Unit 3. World-Wide Net

Objectives of the unit

At the unit end the student should know

- Channels and networks
- Shapes of nets
- Lines and signals
- Monocentric and polycentric networks
- Client-server architecture
- Internet entities
- Physical and logical addresses
- History of internet
- Legal tenets
- Intranet

Roads for Information

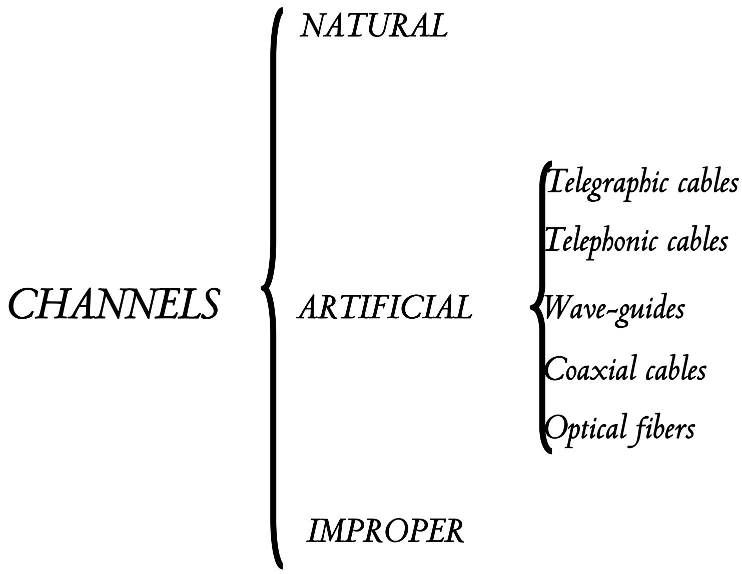


Figure 3-1

In the previous pages, we have overlooked the most simple and common component: the **wires** which transmit data inside and outside the computer system. They link the microchips and enhance the miniaturization of circuits. They are necessary to connect the peripherals to the central unit. They relate men and women all around the world. Wires take a noteworthy role everywhere. They are vital in narrow intervals, even more they are important within long distances. Wires are the most common and serviceable channels. What are **channels**?

Channels convey information from one geographic point to another; namely they change the position of E and transform E in physical terms. The channel carries on a conversion.

Channels are the basic and most simple TR units.

Engineers build the following channels:

- ✓ Telegraphic/Telephonic cables
- ✓ Wave-guides
- ✓ Coaxial cables
- ✓ Optic fibers

They are manufactured hence we tell they are ***artificial.***

Other channels may be found in Nature free and ready to use. The space is the most important ***natural channel,*** which broadcasts the light, the radio waves, the microwaves, sounds etc. all around. Space is boundless and emerges as the most astonishing and important resource. *Wireless systems* are at the cutting edge of modern ICT because they are the cheapest way to communicate.

Besides natural and artificial channels, we have ***improper channels***. They are lines devoted to various purposes that convey information too. The electrical power grid constitutes the most popular improper channel as it supplies electricity and also delivers data. An institution saves money with this channel already in hand instead of connecting computers with coaxial cables which have to be installed.

Roads for Information (contd.)

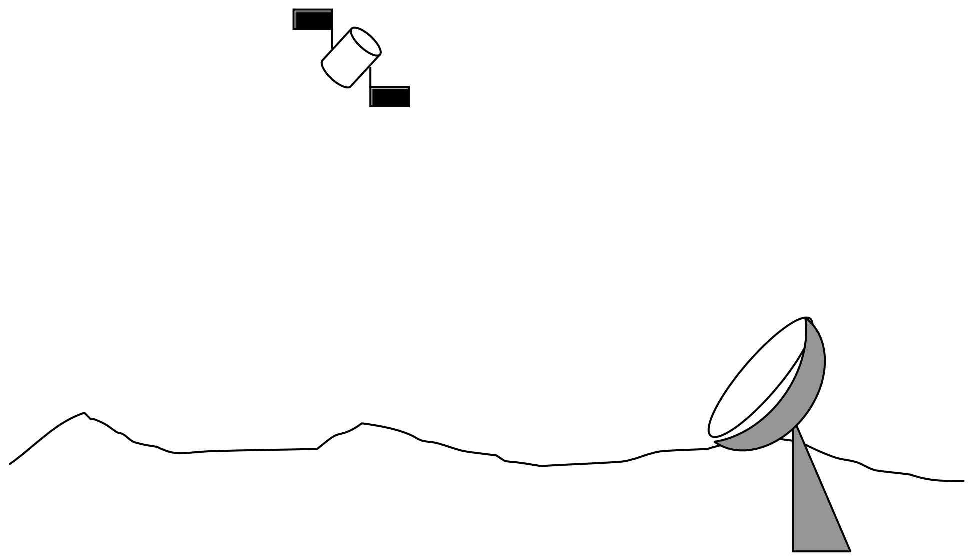


Figure 3.2

Channels operate in two distinguished ways.

1) The channel throws forth information in all directions at the same time. Anyone with a receiver tuned to the right frequency can detect the signals. This method is exclusive to the space.

2) The channel is linear and information flows through. All the artificial infrastructures make this connection.

We detail wireless communication hereunder and the second method in the next section.

1) - Broadcasting Systems - A variety of radio-stations broadcasts signals. Relay stations capture the messages and resend them forward. They lie on the ground, as aerials on top of the skyscrapers, or fly in the space as satellites for communication that have to be ***geostationary.*** They occupy fix spots in the sky and the ground stations easily locate them and direct the dish. A geostationary satellite can "see" approximately 40 percent of the earth's surface because it flies at around 36,000 kilometers (some 22,300 miles) above the earth. In principle, tree such satellites, spaced at equal intervals, can provide coverage of the entire civilized world. A geostationary satellite offers a number of distinguished services such as the Global Positioning System (GPS).

Broadcasting is an optional method for fixed terminals instead it is necessary to strike mobile devices. Cellular phones move around the world and cannot be connected with wires. A special infrastructure covers systematically the territory where mobile handsets get around. In detail, the transmitting station serves the ***cell*** that is a portion of territory ranging from one to twenty kilometers (or even more) in diameter. As X moves around, the nearest station picks up the signals from the cellular phone and forwards them. All the transmitters interconnect in the way that x can retrieve the user Y even if he lies very far away.
If the mobile phone X moves from one cell to the next, the control shifts from the transmitter x to z. The cellular system enables X to be handled by the neighboring cell without of being aware of it.

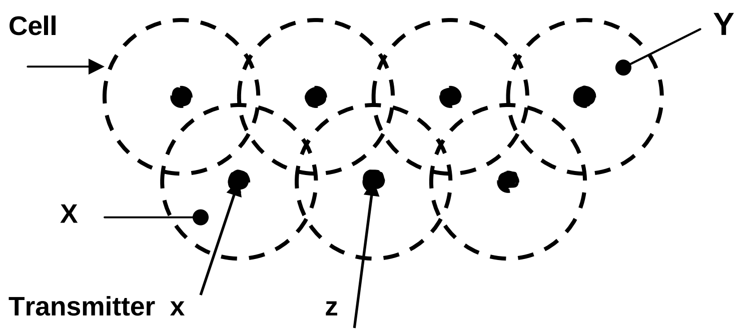


Figure 3.2bis

Cellular services are available in urban areas and along major highways, but coverage is spotty over less well-developed regions, and is nonexistent at most points over the oceans.

