INTERNATIONAL ATOMIC ENERGY AGENCY
UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY, CABLE: CENTRATOM TRIESTE

The United Nations University

SMR/774 - 21

THIRD COLLEGE ON MICROPROCESSOR-BASED REAL-TIME CONTROL - PRINCIPLES AND APPLICATIONS IN PHYSICS
26 September - 21 October 1994

LOCAL AREA NETWORKS-LAN's

Abhaya S. INDURUWA
Dept. of Computer Science & Engineering
Faculty of Engineering
University of Moratuwa
Moratuwa
SRI LANKA

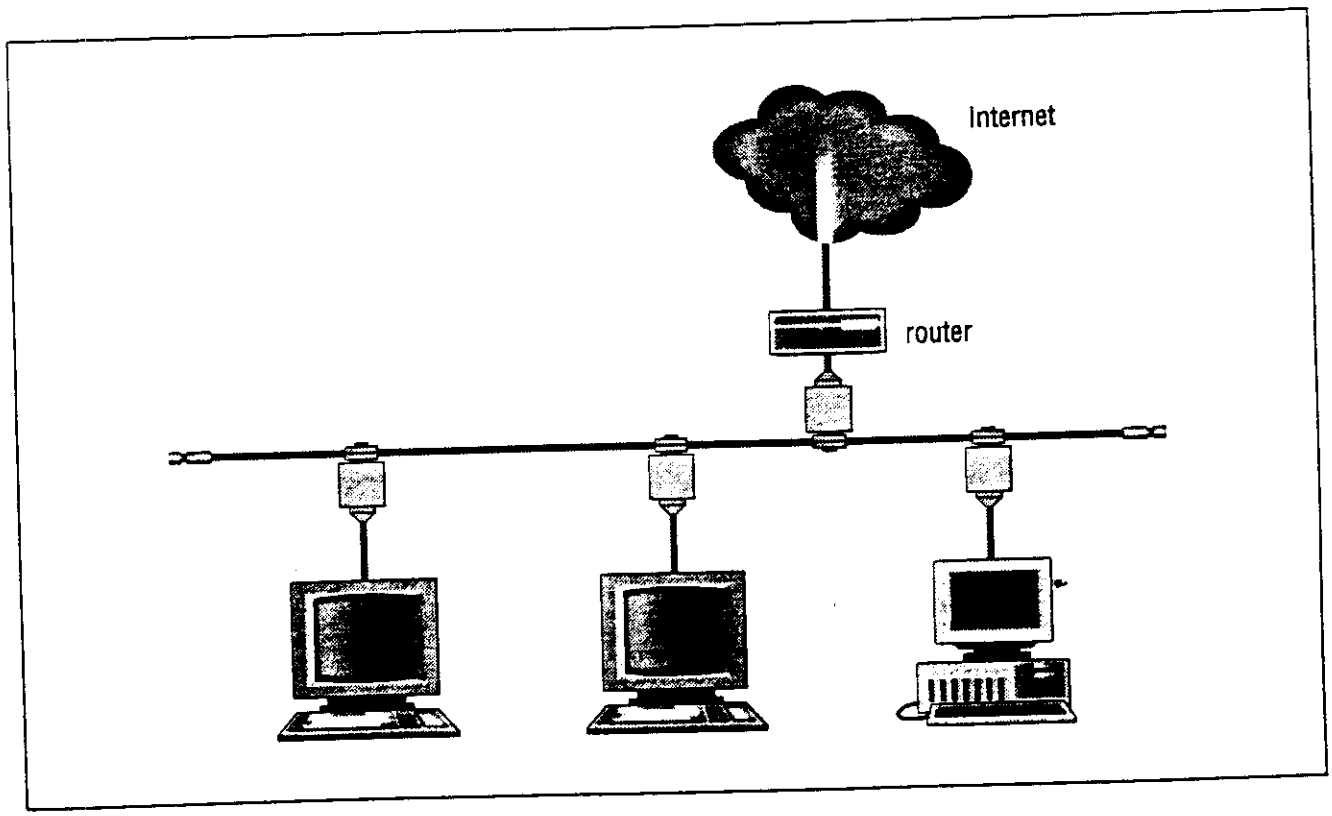
Networks (3)

Local Area Networks - LANs

Local Area Networks (LANs)

A network interconnecting computer equipment spread in a **small geographical area** is called a LAN. The interconnection is based on links which support a reasonably high bandwidth (10 ~20 Mbps range) to a relatively high bandwidth (100 Mbps). One of the characteristic features of a LAN is that it is ***almost*** completely under the local control.

