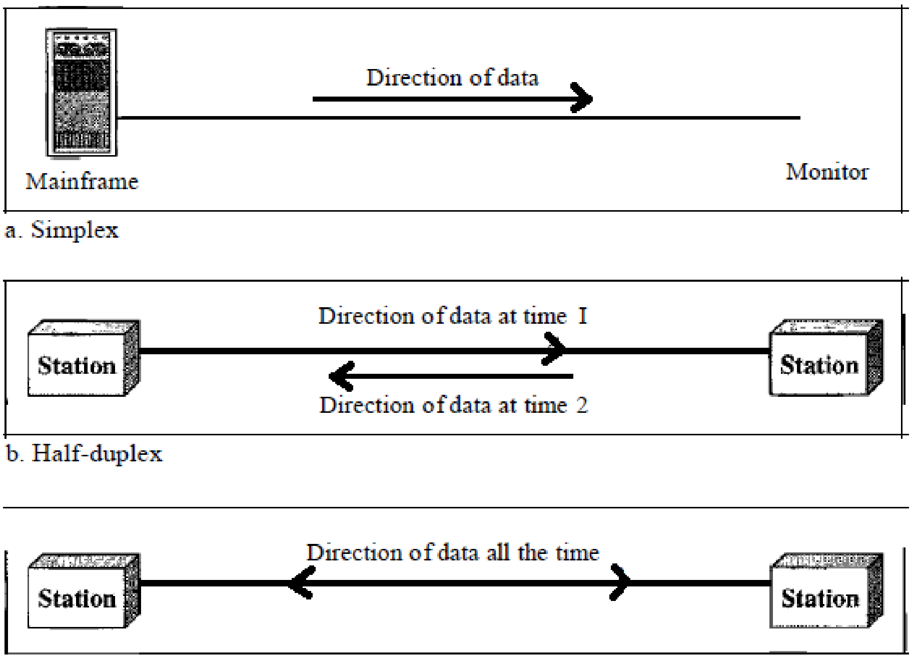
Five components ofdata communication



Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex.

Data flow (simplex, half-duplex, andfull-duplex)


Direction of data
Mainframe
Monitor
Direction of data at time 1
Station
Station
Direction of data at time 2
Direction of data all the time
Station
Station

a. Simplex

b. Half-duplex

c. Full-duplex

Simplex

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output.

Half-Duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.

Full-Duplex

In full-duplex mode, (also called duplex), both stations can transmit and receive simultaneously.

Network Structure

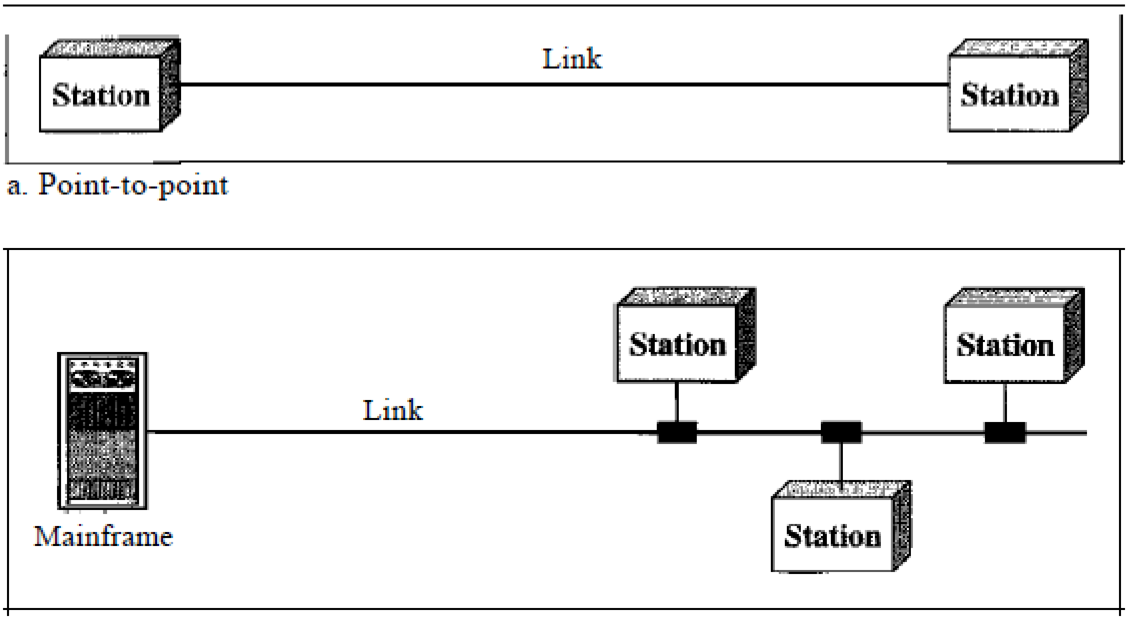
There are two possible types of connections: point-to-point and multipoint.

Point-to-Point: A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

Multipoint: A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a *spatially shared* connection. If users must take turns, it is a *timeshared* connection.

-

Types ofconnections: point-to-point and multipoint



a. Point-to-point

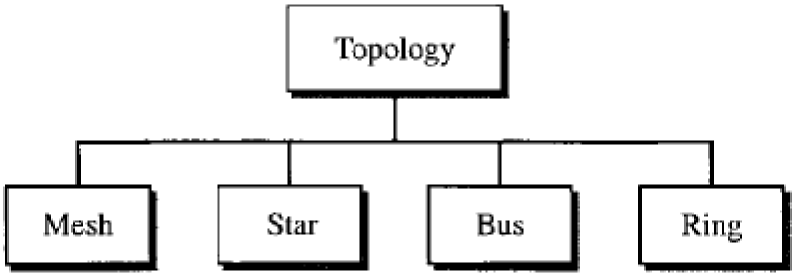
b. Multipoint

Network Topology

The term *physical topology or Network Topology* refers to the way in which a network is laid out physically. One or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.

There are four basic topologies possible: mesh, star, bus, and ring.

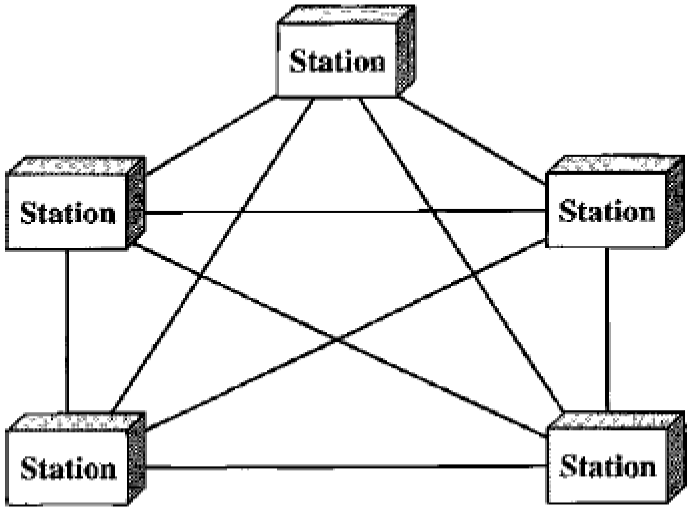
Categories oftopology



Mesh Topology:

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects.

A fully connected mesh topology (five devices)



To find the number of physical links in a fully connected mesh network with *n* nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to *n* - 1 nodes, node 2 must be connected to *n* – 1 nodes, and finally node *n* must be connected to *n* - 1 nodes. We need *n(n* - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need *n(n* -1) /2 duplex-mode links. To accommodate that many links, every device on the network must have *n* – 1 input/output *(I/O)* ports to be connected to the other *n* - 1 stations.

A mesh offers several **advantages** over other network topologies:

First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

Second, a mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.

Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

The main **disadvantages** of a mesh are related to the amount of cabling and the number of I/O ports required.

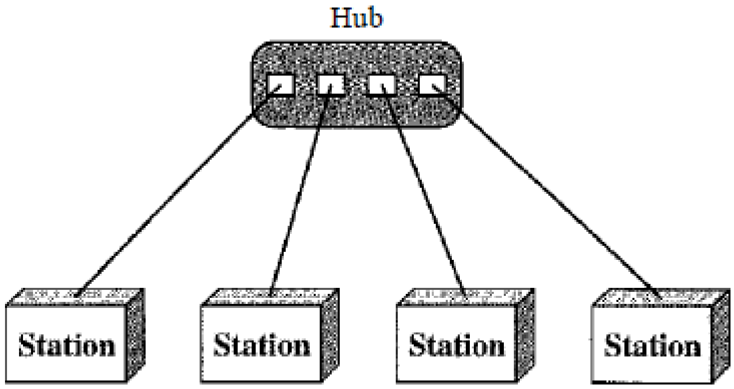
First, because every device must be connected to every other device, installation and reconnection are difficult.
Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive. For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology

Star Topology In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a *hub* or a *switch*. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

A star topology connecting four stations



A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub. Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

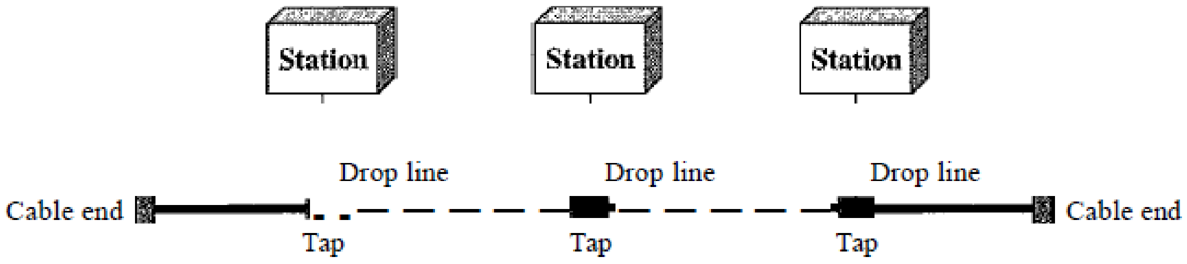
One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

The star topology is used in local-area networks (LANs). High-speed LANs often use a star topology with a central hub.