Networks

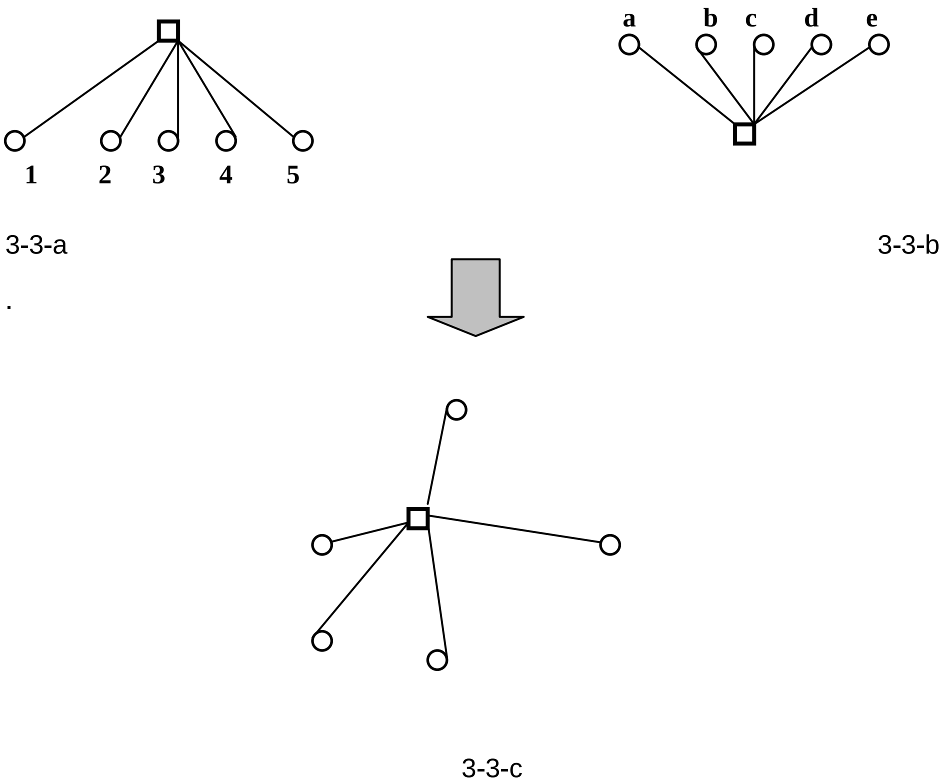


Figure 3-3

2) - Network Systems - Artificial channels and also the space are capable of linking a point to point and compound a variety of nets. Can we find a guide of this endless topic?

As first we select the node which controls another node, to wit they have the hierarchical property. For example:

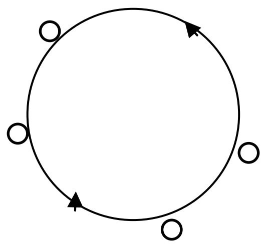
- The local-exchange manages the telephone-numbers 1, 2, 3, 4 of the local area. This node governs the other points and is paramount with respect to them (Fig 3-3-a).

- The server works for the users a, b, c, d, e in the Internet, namely these points have influence on the server and there is an evident hierarchy (Fig 3-3-b).

The hierarchical property provides the first shape for nets. In the practice, the vertices scatter over the ground and the tree becomes a ***star*** (Fig 3-3-c), namely the hierarchical tree entails a star net (see also Chapter 2).
Engineers build stable star-shaped infrastructures if the hierarchy of the nodes is definitive. Instead if the hierarchy varies, as we shall see in the next pages, the star cannot be constructed with hardware technology, but is formed through software bonds. Software programs run and determine the star-connections.

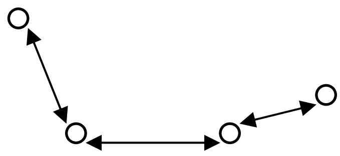
Linguistic Remark: Some author calls *broadcasting* the transmission of data from the center of the star to the nodes. This is a very approximate expression because the space only allows broadcasting toward any direction.

Networks (contd.)



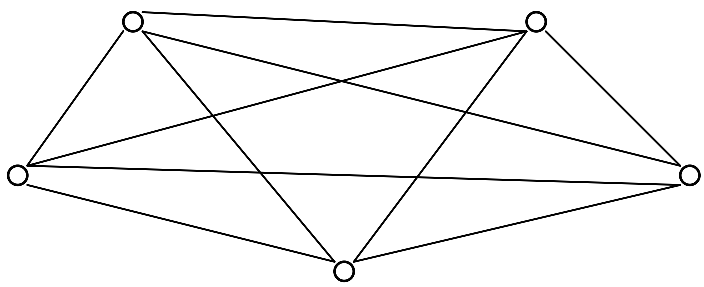
token ring

3-4-a



ethernet

3-4-b



Complete Mesh

Figure 3-4

If the nodes do not rank hierarchical tiers, the net complies with two prototypes: the ***linear graph*** and the ***complete graph*** that have the ensuing features.

a) The nodes make a line that is:
- The cheapest infrastructure,
- The simplest net,
- The less reliable solution because the whole system fails if only one stretch breaks down.

b) The complete graph includes nodes that are fully connected. Each node links all the remaining ones. The overall arrangement is:
- The most expensive infrastructure,
- The most intricate net,

- The most reliable solution since the net collapses only if all the edges break down.

These extreme patterns have strong points and weaknesses; hence we assume the following criteria.

- ♦ If the nodes cover a small area, than damages are improbable and weak, and we select a).
- ♦ If the nodes scatter on a large area, than risks are very high and we prefer b).

Experience confirms that our reasoning is correct. The **local area network (LAN)** runs a few risks and is usually an open line or otherwise a close line.

- The messages come through double way ***along the open line***, named **Ethernet,** (Fig 3-4-b).

- Signals run in one way in the ***close*** **line**. This system is best known as **token ring** (Fig 3-4-a).

The **geographic network** is a **mesh** covering a wide area such a country. Messages conveyed through may be lost, attenuated, deviated; in short transmissions are exposed to frequent dangers. The complete graph appears as the most reliable solution but is very expensive and engineers make a trade-off between the theoretical prototype and the traffic requirements.

Networks (contd.)

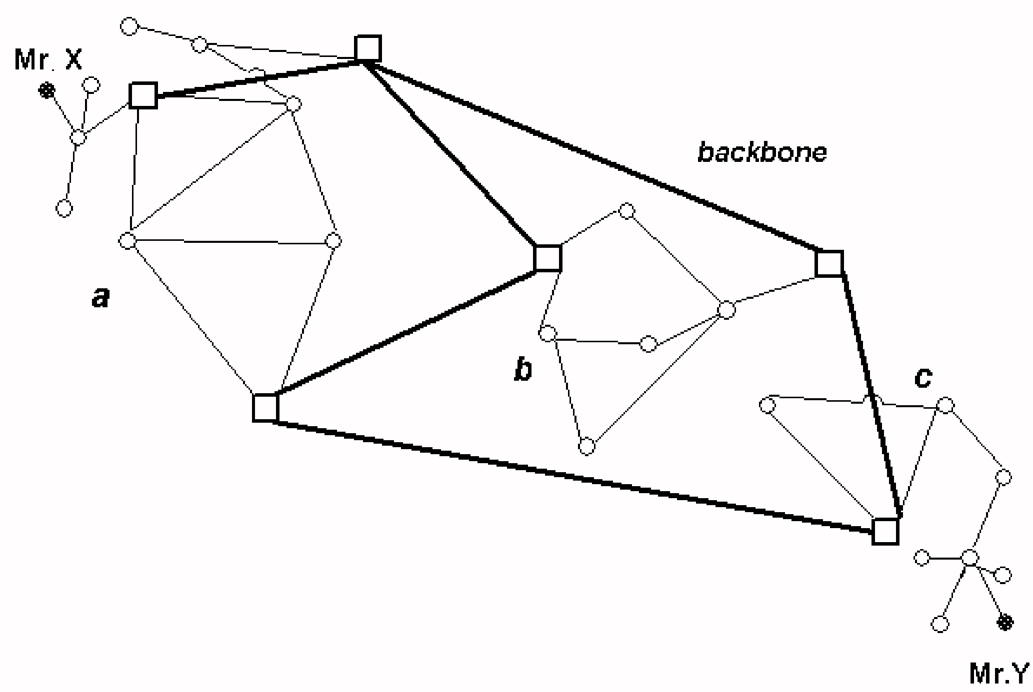


Figure 3-5

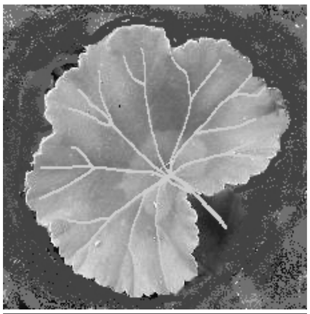
The Internet exploits odd installations existing in the world: wireless and channeled infrastructures, fixed and mobile systems, stars, linear lines and meshes. Internet crosses the planet through these resources, which can potentially reach any individual.