A LAN by itself is not very exciting. It is more useful if LANs in a single premises are interconnected. The next step then is to open your network into the world, thus becoming a part of the world wide network. This type of networks are known as Wide Area Networks (WANs). The most useful WAN for scientists and researchers is the Internet.



Components of a LAN

Components of a LAN

A LAN comprises:

- access points (PCs, workstations or just dumb terminals!)
- network server/s (reasonably sized PC or a WS)
- network interfaces (or terminal servers)
- network cables and other accessories (transceivers, etc)
- network routing equipment (bridges, routers, etc)
- networking software.

Network server

Most network operating systems require a dedicated server. A **reasonably configured PC or a workstation** can be used as a network server. Care must be taken in selecting a suitable one as bottlenecks in the server configuration can be the cause for problems in many networks.

Some of the points that should be considered in selecting a server are:

- the type of **internal bus** used in PCs (ISA, EISA, VL, PCI, etc) or the data rate of the bus in the case of WSs
- the disk **access time** (controller !). The capacity of the disk is not a serious problem these days.
- the **input/output bandwidth** of the disk controller (how many Mbps ?) **SCSI II** *aka* **fastSCSI** is a good choice.
- the **capacity and the speed of memory** on the server (8 - 16 MB is usual).

In the case of PCs and WSs, specially configured machines are available for use as network servers. These are obviously more expensive than an ordinary PC or a workstation. However, an ordinary PC or a WS should serve the purpose of a server for a start.

Network topology and Network Interface Units (NIUs)

The selection of the NIUs depends on the topology used. The most popular networking technologies are based on the **bus** and the **ring topologies**. The following are the ISO recommended protocols used in these topologies.

ISO 8802/3 (IEEE802.3)	**CSMA/CD** protocol for bus topology (Ethernet !!)
ISO 8802/4 (IEEE802.4)	**Token passing** bus
ISO 8802/5 (IEEE802.5)	**Token passing** ring
ISO 8802/6 (IEEE802.6)	**FDDI** (ring topology)

The early protocols for star topologies, such as ARCNet, have not been recommended by the ISO. The use of **hubs in a bus** topology allows some form of a star configuration. The ATM technology, when commercially available, will offer a solution for star topologies in LANs.

Bus topology

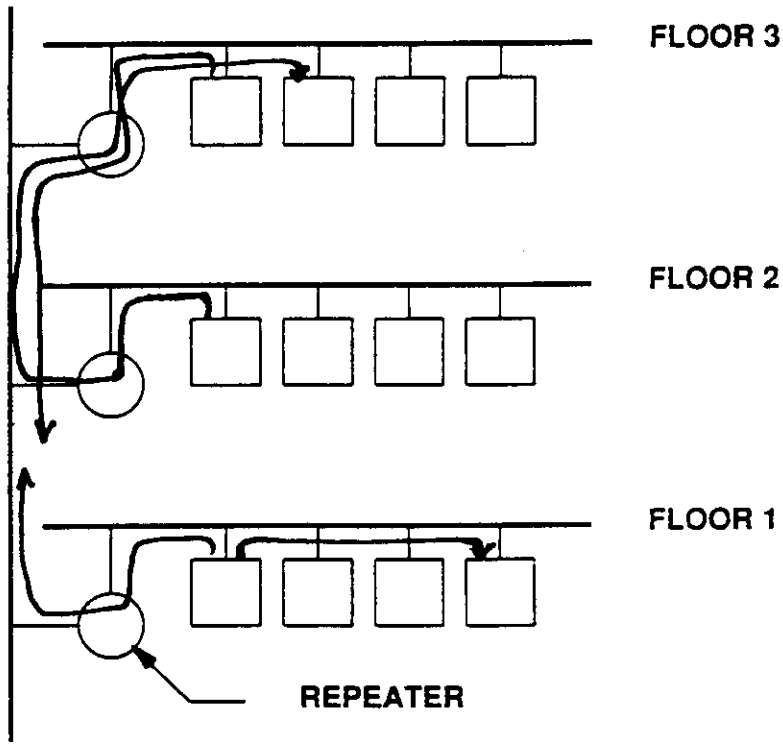
By far the most commonly found topology in local area networks is the bus topology based on **CSMA/CD (Carrier Sense Multiple Access/ Collision Detect)**. This is based on the early work of Digital, Intel and Xerox and is often referred to as the Ethernet™ topology and protocol. The nominal data rate on a CSMA/CD network is 10 Mbps. However due to the contention arising out of two or more stations asking for the network bandwidth at the same time, the maximum throughput is in the range of 30 - 40 %.