Bus Topology

The preceding examples all describe point-to-point connections. A **bus topology,** on the other hand, is multipoint. One long cable acts as a **backbone** to link all the devices in a network.

A bus topology connecting three stations



Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, and then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

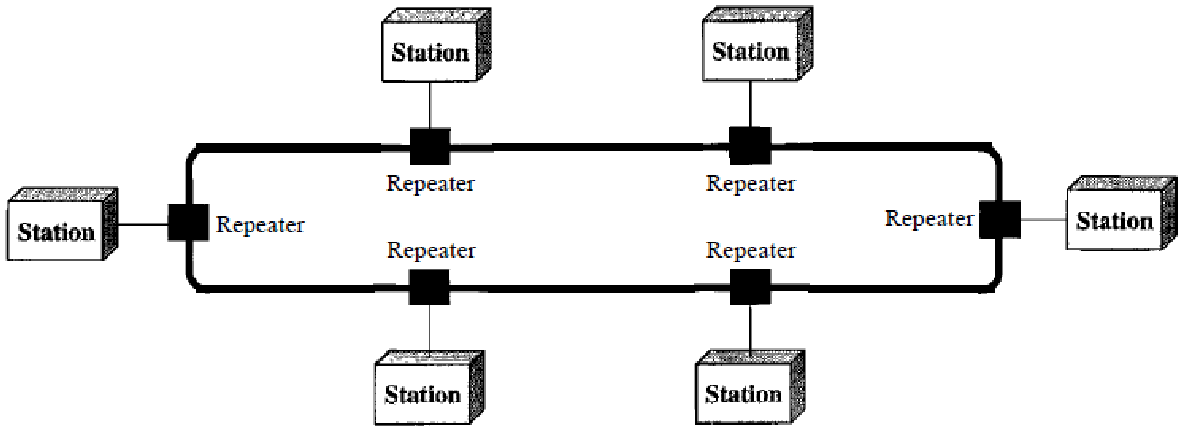
Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone. In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

Bus topology was the one of the first topologies used in the design of early localarea networks. Ethernet LANs can use a bus topology, but they are less popular now for reasons.

Ring Topology

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

A ring topology connecting six stations



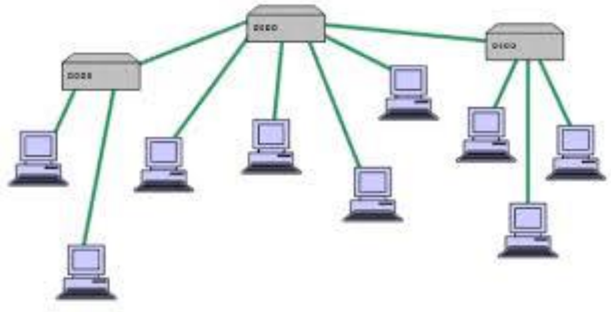
A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

Tree Topology

A tree topology is essentially a combination of bus topology and star topology. The nodes of bus topology are replaced with standalone star topology networks. This results in both disadvantages of bus topology and advantages of star topology.



Tree Topology

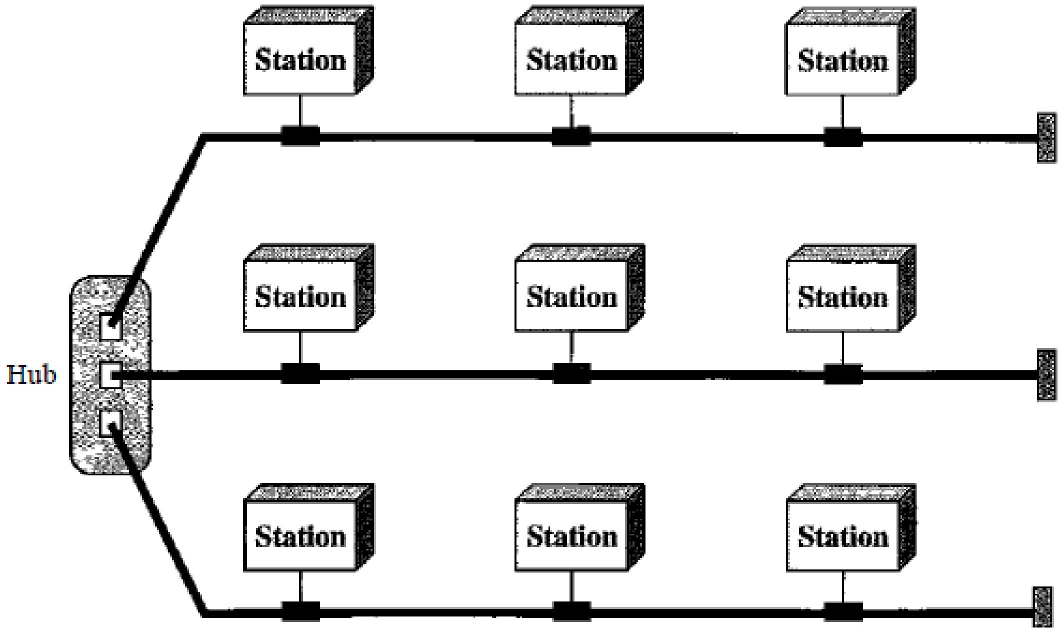
It has a root node, intermediate nodes, and ultimate nodes. This structure is arranged in a hierarchical form and any intermediate node can have any number of the child nodes.

Many supercomputers use a fat tree network, including the Yellowstone (supercomputer), the Tianhe-2, the Meiko Scientific CS-2, the Earth Simulator, the Cray X2, the CM-5, and many Altix supercomputers.

Hybrid Topology

A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology.

A hybrid topology: a star backbone with three bus networks



Daisy Chain Topology

Except for star-based networks, the easiest way to add more computers into a network is by daisy-chaining, or connecting each computer in series to the next. If a message is intended for a computer partway down the line, each system bounces it along in sequence until it reaches the destination. A daisy-chained network can take two basic forms: linear and ring.

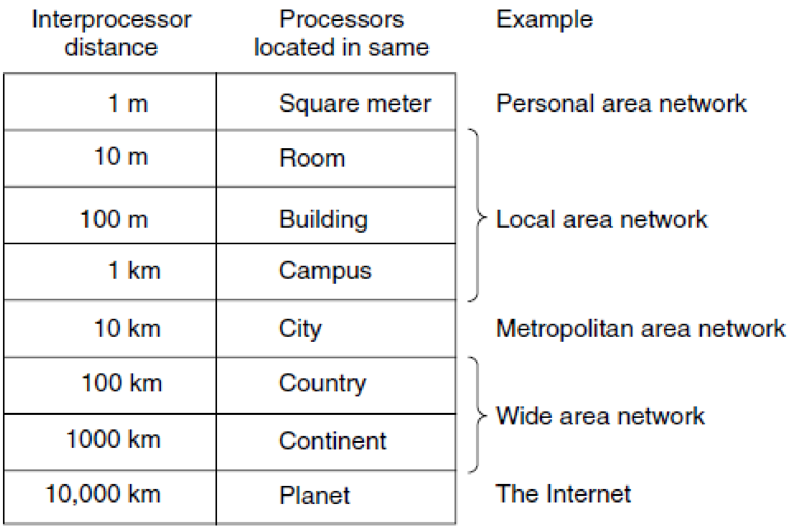
By connecting the computers at each end, a ring topology can be formed. An advantage of the ring is that the number of transmitters and receivers can be cut in half, since a message will eventually loop all of the way around. When a node sends a message, the message is processed by each computer in the ring. If the ring breaks at a particular link then the transmission can be sent via the reverse path thereby ensuring that all nodes are always connected in the case of a single failure.

TYPES OF NETWORKS

Network Hardware

As stated earlier, there are two types of transmission technology that are in widespread use: **broadcast** links and **point-to-point** links. Point-to-point links connect individual pairs of machines. In contrast, on a broadcast network, the communication channel is shared by all the machines on the network; packets sent by any machine are received by all the others.

An alternative criterion for classifying networks is by scale. Distance is important as a classification metric because different technologies are used at different scales. In Fig. 1-6 we classify multiple processor systems by their rough physical size. At the top are the personal area networks, networks that are meant for one person. Beyond these come longer-range networks. These can be divided into local, metropolitan, and wide area networks, each with increasing scale. Finally, the connection of two or more networks is called an internetwork. The worldwide Internet is certainly the best-known (but not the only) example of an internetwork.



Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Classification of interconnected processors by scale.

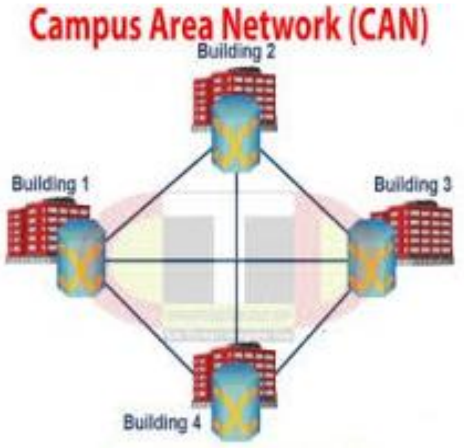
Soon we will have even larger internetworks with the **Interplanetary Internet** that connects networks across space (Burleigh et al., 2003).

Storage Area Network (SAN)

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network by other devices. The cost and complexity of SANs dropped in the early 2000s to levels allowing wider adoption across both enterprise and small to medium-sized business environment.

Campus Area Network (CAN)

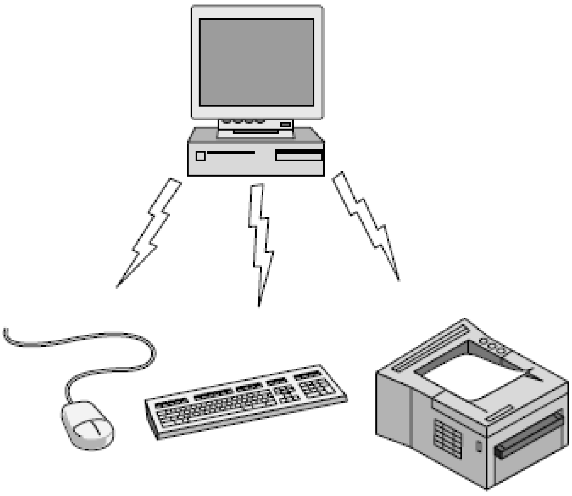
A campus area network (CAN) is made up of an interconnection of LANs within a limited geographical area. The networking equipment (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling, etc.) are almost entirely owned by the campus tenant / owner (an enterprise, university, government, etc.).



Personal Area Network (PAN)

PANs (Personal Area Networks) let devices communicate over the range of a person. A common example is a wireless network that connects a computer with its peripherals. Almost every computer has an attached monitor, keyboard, mouse, and printer. Without using wireless, this connection must be done with cables. So many new users have a hard time finding the right cables and plugging them into the right little holes (even though they are usually color coded) that most computer vendors offer the option of sending a technician to the user’s home to do it. To help these users, some companies got together to design a short-range wireless network called **Bluetooth** to connect these components without wires. The idea is that if your devices have Bluetooth, then you need no cables. You just put them down, turn them on, and they work together. For many people, this ease of operation is a big plus.

In the simplest form, Bluetooth networks use the master-slave paradigm. The system unit (the PC) is normally the master, talking to the mouse, keyboard, etc., as slaves. The master tells the slaves what addresses to use, when they can broadcast, how long they can transmit, what frequencies they can use, and so on.



Bluetooth PAN configuration.

Bluetooth can be used in other settings, too. It is often used to connect a headset to a mobile phone without cords and it can allow your digital music player to connect to your car merely being brought within range. A completely different kind of PAN is formed when an embedded medical device such as a pacemaker, insulin pump, or hearing aid talks to a user-operated remote control. PANs can also be built with other technologies that communicate over short ranges, such as RFID on smartcards and library books.

Local Area Network (LAN)

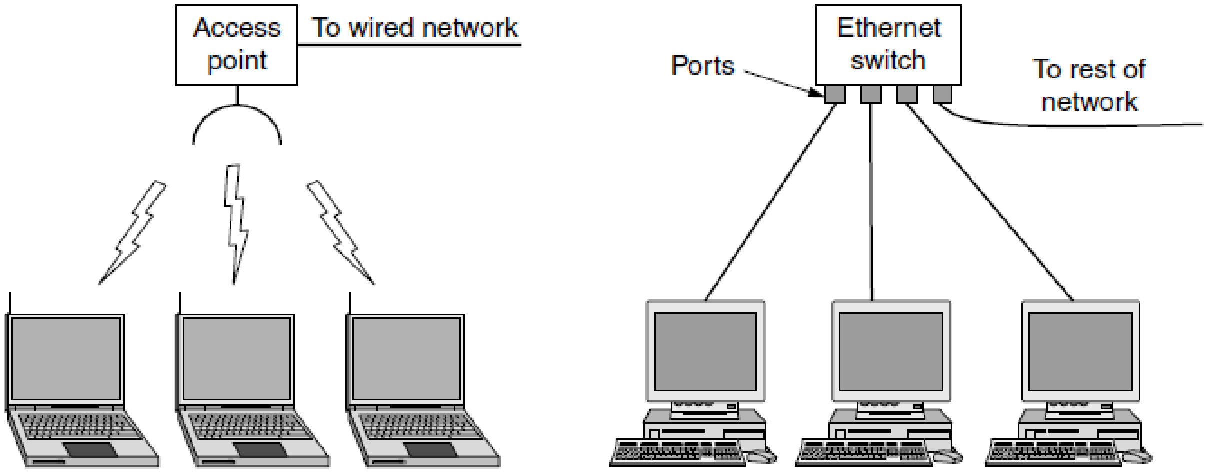
A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory. LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information.

When LANs are used by companies, they are called **enterprise networks**. Wireless LANs are very popular these days, especially in homes, older office buildings, cafeterias, and other places where it is too much trouble to install cables. In these systems, every computer has a radio modem and an antenna that it uses to communicate with other computers. In most cases, each computer talks to a device in the ceiling. This device, called an **AP** (**Access Point**), **wireless router**, or **base station**, relays packets between the wireless computers and also between them and the Internet. However, if other computers are close enough, they can communicate directly with one another in a peer-to-peer configuration.

There is a standard for wireless LANs called **IEEE 802.11**, popularly known as **WiFi**, which has become very widespread. It runs at speeds anywhere from 11 to hundreds of Mbps

Compared to wireless networks, wired LANs exceed them in all dimensions of performance. It is just easier to send signals over a wire or through a fiber than through the air.

The topology of many wired LANs is built from point-to-point links. IEEE 802.3, popularly called **Ethernet**, is, by far, the most common type of wired LAN. The following shows a sample topology of **switched Ethernet**. Each computer speaks the Ethernet protocol and connects to a box called a **switch** with a point-to-point link. Hence, the name. A switch has multiple **ports**, each of which can connect to one computer. The job of the switch is to relay packets between computers that are attached to it, using the address in each packet to determine which computer to send it to.



Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet.

To build larger LANs, switches can be plugged into each other using their ports. If you plug them together in a loop, It is the job of the protocol to sort out what paths packets should travel to safely reach the intended computer. It is also possible to divide one large physical LAN into two smaller logical LANs. Sometimes, the layout of the network equipment does not match the organization’s structure. For example, the engineering and finance departments of a company might have computers on the same physical LAN because they are in the same wing of the building but it might be easier to manage the system if engineering and finance logically each had its own network **Virtual LAN** or **VLAN**. In this design each port is tagged with a ‘‘color,’’ say green for engineering and red for finance. The switch then forwards packets so that computers attached to the green ports are separated from the computers attached to the red ports. Broadcast packets sent on a red port, for example, will not be received on a green port, just as though there were two different LANs.

There are other wired LAN topologies too. In fact, switched Ethernet is a modern version of the original Ethernet design that broadcast all the packets over a single linear cable. At most one machine could successfully transmit at a time, and a distributed arbitration mechanism was used to resolve conflicts. It used a simple algorithm: computers could transmit whenever the cable was idle. If two or more packets collided, each computer just waited a random time and tried later. We call that version **classic Ethernet**.

Both wireless and wired broadcast networks can be divided into static and dynamic designs, depending on how the channel is allocated. A typical static allocation would be to divide time into discrete intervals and use a round-robin algorithm, allowing each machine to broadcast only when its time slot comes up.

Static allocation wastes channel capacity when a machine has nothing to say during its allocated slot, so most systems attempt to allocate the channel dynamically (i.e., on demand).

Dynamic allocation methods for a common channel are either centralized or decentralized. In the centralized channel allocation method, there is a single entity, for example, the base station in cellular networks, which determines who goes next. It might do this by accepting multiple packets and prioritizing them according to some internal algorithm. In the decentralized channel allocation method, there is no central entity; each machine must decide for itself whether to transmit.