The Internet although cannot fulfill its duties by the mere combination of nets already in use. For example, the meshes a, b and c cover three neighboring countries. If Mr. X communicates to Mr. Y, the messages should pass through an intricate pathway in between a, b and c. Mr. X spends so much time that the service becomes rather useless.
Engineers have remedied this shortcoming by the **backbones** that link geographical networks with long-distance interconnections. In brief, they form a planetary mesh in accordance to the tenets that we have discussed. These transmission channels of high capacity carry data gathered from smaller lines that interconnect with it. The connection points are known as telecommunication data switching exchanges (DSEs).

Information is physical and this interpretation aids you once again. You can compare the telecommunications with other arrangements for traffic and flood feeder that move material items. The ensuing examples reinforce your understanding of this matter.

- o Regional streets form a mesh like the nets a, b and c.
- o Highways connect the major areas like backbones.

- o Several leaves of vegetables have star-shaped conducts because of the hierarchy of the biological components. They obey the same rules as telecommunication nets do.



PROS & CONS

LINEAR GRAPH:
- Cheap
- Unreliable

COMPLETE GRAPH:
- Expensive
- Reliable

Signals

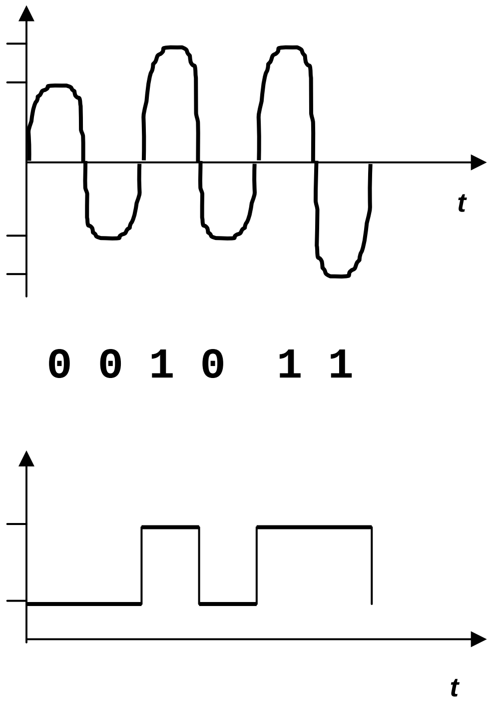


Figure 3-6

We have examined the electric bits that are **square waves**. Unfortunately these signals run through short distances. They distort and become unrecognizable when they are launched over hundreds of meters. Square waves are OK inside the computer circuits but they deform in telecommunications.

Technicians adopt **sinusoidal waves** that are more reliable than the square waves. These signals may be **analog** or **digital** in accordance to the classification of Chapter 1.

- Analog waves imitate the natural signals. For ease the output of the microphone in Fig 1-19bis absolutely looks like the sound in input.

- Digital signal make the bits 1 and 0. They are got through the **modulation,** namely the deformation of a regular wave. There are three methods:

    - **amplitude modulation**

- **frequency modulation**
- **phase modulation**

Figure 3-5 exhibits an example of amplitude modulation which deforms the sinusoidal wave along the vertical axis. If the curve lengthens, the bit is 1. The unchanged curve stands for 0.

Electronic devices handle square waves whereas channels convey modulated signals. A special interface converts the bits in two directions. The **modem** (= modulator/demodulator) performs this double function. We shall remind this appliance at the end of the present chapter.

The number of bits transmitted or received each second, abbreviated ***bps***, is the specific measure for the channel capacity. We usually adopt the higher units:

1 Kbps =1000 bps
1 Mbps = 1000000 bps

For example, telephone lines usually operate at about 50 Kbps. So-called "cable modems," designed for use with TV cable networks, operate at more than 1.5 Mbps. Optic fibers send and receive data at many Mbps.
Concluding remark: These measurements should be impracticable if the bits were abstract values!

Linguistic Remark: Technicians use a simplified jargon and call the *modulated* signals as *analog* signals. Both of them are continuous values, but there is a neat difference between them from the conceptual viewpoint.

PROS & CONS

SQUARE WAVES:

- Suitable for binary circuits
- Unreliable over long hundreds of meters

SINUSOIDAL WAVES:

- Inadequate for computations
- Very reliable in long distance.

Clients and Servers

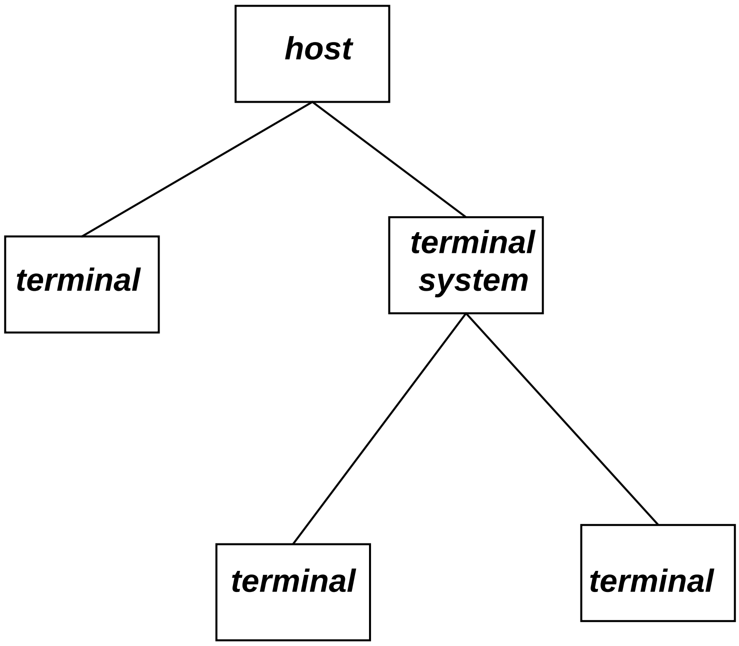


Figure 3-7

Which is the main technical characteristic of Internet with respect to other large infrastructures? What does discriminate the Internet from previous computer nets?

The units of the computer systems rank different hierarchical positions (Figure 2-6). In particular, all the peripherals depend on the CPU. The first computer networks kept this basic hierarchy illustrated in the previous chapter.
The peripherals, moved several miles away, lie under the control of the central unit that manages them similarly to the local input/output units from the conceptual viewpoint. Software programs integrate the hardware control. Such a net, today very effective and still in use, is **monocentric.** It revolves on only one computer that acts as the **host** or "owner" of the infrastructure**.** The peripherals placed all around take the reasonable name of **terminals** due to their passive roles.

If an intermediate system manages a section of the network, nevertheless it is a terminal with respect to the host. The **terminal-system** is a two-fold system as it rules over the terminals and the host controls contemporary it.

Master-Slave hierarchy allows rigid controls in the monocentric net that is star-shaped in accordance to the criteria we have introduced in the first pages.

Linguistic Remark: The master-slave nets are called *hierarchical nets* with the technical slang by virtue of their rigid authority.

Clients and Servers (contd.)