CSMA/CD Protocol

This protocol is almost always related to the bus topology. It works on the principle of contention.

When stations attached to the network are not transmitting they listen to the network (hence **carrier sense**). When a station has to transmit it puts the information on the network when it finds that the network is not busy.

When no station is transmitting all stations will have an equal chance to access the network (hence **multiple access**).



If two stations try to transmit together there will be a collision which the network electronics will detect (hence **collision detect**). When this happens the stations involved in the transmission will stop and wait for a random time determined by the network interface on the machines before attempting to retransmit. CSMA/CD uses a binary exponential backoff policy to avoid the same pair trying to transmit together again.

This is the reason for low throughput on the CSMA/CD bus networks and also why a response cannot be guaranteed within a specified time.

CSMA/CD Frame Format

Preamble	Destination Address	Source Address	Frame Type	Frame Data	CRC
64 bits	48 bits	48 bits	16 bits	368-12000 bits	32 bits

The CSMA/CD frame (packet) format

CSMA/CD uses physical addresses in its frames. A 48 bit unique address is given to each NIU. This allows 2^{48} or 256 x 10^{12} physical addresses (not a lot !!). The NIU manufacturers are given a block of addresses and the recovery of unused addresses is difficult.

CSMA/CD frames are of variable length. Each frame will contain the **physical source address** and the **physical destination address**. The *preamble* is a sequence of 0 s and 1 s to achieve synchronisation and the *cyclic redundancy check* is to detect errors. The ***frame type field*** contains a 16 bit integer that identifies the type of the data being carried in the frame. When a frame arrives at a machine the **operating system** uses the frame type to determine which software module should process the frame. Due to this feature CSMA/CD frames are called self identifying frames. The self identifying frames offer the following advantages:

- allow multiple protocols on a single machine
- allow multiple protocols to be intermixed on the same physical network without interference.

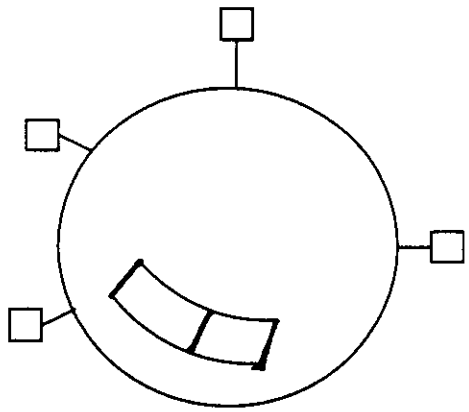
On the other hand Internet uses a 32 bit address to locate a machine depending on its geographical location. This is called domain type addressing. There is a set of IP protocols (ARP and RARP) which will allow the mapping of physical addresses to IP addresses.

Ring Topology & the Token Passing Protocol

An example of a network based on ring topology is the IBM Token Ring which is rated to run at 16 Mbps. The token passing protocol works on the principle of passing a token round the ring. When the token reaches a station and if it is empty, the station can fill it with data and mark the token full. As the token passes through the ring, the other stations will look at the destination address and will copy the data to the station only if its own address matches with the intended destination address. The token is then returned to the sender with the data and the sender will pass the token to the next station after making the token empty.

To give an equal chance for every station to transmit, the protocol does not allow the same station to grab the token immediately after releasing. If a station does not wish to transmit when the token reaches it, then it will simply pass the token to the next station.