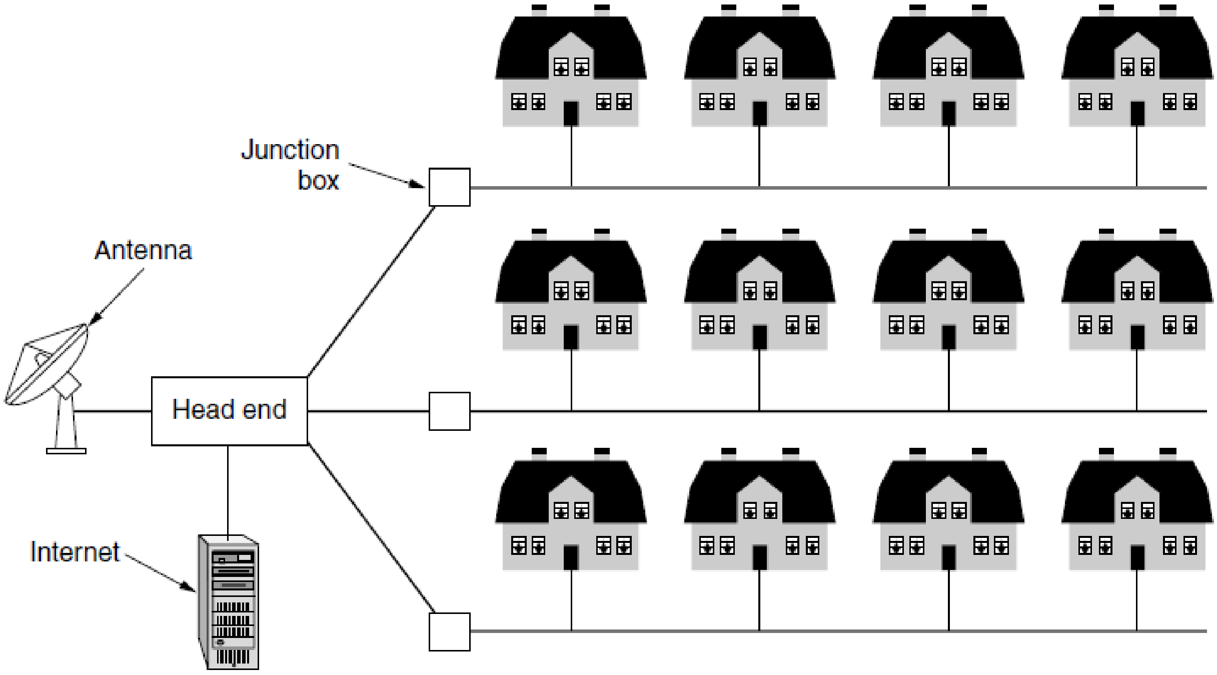
Metropolitan Area Network (MAN)

A **MAN** (**Metropolitan Area Network**) covers a city. The best-known examples of MANs are the cable television networks available in many cities. These systems grew from earlier community antenna systems used in areas with poor over-the-air television reception. In those early systems, a large antenna was placed on top of a nearby hill and a signal was then piped to the subscribers' houses.

At first, these were locally designed, ad hoc systems. Then companies began jumping into the business, getting contracts from local governments to wire up entire cities. The next step was television programming and even entire channels designed for cable only. Often these channels were highly specialized, such as all news, all sports, all cooking, all gardening, and so on. But from their inception until the late 1990s, they were intended for television reception only.

When the Internet began attracting a mass audience, the cable TV network operators began to realize that with some changes to the system, they could provide two-way Internet service in unused parts of the spectrum. At that point, the cable TV system began to morph from simply a way to distribute television to a metropolitan area network. To a first approximation, a MAN might look something like the system shown in figure. In this figure we see both television signals and Internet being fed into the centralized **cable headend** for subsequent distribution to people's homes.

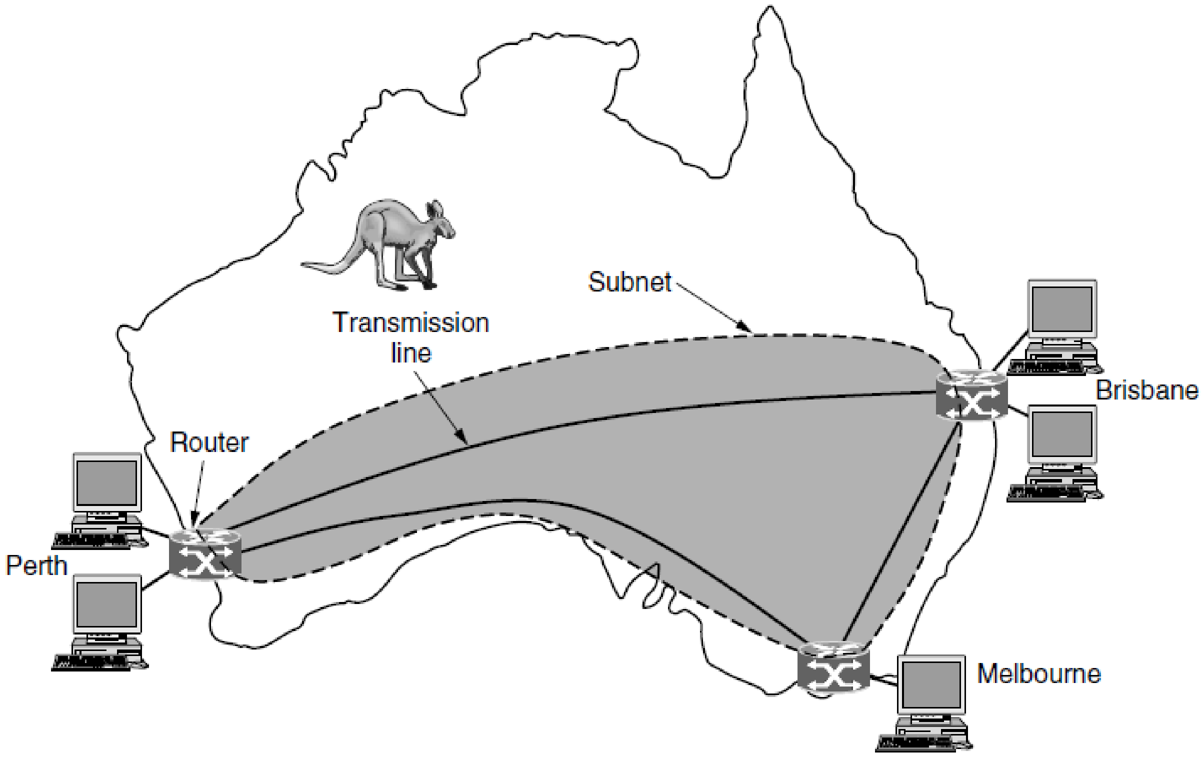
Cable television is not the only MAN, though. Recent developments in highspeed wireless Internet access have resulted in another MAN, which has been standardized as IEEE 802.16 and is popularly known as **WiMAX.**



A metropolitan area network based on cable TV.

Wide Area Networks (WAN)

A WAN (Wide Area Network) spans a large geographical area, often a country or continent. The WAN in the figure is a network that connects offices in Perth, Melbourne, and Brisbane. Each of these offices contains computers intended for running user (i.e., application) programs. We call these machines **hosts**. The rest of the network that connects these hosts is then called the **communication subnet**, or just **subnet** for short. The job of the subnet is to carry messages from host to host, just as the telephone system carries words (really just sounds) from speaker to listener.



WAN that connects three branch offices in Australia.

In most WANs, the subnet consists of two distinct components: transmission lines and switching elements. **Transmission lines** move bits between machines. They can be made of copper wire, optical fiber, or even radio links. Most companies do not have transmission lines lying about, so instead they lease the lines from a telecommunications company. **Switching elements**, or just **switches**, are specialized computers that connect two or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them. Originally, the name subnet's **only** meaning was the collection of routers and communication lines that moved packets from the source host to the destination host.

The WAN as we have described it looks similar to a large wired LAN, but there are some important differences that go beyond long wires. Usually in a WAN, the hosts and subnet are owned and operated by different people.

A second difference is that the routers will usually connect different kinds of networking technology. The networks inside the offices may be switched Ethernet, for example, while the long-distance transmission lines may be SONET links Some device needs to join them. This means that many WANs will in fact be I**nternetworks**, or composite networks that are made up of more than one network.

A final difference is in what is connected to the subnet. This could be individual computers, as was the case for connecting to LANs, or it could be entire LANs. This is how larger networks are built from smaller ones. As far as the subnet is concerned, it does the same job.

There are some other varieties of WAN too. For example, a company might connect its offices to the Internet This allows connections to be made between the offices as virtual links that use the underlying capacity of the Internet. This arrangement is called a **VPN** (**Virtual Private Network**). Compared to the dedicated arrangement, a VPN has the usual advantage of virtualization, which is that it provides flexible reuse of a resource (Internet connectivity).

The second variation is that the subnet may be run by a different company. The subnet operator is known as a **network service provider** and the offices are its customers. The subnet operator will connect to other customers too, as long as they can pay and it can provide service. Since it would be a disappointing network service if the customers could only send packets to each other, the subnet operator will also connect to other networks that are part of the Internet. Such a subnet operator is called an **ISP** (**Internet Service Provider**) and the subnet is an **ISP network**. Its customers who connect to the ISP receive Internet service.