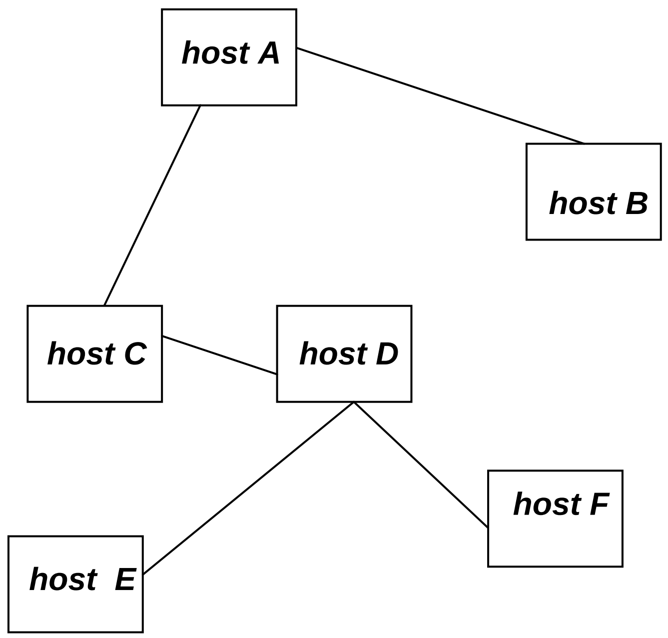


Figure 3-8

The monocentric network revolves around one main system; instead many hosts constitute the **polycentric network**. Peer computers cannot make a hierarchy and none ranks the top that does not exist.

The Internet comprises a lot of hosts and is polycentric by definition. No equipment is capable of supervising the whole system that cannot have any mechanical checkpoint either today or tomorrow. By definition the Internet hasn't any executive center and will not have anyone forever. We shall elucidate these features next in this chapter.

Hosts exchange messages in a polycentric network. In detail, the host A, requiring data, acts as a client and B, that provides information, works as a shopkeeper. In a subsequent moment B may be the client of A and their roles invert. Hierarchy still exists in the polycentric net but constraints change time and again. The Internet architecture fully complies with the **Client-Server** model. All the applications run with servers and clients, as we shall see later.

The Internet is comprised of a very high number of systems along with several sub-nets. For example, if the host in Figure 3-7 is connected to the Internet than this resource is available to all the terminals.

Clients and Servers (contd.)

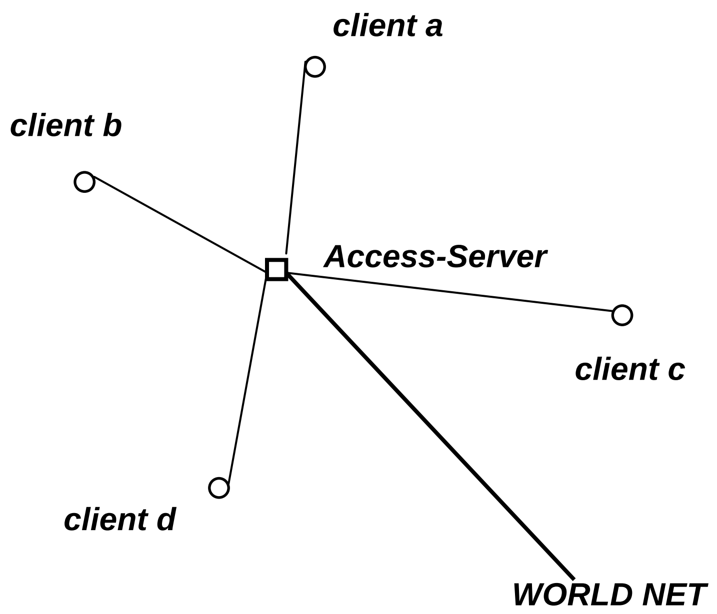


Figure 3-9

Several nodes play systematically the role of server while the number and type of clients varies. The server lies at the bottom in Figure 3-3b and works at the center of a star in accordance with our explanations. People access time and again hence connections are not rigid instead they are established through software programs.

We list the most popular applications

- Web
- E-mail
- File transfer
- News group
- Host session
- Access

And we briefly list a number of servers.

- The **web-server** shows texts, pictures and music to the *net-surfer* who visits the site.

- The **email-server** receives and sends letters in the network by means of the email boxes.

- The software experts download programs and are clients of the **ftp-server.**

- Hosts run 24 hours a day whereas an individual connects to the net randomly. The access constitutes the basic service for private users. The *provider* is the **access-server** which allows an individual to enter the Internet**.** Very frequently this host also works as an email-server and a web-server.

PROS & CONS

MONOCENTRIC NETWORK:

- It is absolutely secure since the host has the full control of the structure.
- Communication among the terminal is poor due to the centralized architecture.

POLYCENTRIC NETWORK:

- Communication is reach and living due to the client/server architecture.
- There is no systematic control. Technicians and police forces take the countermeasures against external attacks.

How Does It Work ?

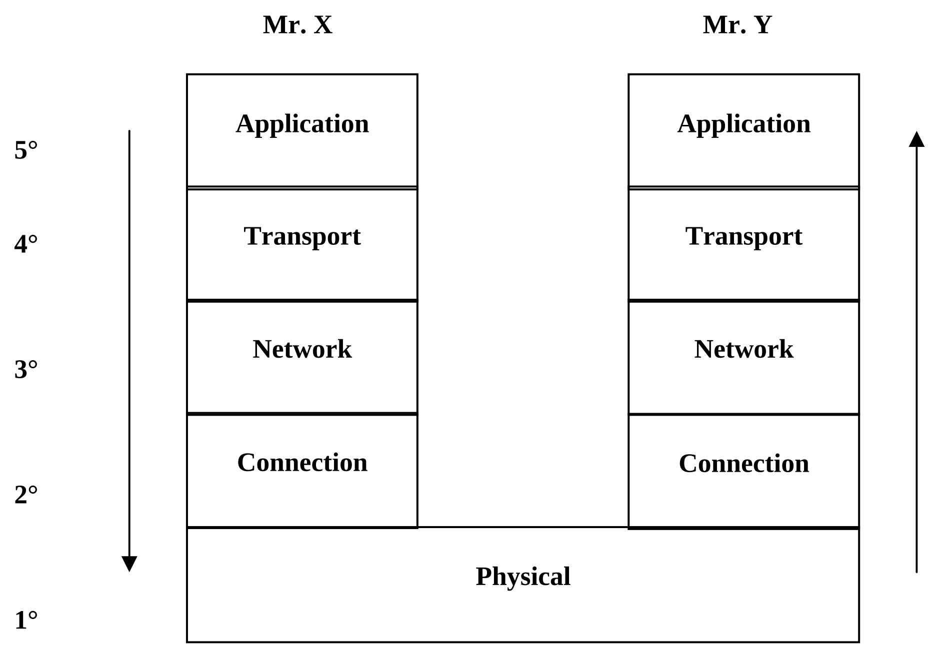


Figure 3-10

How does the Internet work?

We introduce this preliminary example which should be familiar to you.
Mr. X writes a letter to Mr. Y. His secretary envelops it and posts (figure 3-3bis). The post office closes the envelopes addressed to the town of Y in a bag and brings this to the railway station. Train transports the bag to the town of Y. The postman delivers the envelope to the secretary of Y; last Mr. Y reads the letter. We conclude that the whole system consists of two main units: the ***transmitter*** and the ***receiver*.** They accomplish similar operations in the inverse order, notably their components are symmetrical and determine the ***layers*** of the structure. Each layer checks if it is all right before starting the operations.
In case of error it merely reactivates the previous layer. This method avoids inquiries and specific investigations. Standard rules ensure the self-correction of the system. As an example, if the bag lands in the intermediate station K instead of the final station, the postal office checks the error and brings back the bag to K. The bag resumes the journey and reaches the destination through normal procedures.

Information is physical and in consequence the Internet must assume the same configuration as the postal system that delivers envelops, bags, parcels etc. The world net has to comply with the **layered model** just seen.

Experience confirms our deductions are true. The Internet is en enormous set of coupled nodes. Millions of pairs make the net to run. They cooperate in turn, for

example A-B pass the messages to B-C, then to C-D, D-E and so on up to the farthest destination. The nodes act as clients and servers because these are the key roles in the net.
The operations fall into six tiers. On top there are the humans; below the are five mechanical layers (Figure 3-10).