One station on the network is designated as the supervisor which will be used to reconfigure the network and also to generate a token if the token is missing.



Token passing protocol

Unlike in the case of CSMA/CD protocol, there is no contention in the token passing protocol architecture and hence it guarantees a response within a specified time. Therefore in applications where a

response is required within a specified maximum time, a token passing ring protocol is appropriate.

In the selection of the NIU (also called the MAU (Medium Access Unit)) the following aspects must be considered.

- the data width of the card (8 bit, 16 bit or 32 bit; specially important for the server).
- the buffer size on the NIU.
- the supported types of cable connections (sockets for 15 pin AUI cable, thin wire BNC, TP; some cards support all three at a marginally higher cost).
- the availability of network drivers for various protocols.

Almost all workstations and most PCs (especially if they are configured as servers) are sold with a built in network interface unit which supports CSMA/CD protocol.

LAN Cabling

Today a CSMA/CD based LAN can be wired using any of the following cable types. The cable segments are appropriately terminated to avoid reflections of the signals at the cable ends.

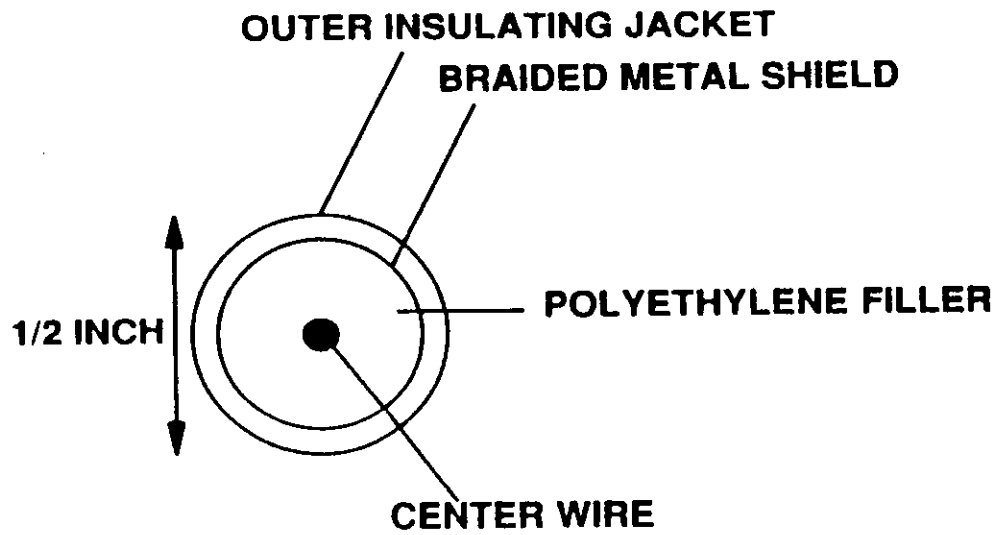
- Thick Wire Coaxial Cable (10 base 5)
- Thin Wire Coaxial Cable (10 base 2)
- Twisted Pair (UTP or STP) Cable (10 base T)
- Optical Fibre Cable (10 base FL)

In addition to the above, telephone links (very slow speed 2.4 Kbps - 28.8 Kbps) or dedicated data circuits (64 Kbps and above) using land lines or radio technology (HF, micro wave or spread spectrum) can be used to interconnect LANs.