Internetworks

Many networks exist in the world, often with different hardware and software. People connected to one network often want to communicate with people attached to a different one. The fulfillment of this desire requires that different, and frequently incompatible, networks be connected. A collection of interconnected networks is called an **internetwork** or **internet**. These terms will be used in a generic sense, in contrast to the worldwide Internet (which is one specific internet), which we will always capitalize. The Internet uses ISP networks to connect enterprise networks, home networks, and many other networks.

Subnets, networks, and internetworks are often confused. The term ‘‘subnet’’ makes the most sense in the context of a wide area network, where it refers to the collection of routers and communication lines owned by the network operator. As an analogy, the telephone system consists of telephone switching offices connected to one another by high-speed lines, and to houses and businesses by low-speed lines. These lines and equipment, owned and managed by the telephone company, form the subnet of the telephone system. The telephones themselves (the hosts in this analogy) are not part of the subnet.

To go deeper, we need to talk about how two different networks can be connected. The general name for a machine that makes a connection between two or more networks and provides the necessary translation, both in terms of hardware and software, is a **gateway**. Gateways are distinguished by the layer at which they operate in the protocol hierarchy.

Since the benefit of forming an internet is to connect computers across networks, we do not want to use too low-level a gateway or we will be unable to make connections between different kinds of networks. We do not want to use too high-level a gateway either, or the connection will only work for particular applications. The level in the middle that is ‘‘just right’’ is often called the network layer, and a router is a gateway that switches packets at the network layer. We can now spot an internet by finding a network that has routers.

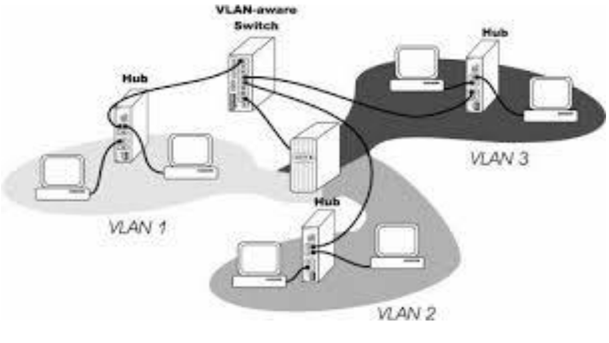
VIRTUAL LOCAL AREA NETWORK (VLAN)

It is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end station even if they are not located physically on the same LAN segment.

This is usually achieved on switch or router devices. Simpler devices only support partitioning on a port level (if at all), so sharing VLANs across devices requires running dedicated cabling for each VLAN. More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs.

Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections. Most enterprise-level networks today use the concept of virtual LANs. Without VLANs, a switch considers all interfaces on the switch to be in the same broadcast domain.

To physically replicate the functions of a VLAN would require a separate, parallel collection of network cables and equipment separate from the primary network. However, unlike physically separate networks.



Virtual Local Area Network (VLAN)

Uses

Network architects set up VLANs to provide the segmentation services traditionally provided only by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic-flow management. By definition, switches may not bridge IP traffic between VLANs as doing so would violate the integrity of the VLAN broadcast domain.

VLANs can also help create multiple layer 3 networks on a single physical infrastructure. For example, if a DHCP server is plugged into a switch it will serve any host on that switch that is configured for DHCP. By using VLANs, the network can be easily split up so some hosts will not use that DHCP server and will obtain link-local addresses, or obtain an address from a different DHCP server.

By using VLANs, one can control traffic patterns and react quickly to relocations. VLANs provide the flexibility to adapt to changes in network requirements and allow for simplified administration.

VLANs can be used to partition a local network into several distinctive segments, for example:

- Production
- Voice over IP
- Network management
- Storage area network (SAN)
- Guest network
- Demilitarized zone (DMZ)
- Client separation (ISP)

VLANs can also be used in a school or work environment to provide easier access to local networks, to allow for easy administration, and to prevent disruption on the network.

In cloud computing VLANs, IP addresses, and MAC addresses on them are resources which end users can manage.

History

After successful experiments with Voice over Ethernet from 1981 to 1984, Dr. W. David Sinofsky joined 1 2 3 IMPLEMENTATION Bellcore and began addressing the problem of scaling up Ethernet networks. At 10 Mbit/s, Ethernet was faster than most alternatives at the time; however, Ethernet was a broadcast network and there was no good way of connecting multiple Ethernet networks together. This limited the total bandwidth of an Ethernet network to 10 Mbit/s and the maximum distance between any two nodes to a few hundred feet.

By contrast, although the existing telephone network's peak speed for individual connections was limited to 56 Kbit/s (less than one hundredth of Ethernet's speed), the total bandwidth of that network was estimated at 1 Tbit/s, capable of moving over a hundred thousand times more information in a given timescale.

Sincoskie invented VLANs by adding a tag to each Ethernet packet. These tags could be thought of as colors, say red, green, or blue. Then each switch could be assigned to handle packets of a single color, and ignore the rest. The networks could be interconnected with three spanning trees, one for each color. By sending a mix of different packet colors, the aggregate bandwidth could be improved. Sincoskie referred to this as a multitree bridge. He and Chase Cotton created and refined the algorithms (called the Extended Bridge Algorithms for Large Networks) necessary to make the system feasible. This "color" is what is now known in the Ethernet frame as the IEEE 802.1Q header, or the VLAN tag. While VLANs are commonly used in modern Ethernet networks, using them for the original purpose would be rather unusual.

In 2012 the IEEE approved IEEE 802.1aq (shortest path bridging) to standardize load-balancing and shortest path forwarding of (multicast and unicast) traffic allowing larger networks with shortest path routes between devices. It was stated by David Allan and Nigel Bragg, in 802.1aq Shortest Path Bridging Design and Evolution: The Architect's Perspective that shortest path bridging is one of the most significant enhancements in Ethernet's history.

Implementation

A basic switch not configured for VLANs has VLAN functionality disabled or permanently enabled with a default VLAN that contains all ports on the device as members. Every device connected to one of its ports can send packets to any of the others. Separating ports by VLAN groups separates their traffic very much like connecting the devices to another, distinct switch of their own.

If a VLAN port group were to exist only on one device, no ports that are members of the VLAN group would need to be tagged. These ports would hence be considered “untagged”. It is only when the VLAN port group is to extend to another device that tagging is used. Every VLAN containing such ports must also contain the uplink port of each switch involved, and these ports must be tagged. This also applies to the default VLAN.

Some switches either allow or require that a name be created for the VLAN, but only the VLAN group number is important from one switch to the next.

Technologies that can implement VLANs are:

Asynchronous Transfer Mode (ATM)
Fiber Distributed Data Interface (FDDI)
Ethernet
HiperSockets

Protocols and design

The protocol most commonly used today to configure VLANs is IEEE 802.1Q. The IEEE committee defined this method of multiplexing VLANs in an effort to provide multivendor VLAN support. Prior to the introduction of the 802.1Q standard, several proprietary protocols existed, such as Cisco's ISL (Inter-Switch Link) and 3Com's VLT (Virtual LAN Trunk). Cisco also implemented VLANs over FDDI by carrying VLAN information in an IEEE 802.10 frame header, contrary to the purpose of the IEEE 802.10 standard.

Both ISL and IEEE 802.1Q tagging perform “explicit tagging” - the frame itself is tagged with VLAN information. ISL uses an external tagging process that does not modify the existing Ethernet frame, while 802.1Q uses a frame internal field for tagging, and therefore does modify the Ethernet frame. This internal tagging is what allows IEEE 802.1Q to work on both access and trunk links: frames are standard Ethernet, and so can be handled by commodity hardware.

Under IEEE 802.1Q, the maximum number of VLANs on a given Ethernet network is 4,094 (the 4,096 provided for by the 12-bit VID field minus reserved values 0x000 and 0xFFF). This does not impose the same limit on the number of IP subnets in such a network, since a single VLAN can contain multiple IP subnets. The VLAN limit is expanded to 16 million with Shortest Path Bridging.

With ISL, an Ethernet frame is encapsulated with a header that transports VLAN IDs between switches and routers. ISL does add overhead to the packet as a 26- byte header containing a 10-bit VLAN ID. In addition, a 4-byte CRC is appended to the end of each frame. This CRC is in addition to any frame checking that the Ethernet frame requires. The fields in an ISL header identify the frame as belonging to a particular VLAN.

A VLAN ID is added only if the frame is forwarded out a port configured as a trunk link. If the frame is to be forwarded out a port configured as an access link, the ISL encapsulation is removed.

Early network designers often configured VLANs with the aim of reducing the size of the collision domain in a large single Ethernet segment and thus improving performance. When Ethernet switches made this a non-issue (because each switch port is a collision domain), attention turned to reducing the size of the broadcast domain at the MAC layer. A VLAN can also serve to restrict access to network resources without regard to physical topology of the network, although the strength of this method remains debatable as VLAN hopping is a means of bypassing such security measures. VLAN hopping can be mitigated with proper switchport configuration.

VLANs operate at Layer 2 (the data link layer) of the OSI model. Administrators often configure a VLAN to map directly to an IP network, or subnet, which gives the appearance of involving Layer 3 (the network layer). In the context of VLANs, the term “trunk” denotes a network link carrying multiple VLANs, which are identified by labels (or “tags”) inserted into their packets. Such trunks must run between “tagged ports” of VLAN-aware devices, so they are often switch-to-switch or switch-torouter links rather than links to hosts. (Note that the term 'trunk' is also used for what Cisco calls “channels”: Link Aggregation or Port Trunking). A router (Layer 3 device) serves as the backbone for network traffic going across different VLANs.