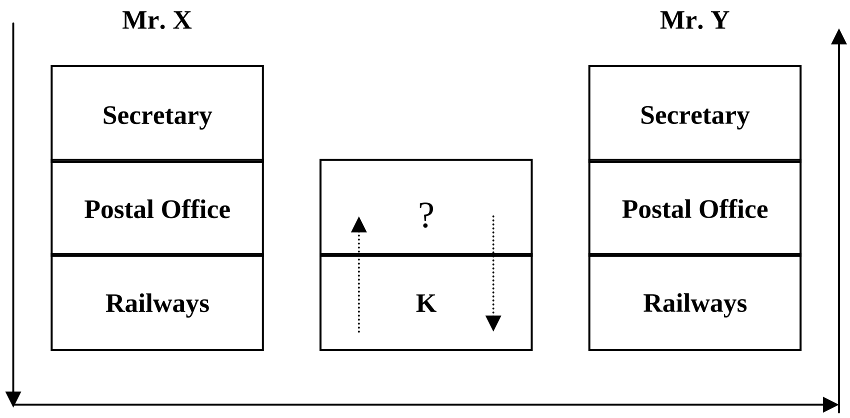


Figure 3-10bis

5° - The ***Application Layer*** receives and provides the contents to the user. For ease, the browser and the program for emailing belong to this tier.

4° - The ***Transport Layer*** manages the end-to-end transmission. It ensures the complete data transfer, for example, it determines whether all packets have arrived.

3° - The ***Network Layer*** splits the message into two or more packets of reasonable length (see Figure 3-11c). It sends the packet in the right direction to the right destination on outgoing transmission and receives the incoming packets.

2° - The ***Connection Layer*** marks the head and the tail of the packet. It manages also connections inside the local area network.

1° - The ***Physical Layer*** conveys and receives the electric signals through the network. It operates at the electrical and mechanical level.

We summarize the email application through the layer. The sender X and the addressee Y are on top in Figure 3-10. The software products such as Eudora, Lotus Notes, Outlook etc. make level 5. Layers 4, 3 and 2 consist of software products that pertain to the operating systems or to other standard packages. Cables, antennas and electronic circuit moves signals at layer 1.
E.g. the web application keeps the layers 4, 3, 2 and 1. Instead layer 5 contains the browser at the client side and the web pages at the server side. On top the client is the web-surfer; instead there is no human being in the server.

How Does It Work ? (contd.)

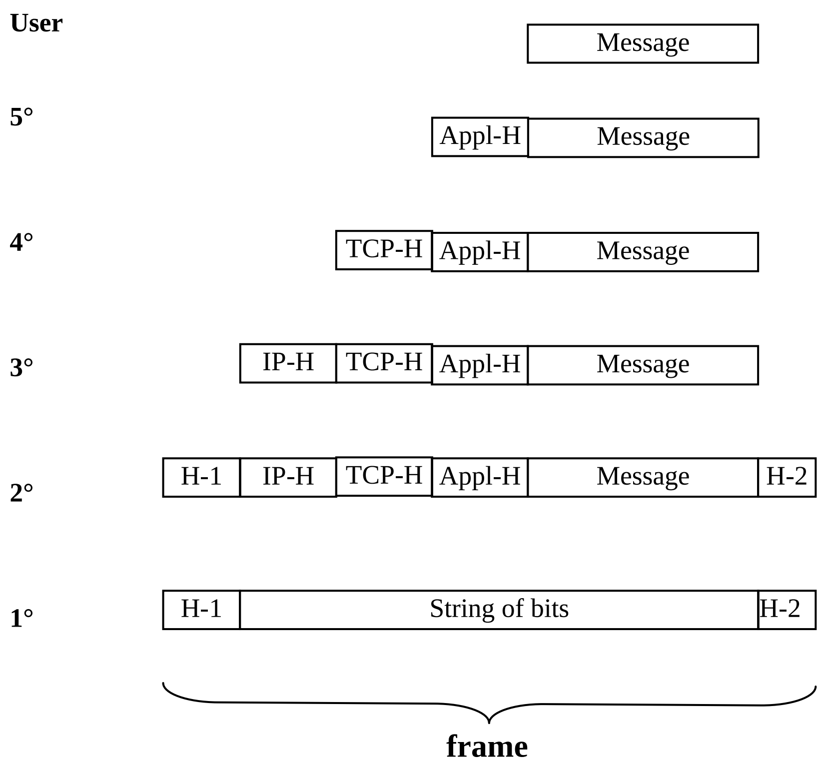


Figure 3-11

The layered model observes this rule:

The corresponding components of the transmitter and those of the receiver must manage their own data.

In particular the transmitting component appends a piece of information that the corresponding receiver checks and then cuts. For ease, the secretary of X adds the address to the letter that the secretary of Y verifies and tears.
The Internet rigidly complies with this rule. In fact, Mr. X writes the message and the five components of the node append its appropriate ***header.*** Each header contains data regarding the responsibility of the layer. As a consequence, the size of the packet increases from the upper layer to the bottom in the transmitting phase. The amount shortens into the receiving node where each receiving component checks the header prepared by the corresponding colleague and detaches it. The component passes the control to the upper unit if it is all right at the receiving stage; otherwise it resends the message back to the lower level.

The components never improvise. They conform to the ***protocols*** that are special rules and international standard. A protocol concerns one or more layers. On the other hand, a layer complies with one, two or more protocols. For example:

5° - The protocols, pertaining to level 5, establish the norms for the applications. E.g. Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) and Telnet govern respectively the web, the file transfer, the host session. Simple Mail Transfer Protocol (SMTP) and POP regulate email.

4° - The Transmission Control Protocol (TCP) and UDP belong to layer 4.

3° - The Internet Protocol (IP) is 3.

2° - SLIP, PPP, Ethernet and others rule over layer 2.

1° - The physical units obey to protocols that determine the electronic parameters of the transmission.

Which duties do the protocols fulfill?

This very complex matter goes beyond the scopes of the present book. We provide a few annotations.

1° The protocols for the physical units establish how many volts make the bits, which is the threshold, the frequency of line etc.

2° The 2nd level protocols regulate the recognition of a station inside the Ethernet or Token Ring by means of the MAC-Address. They specify how to arrange five ones at the head of the bit string and at the tail. (See H-1 and H-2 in Figure 3-11).

3° The IP header contains both sender's address and receiver's address. These data will be detailed next. IP is the method which data is sent from one computer to another on the Internet. IP states how to handle the address of each packet so that it gets to the right destination. An intermediate node on the network checks this address to see where to forward the message. Some packets from the same message may be routed differently than others.

4° IP treats each packet that travels through the Internet as an independent piece of data without any relation to any others; conversely TCP takes care of the data flow. In particular, the TCP layer is responsible for dividing the message into the packets and for reassembling them back into the complete message. For example, when the web server sends a HTML page to you, the Transmission Control Protocol program divides this page into one or more packets at the initial point. It numbers the packets, and then forwards them individually to the IP layer. At the other end-point, TCP reassembles the individual packets and waits until they complete the page. These packets frequently arrive in a different order than the order they were sent in. TCP establish how they must be put together in the right order, in fact TCP maintains the connection until such time as the messages to be exchanged by the application programs at each end-points have been exchanged.
Moreover TCP sends each message to the appropriate application when email, web, telnet etc. contemporary run.

How Does It Work ? (contd.)