Cable types

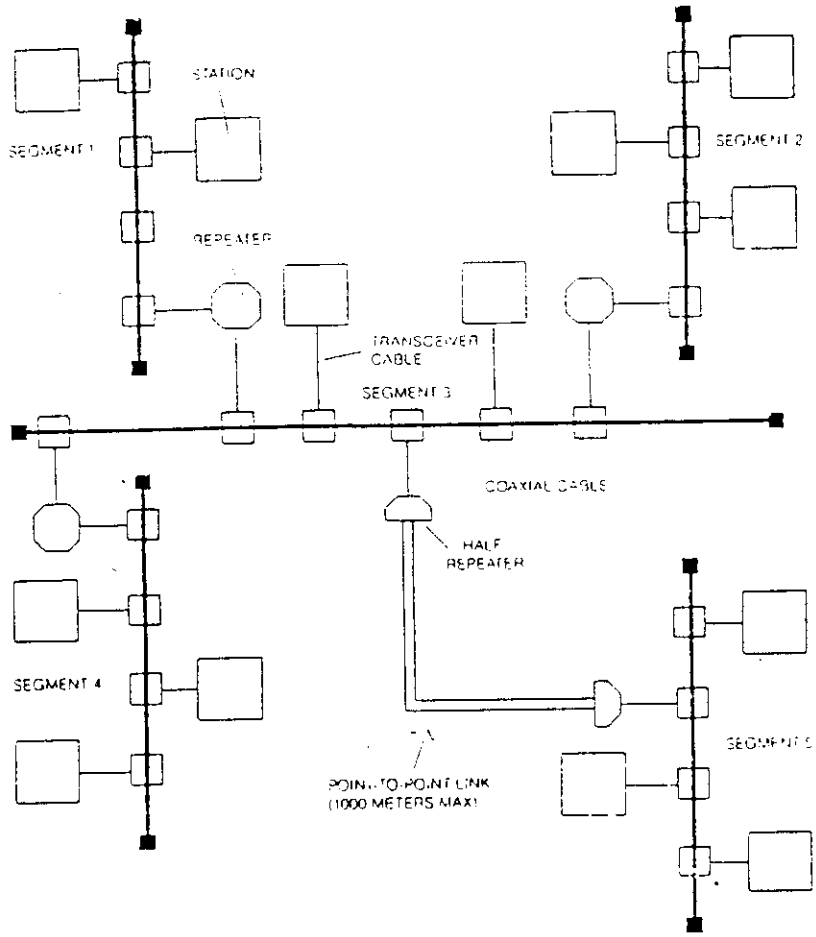
Coaxial cables

ISO standards detail two types of coaxial cables for wiring LANs namely the **thick wire** and the **thin wire**. Historically the thick wire has been used in the Ethernet™. In fact the Ethernet standard specifies even the colour of the coaxial cable used in thick wire Ethernets.



Coaxial cables used in LANs

Thick wire coaxial cables are robust in construction, heavy and are expensive. They have bandwidths up to about 500 Mbps although in the Ethernets they are only running at 10 Mbps. Thick wire is more suitable as **back bone** cables. The CSMA/CD standard specifies a maximum length of 500 m in one thick wire segment. Upto 5 segments can be connected with no more than 2 repeaters between a pair of communicating machines. These limitations are basically due to the signal attenuation in cables.



The thin wire coaxial cable is less expensive, flexible and easy to handle. They are more suitable for internal wiring for eg. in a laboratory or in an office. In a CSMA/CD network they have a maximum length of 200 m in one segment. One of the problems in using thin wire is that a disconnection in the middle can cause the entire segment to be out of service. Since the cable runs are difficult to locate, trouble shooting and repair is difficult.

Twisted Pair

This is derived from the familiar cables for telephone wiring. They come in two flavours namely, **Unshielded TP (UTP)** and **Shielded TP (STP)**. STP is more expensive but is suitable for environments which are affected by EM/ RF interference. The TP cables use a snap on plug and socket (RJ45 which is similar to the RJ11 socket used in telephones). If used on a CSMA/CD they can be used up to 100 m

from the hub. Unlike in the case of thin wire, a disconnection in a single TP cable will not affect the operation of the others connected to the same hub.

