LECTURE 2

1.6. LAN Topology

Most computers in organizations connect to the Internet using a LAN. These networks normally consist of a backbone which is a common link to all the networks within the organization. This backbone allows users on different network segments to communicate and also allows data into and out of the local network. Figure 7 shows a local area network which contains various segments: LAN A, LAN B, LAN C, LAN D, LAN E and LAN F. These are connected to the local network via the BACKBONE 1.Thus if LAN A talks to LAN E then the data must travel out of LAN A, onto BACKBONE 1, then into LAN C and through onto LAN E.

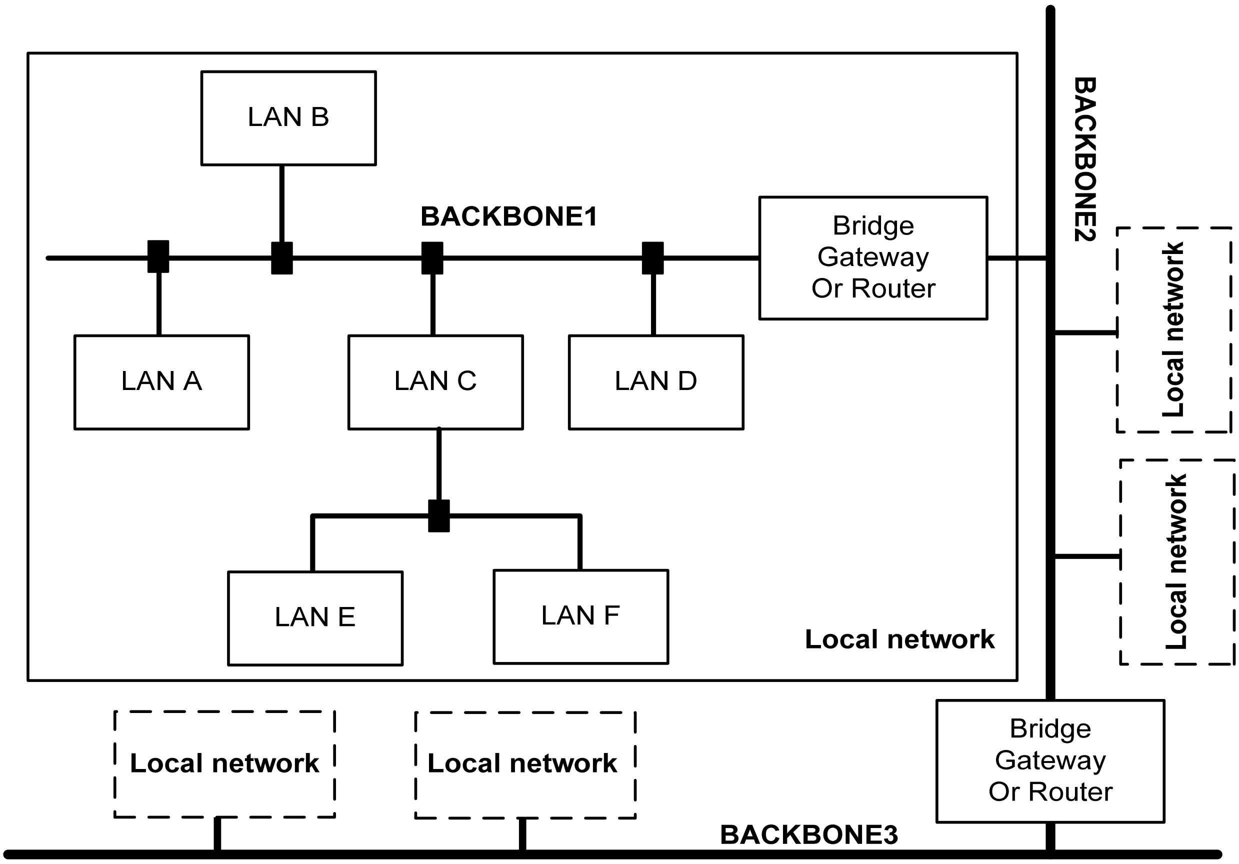


Figure 7. *Interconnection of local networks*

Networks are partitioned from other networks with a bridge, a gateway or a router. A bridge links a network of one type to an identical type, such as Ethernet, or Token Ring to Token Ring. A gateway connects two dissimilar types of networks and routers operate in a similar way to gateways and can either connect to two similar or dissimilar networks. The key operation of a gateway, bridge or router is that they only allow data traffic through that is intended for another network, which is outside the connected network. This filters traffic and stops traffic, not intended for the network, from clogging-up the backbone. Most modern bridges, gateways and routers are intelligent and can automatically determine the topology of the network.

Spanning-tree bridges have built-in intelligence and can communicate with other bridges. They then can build up a picture of the interconnected networks. Then if more than one path exists between individual segments then the bridge automatically finds the alternate routers. This is useful when a fault develops on a route or a route becomes too heavily loaded. Conventional bridges can cause frames to loop around forever.

1.7 Network topologies

There are three basic topologies for LANs, which are shown in Figure 8, these are :

- A star network
- A ring network
- A bus network

There are other topologies which are either a combination of two of more topologies or are derivatives of the main types. A typical topology is a tree topology which is essentially a star and a bus network combined, as illustrated in Figure 8. A concentrator is used to connect the nodes onto the network.