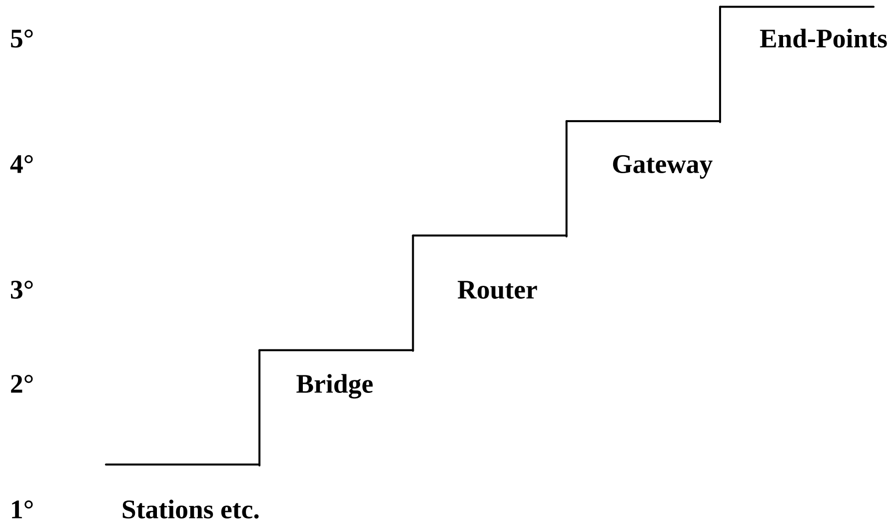


Figure 3-11

Figure 3-10 exhibits the transmitter and the receiver. The complete connection between two end-points includes several intermediate nodes. For example the node of Mr. X links the node A, this in turn connects B, and so on

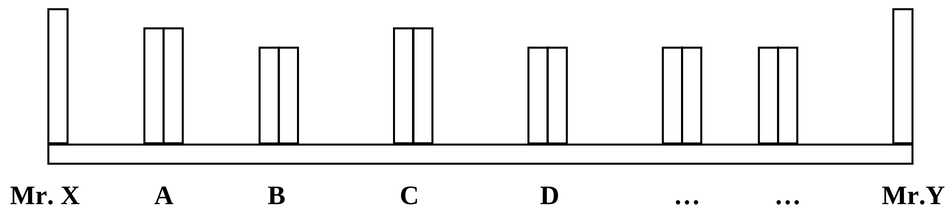


Figure 3-11a

The end points include five layers, while the intermediate nodes that fulfill less heavy duties have one up to four levels. Besides the end points, the nodes of the network fall into four classes.

Relay Station, Satellite, Modem etc. – They operate at the physical layer and are responsible for the mere movement of bits.

Bridge – This node operates at the layers 1 and 2. Take for example the sender X in the Ethernet and the receiver Y in the adjacent token-ring. They comply with two different protocols at level 2 since they operate in two diverse LAN. It is necessary to interpret and convert the headers from Ethernet to Token Ring and vice versa. Other interventions are unnecessary.

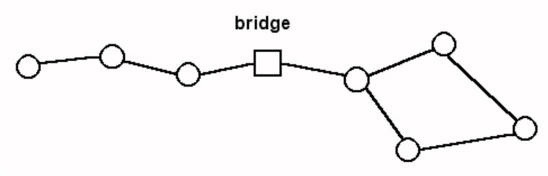


Figure 3-11b

Router – This important node works at the layers 1, 2 and 3. Take for example the end points are far away so that there are several ways to reach the receiver. Each bifurcation has a router that conveys the packet toward the most speed direction. It operates with the layer 3 responsible for addressing. Note that the IP header handles the addresses. The next figure illustrates the message of X whose host splits into three packets. Each one follows a different pathway. The TCP layer reassembles them at the receiving end-point.

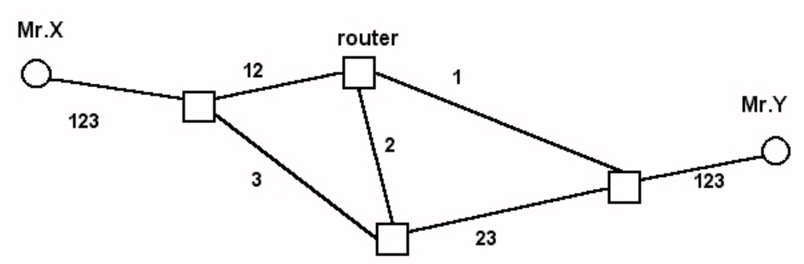


Figure 3-11c

Gateway – It operates at the layers 1, 2, 3 and 4. Take for example an end point in the Internet and the other end point inside a network, which complies with a special architecture. The messages and Appl-H (Figure 3-11) that pertain to the layer 5° remain untouched. All the other headers must be converted from the Internet protocols to the special protocols and vice versa. The gateway accomplishes this job and does not modify information at level 5.

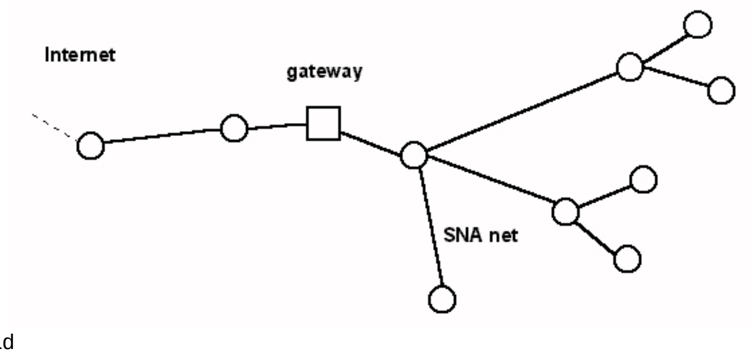


Figure 3-11d

The bridge and the gateway support special connections and are less than the others. The router emerges as the fundamental host in the Internet.

Intranet

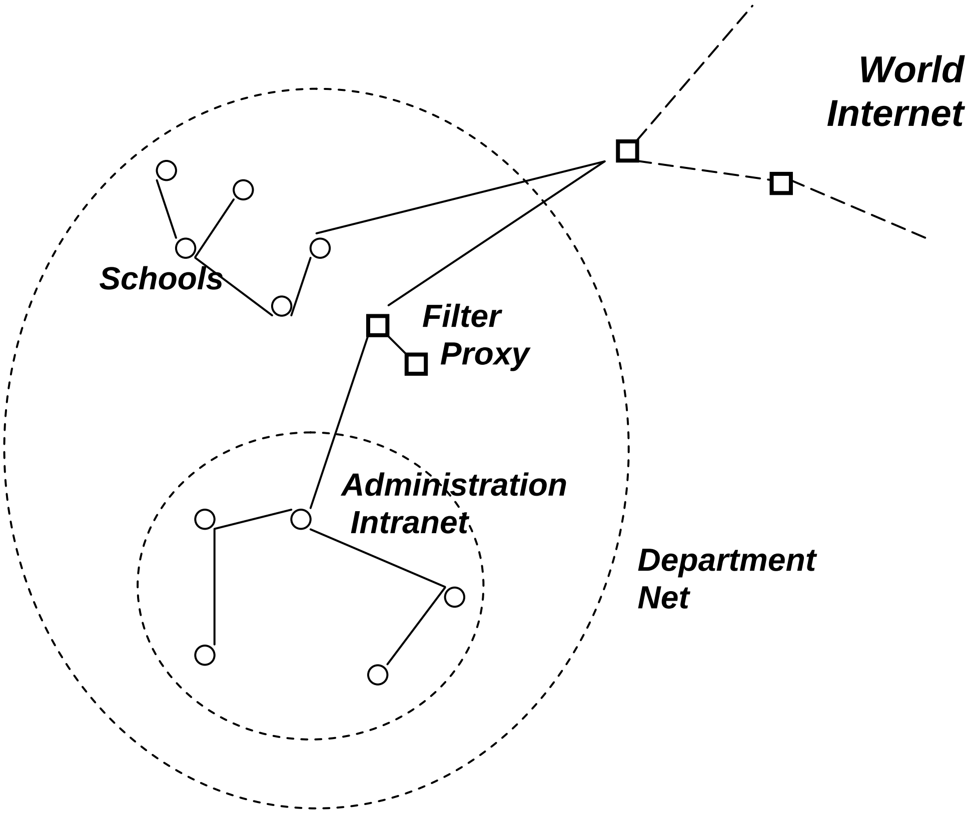


Figure 3-12

No physical device can warrant the absence of risks in the Internet. There are factual threats by humans and technical failures. Unauthorized people obtain sensitive data; others sabotage the resources of the infrastructure. E.g. a router is manipulated so that this machine becomes incapable of addressing messages. E.g. a wrecker overloads a system so that it can be no longer in use.