Optical Fibre

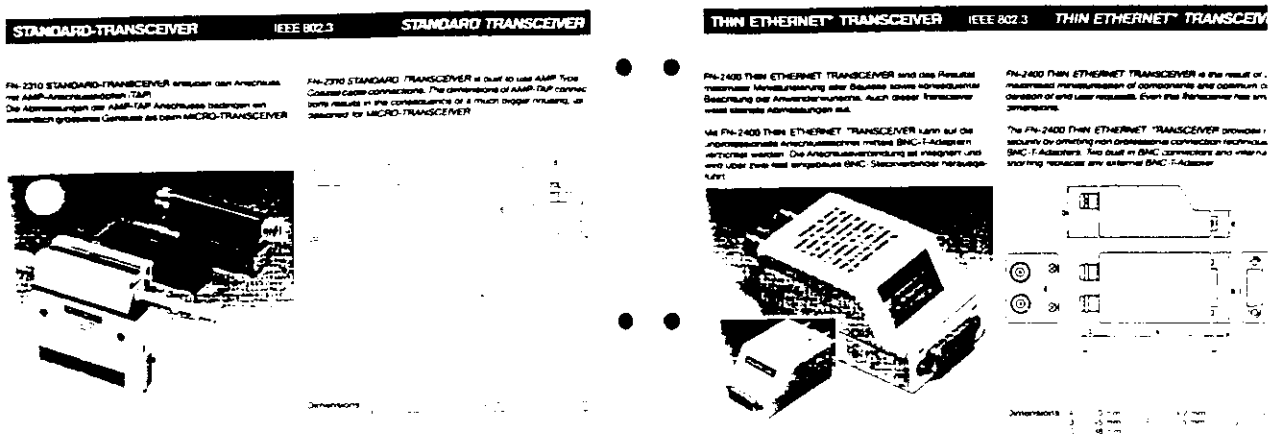
Useful in interconnecting different buildings. Particularly useful when the interconnections have to be done in the open and the **risk of interference and damage due to lightning is high**. Since optical cables carry light signals they are completely immune to interference from electromagnetic / radio frequency signals and lightning. They can support very high data rates (in the Gbps - Tbps range) with very low attenuation (hence larger distances between repeaters) and low bit error rates. On many good quality optical cables a BER of 10^{-12} is typical.

The major problems with the optical cables are two fold. Firstly it is difficult to tap or join. This is also an advantage since it is difficult to do unauthorised tapping. Secondly the repeaters are still costly because they go through an optical/electrical/optical signal conversion at each repeater. The availability of optical repeaters are expected to solve this problem. On the whole optical fibre cables are more expensive to buy and also to lay.

Other Components in a CSMA/CD LAN

In a small LAN based on coaxial fibre the stations will be connected to the network through a **transceiver** which will allow the traffic to flow from the station to the network and vice versa. Different types of transceivers are available depending on the type of cable and the interface connection selected.

For twisted pair connections a multiport hub is used.



Networking software

The following networking software is popularly found in LANs.

Novell Netware (version 4)
Banyan Vines (version 5.5)
TCP/IP based products for UNIX based servers.

Novell and Banyan Vines are commercially available network operating systems (NOSs). While Novell has found its place mainly in the office environment, Banyan Vines can support **enterprise wide networking**; in other words wide area networking.

TCP/IP is not a **complete network operating system.** It is a networking utility which is usually available in UNIX systems. TCP/IP is also the networking protocol on which the world wide Internet is based. Therefore the use of **TCP/IP in the LAN will allow seamless integration** of the local resources into the global network.

Both Novell and Banyan Vines network operating systems provide gateways to TCP/IP based networks. Most of the network interfaces have drivers which allow them to carry traffic based on multiprotocols. This way a network based on Novell or Banyan Vines can be made to carry IP traffic.