THE OSI MODEL

There two important network architectures: the OSI reference model and the TCP/IP reference model. Although the *protocols* associated with the OSI model are not used any more, the *model* itself is quite general and still valid, and the features discussed at each layer are still very important. The TCP/IP model has the opposite properties: the model itself is not of much use but the protocols are widely used.

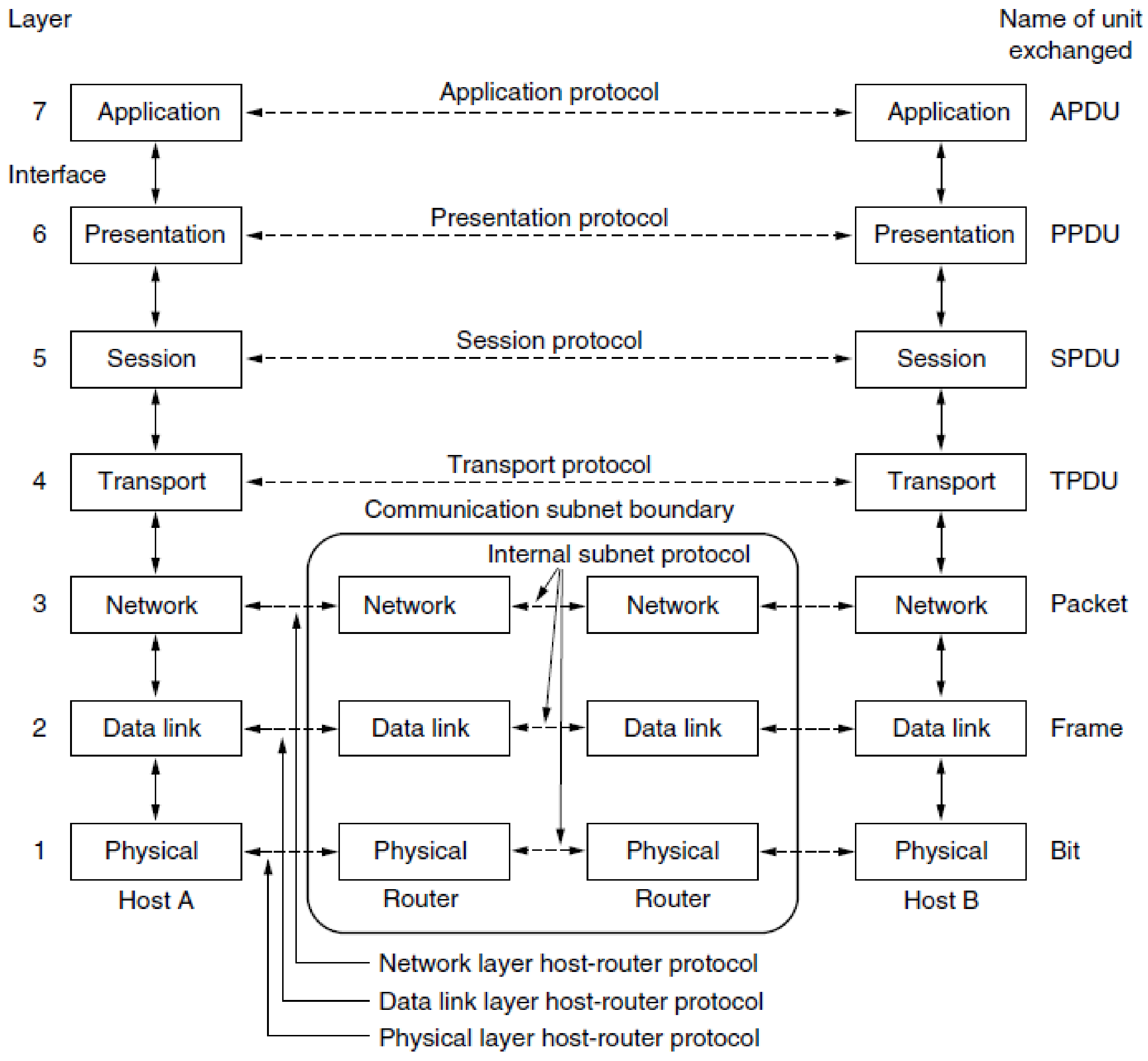


Figure 1-20. The OSI reference model.

The OSI model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983). It was revised in 1995 (Day, 1995). The model is called the ISO **OSI** (**Open Systems**

Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems. We just call it the **OSI model** for short.

The OSI model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.

2. Each layer should perform a well-defined function.

3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.

4. The layer boundaries should be chosen to minimize the information flow across the interfaces.

5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

The OSI model itself is not a network architecture because it does not specify the exact services and protocols to be used in each layer. It just tells what each layer should do. However, ISO has also produced standards for all the layers, although these are not part of the reference model itself. Each one has been published as a separate international standard. The *model* (in part) is widely used although the associated protocols have been long forgotten.

History

In the late 1970s, two projects began independently, with the same goal: to define a unifying standard for the architecture of networking systems. One was administered by the International Organization for Standardization (ISO), while the other was undertaken by the International Telegraph and Telephone Consultative Committee, or CCITT (the abbreviation is from the French version of the name). These two international standards bodies each developed a document that defined similar networking models.

In 1983, these two documents were merged to form a standard called The Basic Reference Model for Open Systems Interconnection. The standard is usually referred to as the Open Systems Interconnection Reference Model, the OSI Reference Model, or simply the OSI model. It was published in 1984 by both the ISO, as standard ISO 7498, and the renamed CCITT (now called the Telecommunications Standardization Sector of the International Telecommunication Union or ITU-T) as standard X.200.

OSI had two major components, an abstract model of networking, called the Basic Reference Model or seven-layer model, and a set of specific protocol.

The concept of a seven-layer model was provided by the work of Charles Bachman at Honeywell Information Services. Various aspects of OSI design evolved from experiences with the ARPANET, NPLNET, EIN, CYCLADES network and the work in IFIP WG6.1. The new design was documented in ISO 7498 and its various addenda. In this model, a networking system was divided into layers. Within each layer, one or more entities implement its functionality. Each entity interacted directly only with the layer immediately beneath it, and provided facilities for use by the layer above it.

Protocols enable an entity in one host to interact with a corresponding entity at the same layer in another host. Service definitions abstractly described the functionality provided to an (N)-layer by an (N-1) layer, where N was one of the seven layers of protocols operating in the local host.

Description of OSI layers

The recommendation X.200 describes seven layers, labeled 1 to 7. Layer 1 is the lowest layer in this model.

At each level N, two entities at the communicating devices (layer N peers) exchange protocol data units (PDUs) by means of a layer N protocol. Each PDU contains a payload, called the service data unit (SDU), along with protocol-related headers and/or footers.

The seven layers are:

Layer 1: Physical layer

The physical layer has the following major functions:

- It defines the electrical and physical specifications of the data connection. It defines the relationship between a device and a physical transmission medium (e.g., a copper or fiber optical cable). This includes the layout of pins, voltages, line impedance, cable specifications, signal timing, hubs, repeaters, network adapters, host bus adapters (HBA used in storage area networks) and more.

- It defines the protocol to establish and terminate a connection between two directly connected nodes over a communications medium.
- It may define the protocol for flow control.
- It defines transmission mode i.e. simplex, half duplex, full duplex.
- It defines topology.

The physical layer of Parallel SCSI operates in this layer, as do the physical layers of Ethernet and other local area networks, such as Token Ring, FDDI, ITU-T G.hn, and IEEE 802.11 (Wi-Fi), And Wi-Fi Hotspot as well as personal area networks such as Bluetooth and IEEE 802.15.4.

Layer 2: Data link layer

The data link layer provides node-to-node data transfer a reliable link between two directly connected nodes, by detecting and possibly correcting errors that may occur in the physical layer. The data link layer is divided into two sublayers:

- Media Access Control (MAC) layer - responsible for controlling how devices in a network gain access to data and permission to transmit it.
- Logical Link Control (LLC) layer - controls error checking and packet synchronization.

The Point-to-Point Protocol (PPP) is an example of a data link layer in the TCP/IP protocol stack.

Layer 3: Network layer

The network layer provides the functional and procedural means of transferring variable length data sequences (called datagrams) from one node to another connected to the same network. It translates logical network address into physical machine address. A network is a medium to which many nodes can be connected, on which every node has an address and which permits nodes connected to it to transfer messages to other nodes connected to it by merely providing the content of a message and the address of the destination node and letting the network find the way to deliver ("route") the message to the destination node. In addition to message routing, the network may (or may not) implement message delivery by splitting the message into several fragments, delivering each fragment by a separate route and reassembling the fragments, report delivery errors, etc.

Datagram delivery at the network layer is not guaranteed to be reliable.

A number of layer-management protocols, a function de- fined in the management annex, ISO 7498/4, belong to the network layer. These include routing protocols, multicast group management, network-layer information and error, and network-layer address assignment. It is the function of the payload that makes these belong to the network layer, not the protocol that carries them.