Companies are very responsive to hazards and protect their resources by mean of standard security countermeasures such as cryptography. Moreover they install a number of appliances capable of sheltering the corporate systems from the variety of attacks. They divide the **Intranet,** which is protected, from the rest of the world. The Intranet may be any: monocentric net or local net, an incorporation of them or otherwise a section of a net. The **firewalls** constitute its essential shelter.

Firewall is a combination of hardware units and special software programs that make the following two main servers.

- **Filters** allow only authorized traffic to pass in and out the corporate net. Only selected operators can come through the firewall that ensures secure protection to private resources.
- A **proxy** logs all the transactions and makes the data ready for investigating suspected violations.

Specialists configure the firewall in accordance to the company security policy, in practice several arrangement of units are possible. E.g. Figure 3-12 shows the protected computers in the administration whereas the firewall does not screen the machines at disposal of the students.

Internet Entities

- ***ISOC : Internet Society***
- ***IAB : Internet Architecture Board***
- ***IETF : Internet Engineering Task Force***
- ***IRTF : Internet Research Task Force***
- ***ICANN : Internet Corporation for Assigned Names and Numbers***

Figure 3-13

No mechanical appliance can rule over the Internet. No technical tool can ensure the full control today and in the years in the come because this infrastructure is a polycentric network. As a consequence, ordinary laws and institutions manage the Intranet and push those who commit criminal offences. The governments of the countries served by Internet are ruling this infrastructure but they have urgently to issue appropriate and uniform regulations. They must streamline the system of justice over the planet which is amply inadequate for the new targets.

Special technical entities, which haven't any executive power or censorship, provide a support to the effective running of the net. They accept proposals; they manage services and establish rules and standard but if someone does not stand by the commitments, they cannot intervene against him. The technical entities do not have any political authority but their support is based on collaboration and fairness of users.

First we remind the **Internet Society** (**ISOC**) that is a professional membership society founded in 1992 with more than 150 organization and 16,000 individual members in over 180 countries. ISOC operates as the international organization for global coordination and cooperation on the Internet, promoting and maintaining a broad spectrum of activities focused on the Internet's development, availability, and associated technologies. The Internet Society provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards. Among the ISOC's activities is the support of the **Internet Architecture Board** (**IAB**). The IAB supervises the **Internet Engineering Task Force** (**IETF**), which oversees the evolution of the protocol TCP/IT and the **Internet Research Task Force** (**IRTF**), which works on network technology.

IETF is a large open international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architecture. This entity values and coordinates different technical proposals that may be long or short suggestions and may be wide or narrow in scope (see next section). IETF operates through its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.).

IRTF coordinates researches activities related to TCP/IP protocols or Internet architecture in general. It gathers the research-groups working on the Internet protocols, applications, architecture and technology. The IRTF chair in consultation with the Internet Research Steering Group (IRSG) manages the whole entity. The IRSG membership includes the IRTF chair, the chairs of the various research group and possibly other specialists from the scientific community.

Last we remind **ICANN** (**Internet Corporation for Assigned Names and Numbers**) is the private non-profit corporation with responsibility for IP address space allocation and domain name system management established through subcommittees all over the world. These services were previously performed by the Internet Assigned Numbers Authority (IANA). The need to internationalize the management of the Internet (among other concerns) led the U.S. government to recommend the origin of ICANN as a global and government-independent entity. Since its beginning, ICANN has had to deal with controversial issues such as what new top-level domain names should be permitted and whether alternative root server systems should be allowed.

Internet Entities (contd.)

RFC 1812 = *Routers*
RFC 1122/1123 = *Host features*
RFC 1166 = *Logical and physical address*
RFC 1087 = *Ethics in Internet*
RFC 1244 = *Site Security Handbook*
RFC 1118 = *The hitchhiker guide to the Internet*
RFC 1175 = *For beginners*
RFC 1208 = *Glossary*

RFC 894 ⇨ ***STD 41*** = *Standard Ethernet*
RFC 1055 ⇨ ***STD 47*** = *Serial Lines*

Figure 3-14

The Internet Engineering Task Force directs the ensuing documents:

Request For Comments (RFC) = Procedures under examination
Standard (STD) = Standards and various regulations
For Your Information (FYI) = Very common documents

Request For Comments follow some steps. For ease, a producer requires the opinion of IETF on a new solution that may be any: a hardware device, a software program or a procedure. The committee examines the document which is **elective** for utilization in the Internet. RFC is openly accepted, or accepted for a restricted usage or refused after the IETF examination.

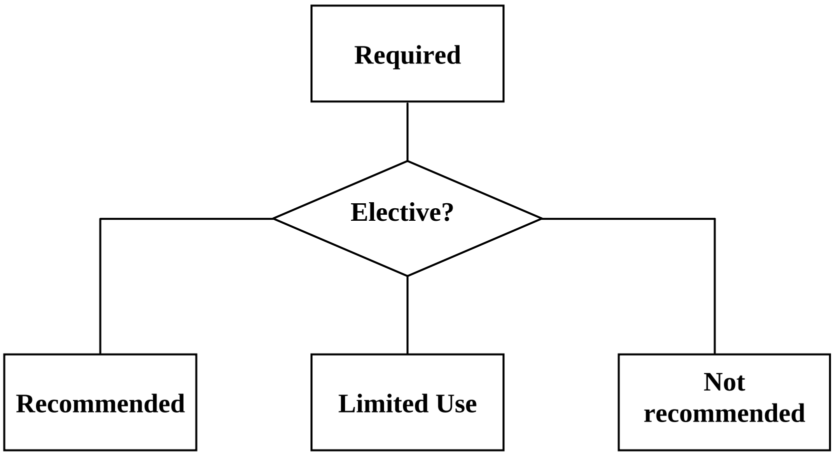


Figure 3-14bis

As examples, we list the ensuing Request for Comments:

RFC 1812 = Routers
RFC 1122/1123 = Host features
RFC 1166 = Logical and physical address
RFC 124 = Site Security Handbook
RFC 1087 = Ethics in Internet
RFC 1118 = The hitchhiker guide to the Internet
RFC 1175 = For beginners
RFC 1208 = Glossary

RFC, if accepted by IETF, can become an Internet Standard (STD). For example:

RFC 894 --> STD 41 = Standard Ethernet
RFC 1055 --> STD47 = Serial Lines

Internet Entities (contd.)

Physical Address

bit *0 8 16 24 31*

10000000011011010000000111111111

128 109 1 255

128.109.1.255

Logical Address

ima.cnr.it

Figure 3-15

A host runs all over the day. It is always available and ICANN assigns the **physical address** to it for identification purposes. Technicians usually write the 32-bits address as four numbers. In fact eight bits correspond to a decimal number ranging between 0 and 255.

Four numbers are easier to handle than 32 bits. For example, compare this string

10000000011011010000000111111111

With the corresponding four numbers

128.109.1.255

Notwithstanding this reduction, people prefer the use of words in natural language and the host has assigned the **logical address** too. This is subdivided into two, three or more parts. The first section on the right side encodes the largest **domain** to which the host belongs. Two alternative criteria qualify this domain:

- **National** (E.g. **it** =Italy, **f** = France etc.)
- **Sectional** (E.g. **com** =company, **edu** =school, **mil** =military etc.)

The second section of the logical address reports a domain smaller than the first domain, such as the name of the company. The third exhibits the branch of the company and so on toward the subtlest grouping. E.g. the logical address in Figure 3-12 tells the host is Italian, it belongs to the national research center CNR and, in detail, to the institute IMA.

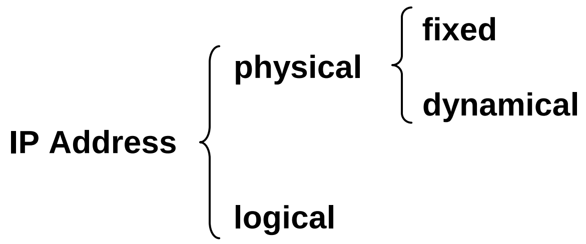


Figure 3-15bis

The IP address is double and man prefers the logical version whereas devices run with physical addresses. Special units provide the translation from the logical address, written by humans, to the physical one necessary to machines. Special **name-servers** perform this task, which is systematic and essential to effective operations in the Internet. People, even if they are unconscious, are clients of the name-servers that are scattered all over the world. An example can clarify this organization. Mr. X emails to Mr. Y thanks to the assistance of the name-server that is close to Mr. X and provides the correct binary address in return for the logical address. If this server has not the required physical address, it calls for support from the closest name-server. If it is also out of the needed codeword, in turn it asks the next server. At worst the name-server of Y provides the keys for conversion.