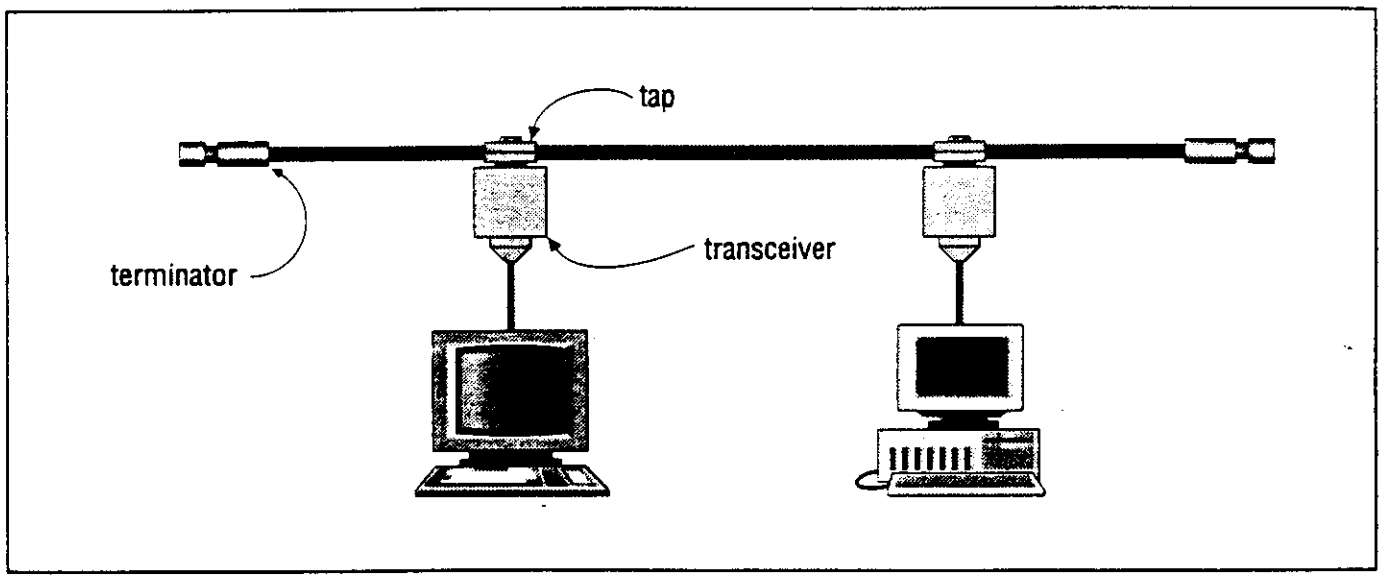
Building Networks

Where do you start ?

The answer depends on what you want to do with the network and what you already have. In any case it is worth trying to understand the available technologies and what they can offer you. The choice of a particular technology will depend on how much money you have !!

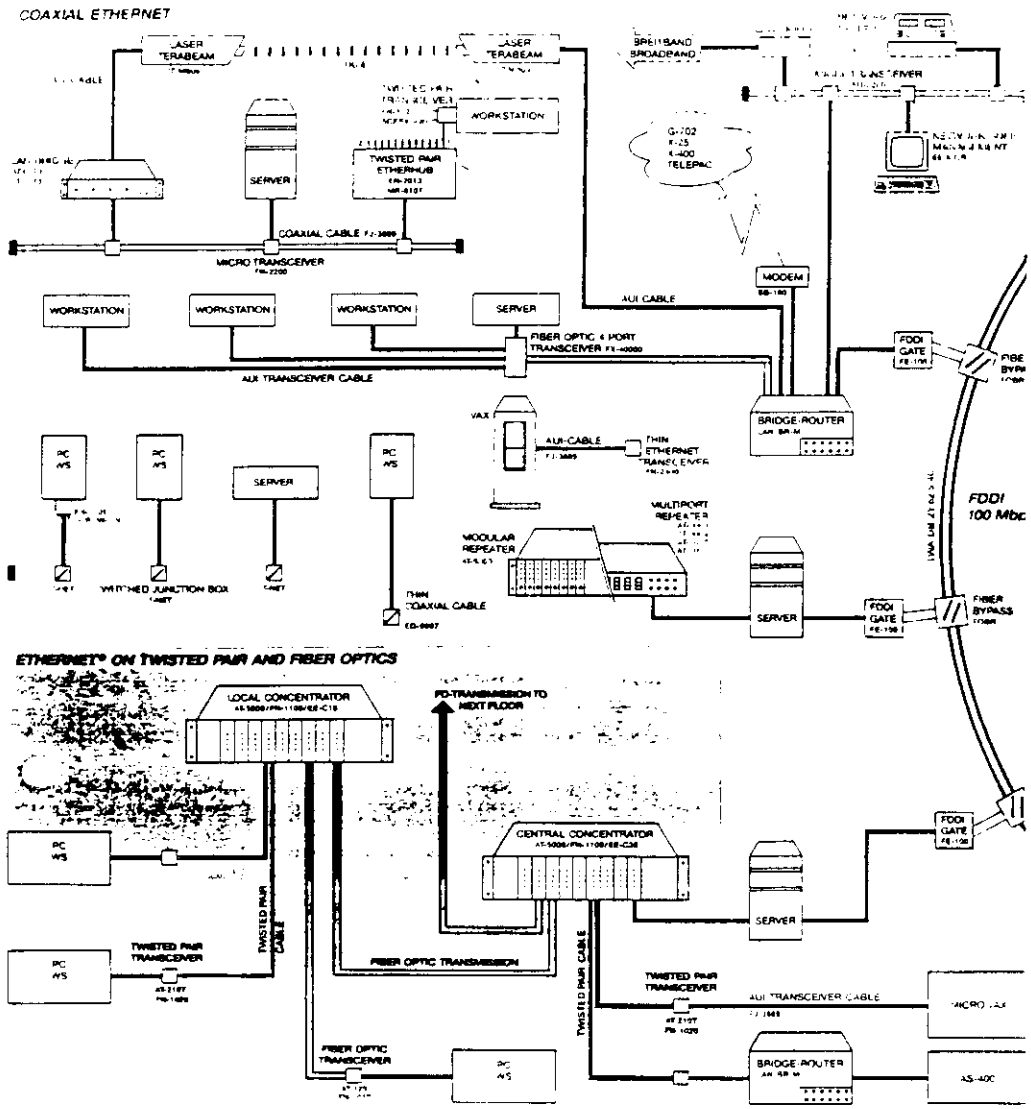
Linux is an operating system complete with full TCP/IP support and hence is **an ideal choice**. You will not need the full linux to do this!!