Layer 4: Transport layer

The transport layer provides the functional and procedural means of transferring variable-length data sequences from a source to a destination host via one or more networks, while maintaining the quality of service function.

The transport layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. Some protocols are state- and connection oriented. This means that the transport layer can keep track of the segments and retransmit those that fail. The transport layer also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred. The transport layer creates packets out of the message received from the application layer. Packetizing is a process of dividing the long message into smaller messages.

OSI defines five classes of connection-mode transport protocols ranging from class 0 (which is also known as TP0 and provides the fewest features) to class 4 (TP4, designed for less reliable networks, similar to the Internet). Class 0 contains no error recovery, and was designed for use on network layers that provide error-free connections. Class 4 is closest to TCP, although TCP contains functions, such as the graceful close, which OSI assigns to the session layer. Also, all OSI TP connection-mode protocol classes provide expedited data and preservation of record boundaries.

Layer 5: Session layer

The session layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes check pointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session check pointing and recovery, which is not usually used in the Internet Protocol Suite. The session layer is commonly implemented explicitly in application environments that use remote procedure calls.

Layer 6: Presentation layer

The presentation layer establishes context between application-layer entities, in which the application-layer entities may use different syntax and semantics if the presentation service provides a big mapping between them. If a mapping is available, presentation service data units are encapsulated into session protocol data units, and passed down the protocol stack.

This layer provides independence from data representation (e.g., encryption) by translating between application and network formats. The presentation layer transforms data into the form that the application accepts. This layer formats and encrypts data to be sent across a network. It is sometimes called the syntax layer.

The original presentation structure used the Basic Encoding Rules of Abstract Syntax Notation One (ASN.1), with capabilities such as converting an EBCDIC-coded text file to an ASCII-coded file, or serialization of objects and other data structures from and to XML.

Layer 7: Application layer

The application layer is the OSI layer closest to the end user, which means both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network or the requested communication exists. In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer. Some examples of application-layer implementations include:

- Web Browsers
- File transfer programs
- Mail programs such as Outlook, Opera
- SolarWinds, Openview

THE INTERNET PROTOCOL

The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahn in 1974; the other being the connection-oriented Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.

The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6).

Function

The Internet Protocol is responsible for addressing hosts and for routing datagrams (packets) from a source host to a destination host across one or more IP networks. For this purpose, the Internet Protocol defines the format of packets and provides an addressing system that has two functions: identifying hosts; and providing a logical location service.

- Datagram construction

Each datagram has two components: a header and a payload. The IP header is tagged with the source IP address, the destination IP address, and other meta-data needed to route and deliver the datagram. The payload is the data that is transported. This method of nesting the data payload in a packet with a header is called encapsulation.

- IP addressing and routing

IP addressing entails the assignment of IP addresses and associated parameters to host interfaces. The address space is divided into networks and sub networks, involving the designation of network or routing prefixes. IP routing is performed by all hosts, but most importantly by routers, which transport packets across network boundaries. Routers communicate with one another via specially designed routing protocols, either interior gateway protocols or exterior gateway protocols, as needed for the topology of the network.

IP routing is also common in local networks. For example, many Ethernet switches support IP multicast operations.[1] These switches use IP addresses and Internet Group Management Protocol to control multicast routing but use MAC addresses for the actual routing.

Reliability

The design of the Internet protocols is based on the end to-end principle. The network infrastructure is considered inherently unreliable at any single network element or transmission medium and assumes that it is dynamic in terms of availability of links and nodes. No central monitoring or performance measurement facility exists that tracks or maintains the state of the network. For the bene- fit of reducing network complexity, the intelligence in the network is purposely mostly located in the end nodes of data transmission. Routers in the transmission path forward packets to the next known, directly reachable gateway matching the routing prefix for the destination address.

As a consequence of this design, the Internet Protocol only provides best effort delivery and its service is characterized as unreliable. In network architectural language, it is a connectionless protocol, in contrast to connection oriented modes of transmission. Various error conditions may occur, such as data corruption, packet loss, duplication and out-of-order delivery. Because routing is dynamic, meaning every packet is treated independently, and because the network maintains no state based on the path of prior packets, different packets may be routed to the same destination via different paths, resulting in out of-order sequencing at the receiver.

Internet Protocol Version 4 (IPv4) provides safeguards to ensure that the IP packet header is error-free. A routing node calculates a checksum for a packet. If the checksum is bad, the routing node discards the packet. The routing node does not have to notify either end node, although the Internet Control Message Protocol (ICMP) allows such notification. By contrast, in order to increase performance, and since current link layer technology is assumed to provide sufficient error detection, the IPv6 header has no checksum to protect it.

All error conditions in the network must be detected and compensated by the end nodes of a transmission. The upper layer protocols of the Internet protocol suite are responsible for resolving reliability issues. For example, a host may cache network data to ensure correct ordering before the data is delivered to an application.

Link capacity and capability

The dynamic nature of the Internet and the diversity of its components provide no guarantee that any particular path is actually capable of, or suitable for, performing the data transmission requested, even if the path is available and reliable. One of the technical constraints is the size of data packets allowed on a given link. An application must assure that it uses proper transmission characteristics. Some of this responsibility lies also in the upper layer protocols. Facilities exist to examine the maximum transmission unit (MTU) size of the local link and Path MTU Discovery can be used for the entire projected path to the destination. The IPv4 internetworking layer has the capability to automatically fragment the original datagram into smaller units for transmission. In this case, IP provides re-ordering of fragments delivered out of order.

The Transmission Control Protocol (TCP) is an example of a protocol that adjusts its segment size to be smaller than the MTU. The User Datagram Protocol (UDP) and the Internet Control Message Protocol (ICMP) disregard MTU size, thereby forcing IP to fragment oversized datagrams.

COMPUTER NETWORKING DEVICES

. Computer networking devices

Apart from any physical transmission medium there may be, networks comprise additional basic system building blocks, such as network interface controller (NICs), repeaters, hubs, bridges, switches, routers, modems, and firewalls.

- **Network interfaces**

A network interface controller (NIC) is computer hardware that provides a computer with the ability to access the transmission media, and has the ability to process low level network information. For example the NIC may have a connector for accepting a cable, or an aerial for wireless transmission and reception, and the associated circuitry.

The NIC responds to traffic addressed to a network address for either the NIC or the computer as a whole. In Ethernet networks, each network interface controller has a unique Media Access Control (MAC) address— usually stored in the controller's permanent memory. To avoid address conflicts between network devices, the Institute of Electrical and Electronics Engineers (IEEE) maintains and administers MAC address uniqueness. The size of an Ethernet MAC address is six octets. The three most significant octets are reserved to identify NIC manufacturers. These manufacturers, using only their assigned prefixes, uniquely assign the three least-significant octets of every Ethernet interface they produce.

N*etwork interface controller*

- **Repeaters and Hubs**

A repeater is an electronic device that receives a network signal, cleans it of unnecessary noise, and regenerates it. The signal is retransmitted at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable that runs longer than 100 meters. With fiber optics, repeaters can be tens or even hundreds of kilometers apart.

A repeater with multiple ports is known as a hub. Repeaters work on the physical layer of the OSI model. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay that affects network performance. As a result, many network architectures limit the number of repeaters that can be used in a row, e.g., the Ethernet 5-4-3 rule.

Hubs have been mostly obsoleted by modern switches; but repeaters are used for long distance links, notably undersea cabling.

Hub

- **Bridges**

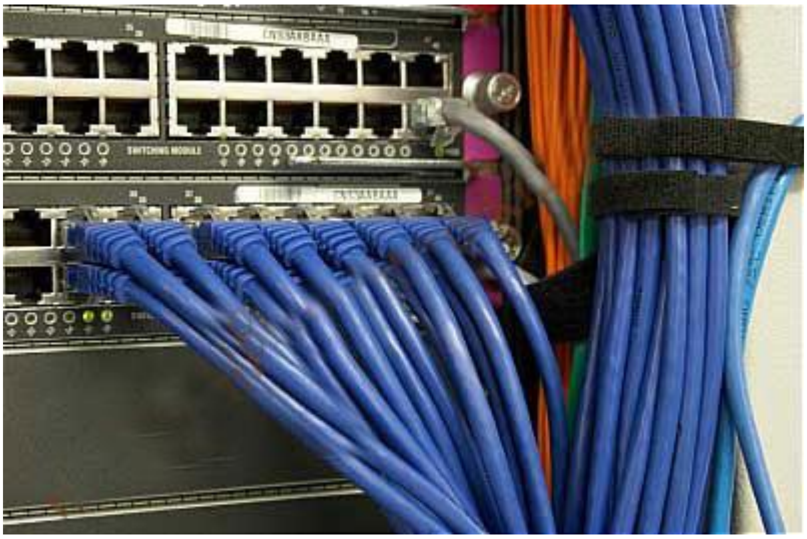
A network bridge connects and filters traffic between two network segments at the data link layer (layer 2) of the OSI model to form a single network. This breaks the network’s collision domain but maintains a unified broadcast domain. Network segmentation breaks down a large, congested network into an aggregation of smaller, more efficient networks.