Hosts run day and night and have the **fix IP address**. Instead occasional users who access random the net do not need a definitive address. The access-server, named as “provider”, assigns a provisional binary address, which is valid only during the connection. When people disconnect, they release the address. Different occasional operators share the same address in the space of the day and we call this value as **dynamical address.**

Legal Principles

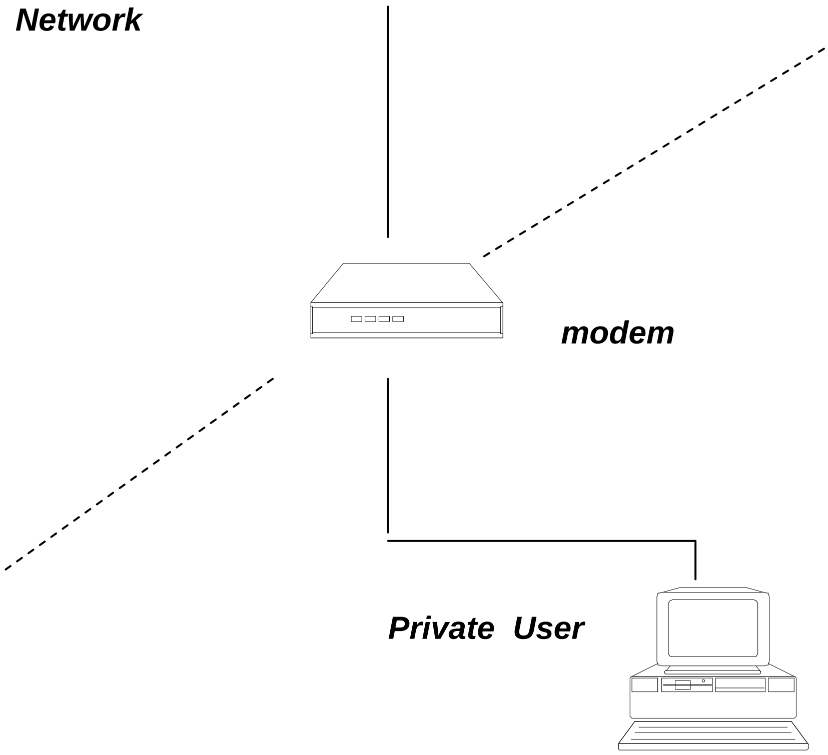


Figure 3-16

National administrations helm human operations in the Internet through ordinary organs such as laws, police offices, courts of law etc. They have to promulgate new rules and to uniform those in use, but they are behind with this duty.

Nevertheless these deficiencies some legal tenets have been adopted since decades. We comment on two of them.

I) - Since the Roman age, a legal principle establishes that an infrastructure (e.g. a road net, a river net) cannot be the exclusive property of an individual since he could win an exceeding power. Thenceforth a state executive office manages a broad infrastructure. Telecommunication networks stick necessarily to this rule.
The state interference threatened the development of electronic technology around the middle of the twentieth century. The officialdom caused delays and

pushed the birth of the movement for *deregulation*. The legal principle was obviously kept but the intervention of the State reduced progressively. Now private business manufacture and sell innovative equipment without bureaucratic hitches. Companies can manage computer networks too, under the government supervision.

II) – Privates' devices and the network belong to distinct owners and we wonder: Where is the border of these belongings?

A technical feature suggested the correct solution.
Bits running in the net differ physically from those running into the appliances. The modulated waves and the square waves are capable of defining the line of properties. The **modem**, that converts the signals, demarcates the boundaries. Experience confirms the special focus on modems. Electronic engineers could reduce this device to a rather invisible chip; instead the modem is much hugger. It makes evident the boundary between the properties.

How Internet Boosted

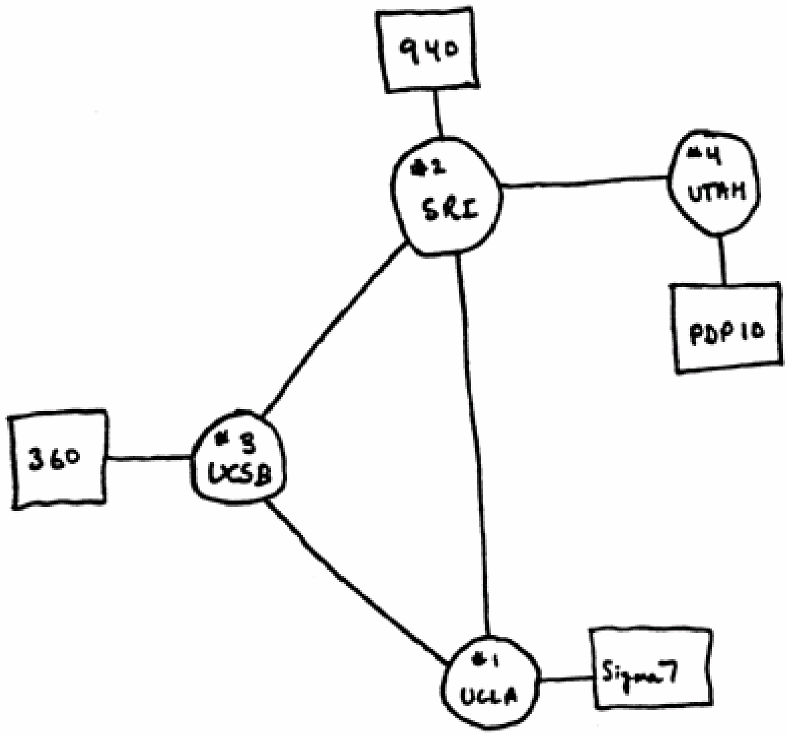


Figure 3-17

In the fifties, high-ranking officers grappled with the problem of making computer systems secure so that appliances could not be targeted and disabled in nuclear attack. They searched for solid solutions and began to build bunkers.

Reinforced concrete soon appeared ineffective and the US Department of Defense contracted out a study on the protection of military sites. Redundancy is the key to successful security of information and the scientists designed a network connecting four sites with the complete mesh (Figure 3-17). The four computer systems were capable of cooperating unless all the links were destroyed. The seeds of the Internet had been planted.

In 1969 this experiment, administered by the Advanced Research Projects Agency, became known as the ARPANet.

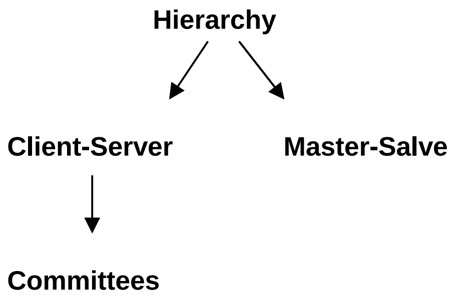
Mounting cooperation with universities improved this telecommunication infrastructure. So many non-military users interconnected that in 1983 the resource split into Milnet, strictly military, and **Internet**, the huge and civil network.

The term ‘Internet’ was the exact definition of a net working on the basis of TCP/IP protocol. Email, Ftp, Telnet, Web and other successful services exploded at successive stages. At the dawn of the third millennium the Internet covers all over the world and assists tens millions of peoples.
Why these historical notes?

History tells that none technical wizard suddenly pulled out the Internet. This huge infrastructure is a scientific product implemented step by step during about four decades. The Internet boomed in the nineties thanks to this prolonged and demanding implementation.

Unit 3 Summary

We have introduced the main features of telecommunication. We have justified the channels, the signals, the geometric configuration etc. The concept of hierarchy elucidates how the Internet is a polycentric structure.



We have discussed a number of consequences derived from a few simple tenets.