From the hardware point of view a single segment Ethernet as shown here can be implemented.



This is perhaps the smallest network you can build, but it is not very cost effective specially when you have spent a great deal of money for the server. To make it cost effective you may want to add more access points and even extend the network. This is the starting point. **Now you are beginning to grow**.

In contrast to this the configuration shown below is a much more complex network. Building such a network and operating same is not so easy.



In addition to the basic components we have seen so far we have to now look at others which will help you to grow gracefully.

CSMA/CD Bridges

Bridges are used to interconnect segments. A **bridge replicates packets (or frames)** while a **repeater replicates electrical signals.** This way a bridge can filter noise, errors and malformed frames and hence is superior to a simple repeater.

A bridge is essentially a fast computer with two network interfaces and a fixed program. It captures a **valid frame** (therefore you need to process) arriving on one segment and delivers it to the other and vice versa. Furthermore bridges understand CSMA/CD rules so collisions and propagation delays on one segment remain isolated from those on the other.

In view of these features the use of a bridge is highly recommended in connecting two segments together even though it is more expensive than a repeater. Since the bridge hides the details of interconnection a set of bridged segments acts like a single segment.

Today most bridges can make intelligent decisions about which frames to forward and which ones to block. These are called **adaptive or learning bridges.**

An adaptive bridge maintains two address lists, one for each network interface. This helps the bridge to learn which machines lie on each segment.

When a packet arrives at the bridge it first examines the source address and adds it to the corresponding list if it is not there. Later when a packet destined to this address arrives at the bridge then it will know on which segment is the machine. This will help to reduce unnecessary traffic flow in the segments.

The learning process of the bridge is automatic. It is not necessary to program the bridge with specific addresses. The filtering feature of a bridge can be used to improve the performance of an overloaded network, because the bridge essentially partitions the network.

Both repeaters and bridges are transparent to the computers on the network because they do not do any routing.

On power up a bridge will check for the presence of other bridges and learn the topology of the network. This is very important as otherwise multiple copies of a broadcast message sent on the segments can be catastrophic.

IP Routers

The interface from your network to the outside IP network is always through a router. A router (as the name implies) is a computer which will route IP packets using IP destination addresses. For this purpose routing tables are used in the routers which will try to route traffic using the **shortest path first**.

In networks which handle more than one protocol the routing device has to understand each protocol used. For this purpose there are devices which are called multiprotocol routers.

Multimedia hubs

When a network is built using different types of cable technologies, for example, twisted pair and optical fibre, the cables can be terminated in a single hub. This type of hub will have ports which will handle different types of transmission media and hence are called multimedia hubs.