Bridge

- **Switches**

A network switch is a device that forwards and filters OSI layer 2 datagrams between ports based on the MAC addresses in the packets.A switch is distinct from a hub in that it only forwards the frames to the physical ports involved in the communication rather than all ports connected. It can be thought of as a multi-port bridge. It learns to associate physical ports to MAC addresses by examining the source addresses of received frames. If an unknown destination is targeted, the switch broadcasts to all ports but the source. Switches normally have numerous ports, facilitating a star topology for devices, and cascading additional switches.

Multi-layer switches are capable of routing based on layer 3 addressing or additional logical levels. The term switch is often used loosely to include devices such as routers and bridges, as well as devices that may distribute traffic based on load or based on application content (e.g., a Web URL identifier).



Switch

- **Routers**

A router is an internetworking device that forwards packets between networks by processing the routing information included in the packet or datagram (Internet protocol information from layer 3). The routing information is often processed in conjunction with the routing table (or forwarding table). A router uses its routing table to determine where to forward packets. (A destination in a routing table can include a “null” interface, also known as the “black hole” interface because data can go into it, however, no further processing is done for said data.)

Router

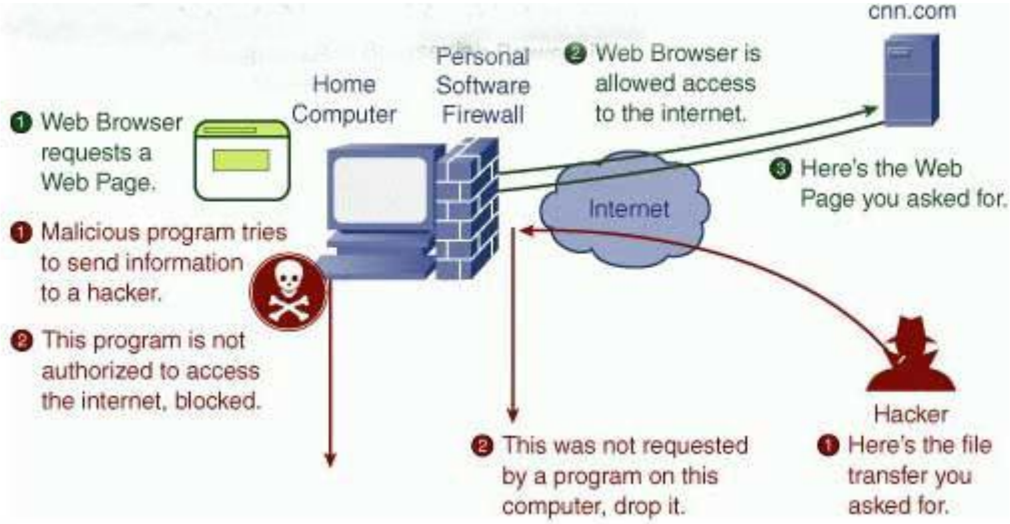
- **Modems**

Modems (MOdulator-DEModulator) are used to connect network nodes via wire not originally designed for digital network traffic, or for wireless. To do this one or more carrier signals are modulated by the digital signal to produce an analog signal that can be tailored to give the required properties for transmission. Modems are commonly used for telephone lines, using a Digital Subscriber Line technology.

Modem

- **Firewalls**

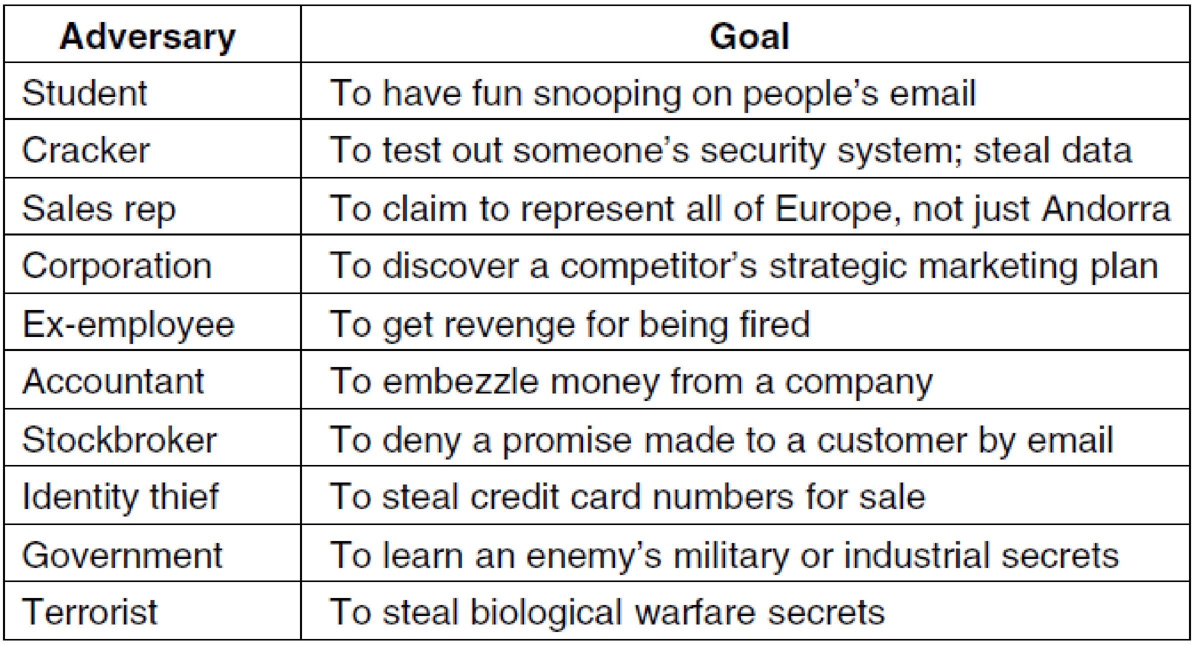
A firewall is a network device for controlling network security and access rules. Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in cyber-attacks.


cnn.com
Home Computer
Personal Software Firewall
❷ Web Browser is allowed access to the internet.
❶ Web Browser requests a Web Page.
❸ Here's the Web Page you asked for.
Internet
❶ Malicious program tries to send information to a hacker.
❷ This program is not authorized to access the internet, blocked.
Hacker
❷ This was not requested by a program on this computer, drop it.
❶ Here's the file transfer you asked for.

Firewall

NETWORK SECURITY

Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or harm someone. A few of the most common perpetrators are listed in figure. It should be clear from this list that making a network secure involves a lot more than just keeping it free of programming errors. It involves outsmarting often intelligent, dedicated, and sometimes well funded adversaries. It should also be clear that measures that will thwart casual attackers will have little impact on the serious ones. Police records show that the most damaging attacks are not perpetrated by outsiders tapping a phone line but by insiders bearing a grudge. Security systems should be designed accordingly.



Adversary	Goal
Student	To have fun snooping on people's email
Cracker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Corporation	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by email
Identity thief	To steal credit card numbers for sale
Government	To learn an enemy's military or industrial secrets
Terrorist	To steal biological warfare secrets

Some people who may cause security problems, and why.

Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the grubby little hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation deals with signatures: how do you prove that your customer really placed an electronic order for ten million left-handed doohickeys at 89 cents each when he later claims the price was 69 cents? Or maybe he claims he never placed any order. Finally, integrity control has to do with how you can be sure that a message you received was really the one sent and not something that a malicious adversary modified in transit or concocted.

All these issues (secrecy, authentication, nonrepudiation, and integrity control) occur in traditional systems, too, but with some significant differences. Integrity and secrecy are achieved by using registered mail and locking documents up.

Network security

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Network Security

Concepts

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name —i.e., the password— this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has’ is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is’ is also used (e.g., a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like Wireshark traffic and may be logged for audit purposes and for later high-level analysis.

Communication between two hosts using a network may be encrypted to maintain privacy.

Honeypots, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honeypots are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual network being protected by the honeypot. A honeypot can also direct an attacker’s attention away from legitimate servers. A honeypot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a honeypot, a honeynet is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker’s methods can be studied and that information can be used to increase network security. A honeynet typically contains one or more honeypots.

Security management

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

Types of attacks

Networks are subject to attacks from malicious sources. Attacks can be from two categories: “Passive” when a network intruder intercepts data traveling through the network, and “Active” in which an intruder initiates commands to disrupt the network’s normal operation.

Types of attacks include:

- Passive
  - Network
    - Wiretapping
    - Port scanner
    - Idle scan
- Active
  - Denial-of-service attack
  - DNS spoofing
  - Spoofing
  - Man in the middle
  - ARP poisoning
  - Smurf attack
  - Buffer overflow
  - Heap overflow
  - Format string attack
  - SQL injection
  - Phishing
  - Cross-site scripting
  - CSRF

REFERENCES

1. Computer Networks, 5th Edition by ANDREW S. TANENBAUM & DAVID J. WETHERALL. Prentice Hall

2. Web: http://en.wikipedia.org/wiki/Computer_network

3. Data Communications and Networking, Fourth Edition by Behrouz A. Forouzan. McGraw Hill.

4. Computer Networks: a systems approach, Fifth Edition by LARRY L. PETERSON & BRUCE S. DAVIE. Elsevier. MK.

*   *   *