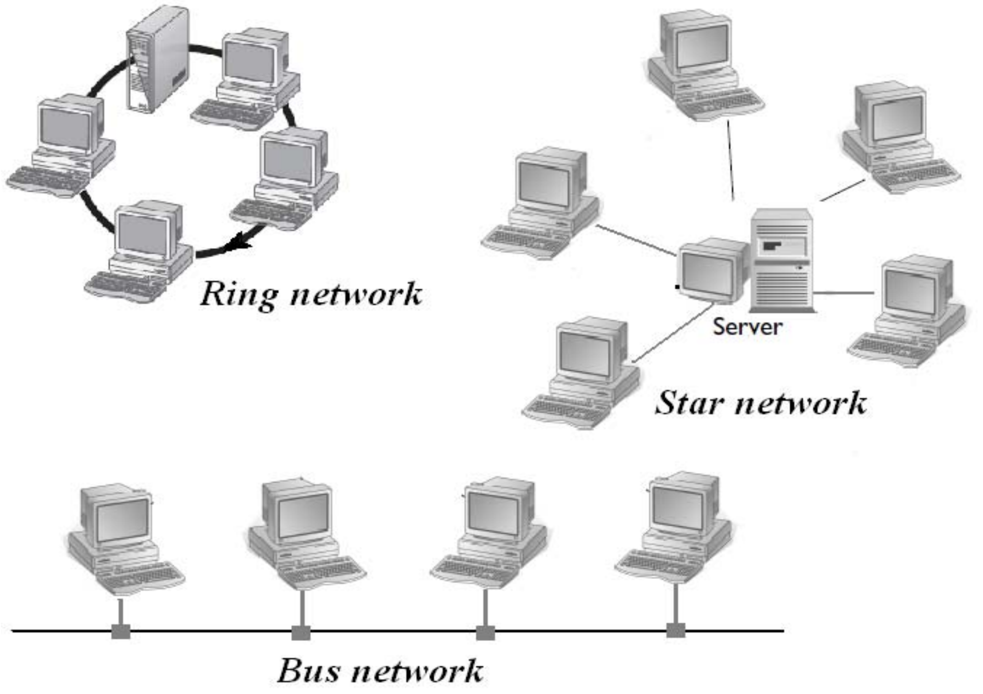


Figure 8. Network topologies

1.7.1. Star network

In a star topology, a central server switches data around the network. Data traffic between nodes and the server will thus be relatively low. Its main advantages are:

- Since the data rate is relatively low between central server and the node, a low-specification twisted pair cable can be used connect the nodes to the server.
- A fault on one of the nodes will not affect the rest of the network. Typically, mainframe computers use a central server with terminals connected to it.

The main disadvantage of this type of topology is that the network is highly dependent upon the operation of the central server. If it were to slow down significantly then the network becomes slow. Also if it was to become unoperational then the complete network would shut down.

1.7.2 Ring network

In a ring network the computers link together to form a ring. To allow an orderly access to the ring a single electronic token is passed from one computer to the next around the ring, as illustrated in Figure 9. A computer can only transmit data when it captures a token. In a manner similar to the star network each link between nodes is basically a point-to –point link and allows almost any transmission medium to be used. Typically twisted-pair cables allow a bit rate up to 16 Mbps, but coaxial and fibre optic cables are normally used for extra reliability and higher data rates.

A typical ring network is IBM Token Ring. The main advantage of token ring networks is that all nodes on the network have an equal chance of transmitting data. Unfortunately it suffers from several problems, the most severe is that if one of the nodes goes down then the whole network may go down.

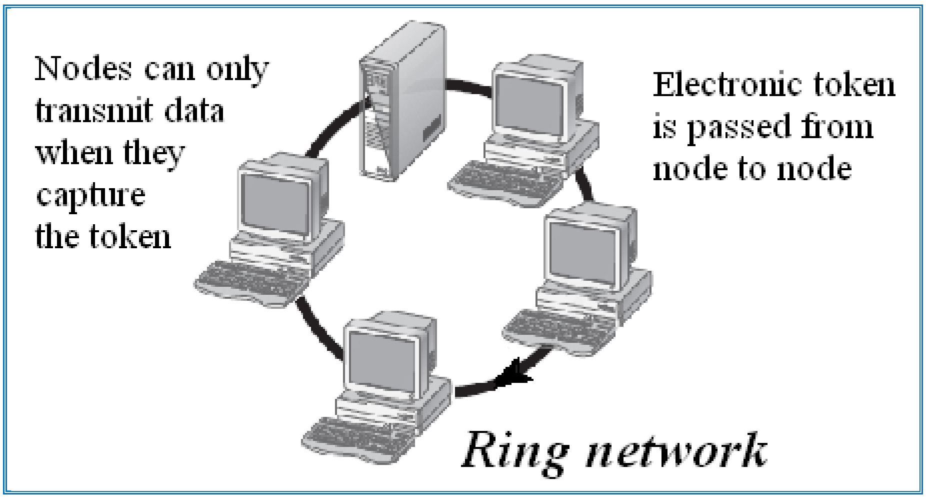

Nodes can only transmit data when they capture the token
Electronic token is passed from node to node
Ring network

Figure 9. Token passing ring network

1.7.3 Bus network

A bus network uses a multi-drop transmission medium, as shown in Figure 10. All nodes on the network share a common bus and all share communications. This allows only one device to communicate at a time. A distributed medium access protocol determines which station to transmit. As with the ring network, data packets contain source and destination addresses. Each station monitors the bus and copies frames addressed to itself.

Twisted-pair cables gives data rates up to 100 Mbps. Coaxial and fibre optic cables give higher bit rates longer transmission distances. A bus network is a good compromise over the other two topologies a s it allows relatively high data rates. Also, if a node goes down then it does not affect the rest of the network. The main disadvantage of this topology is that it requires a network protocol to detect when two nodes are transmitting at the same time. A typical bus network is Ethernet 2.0.

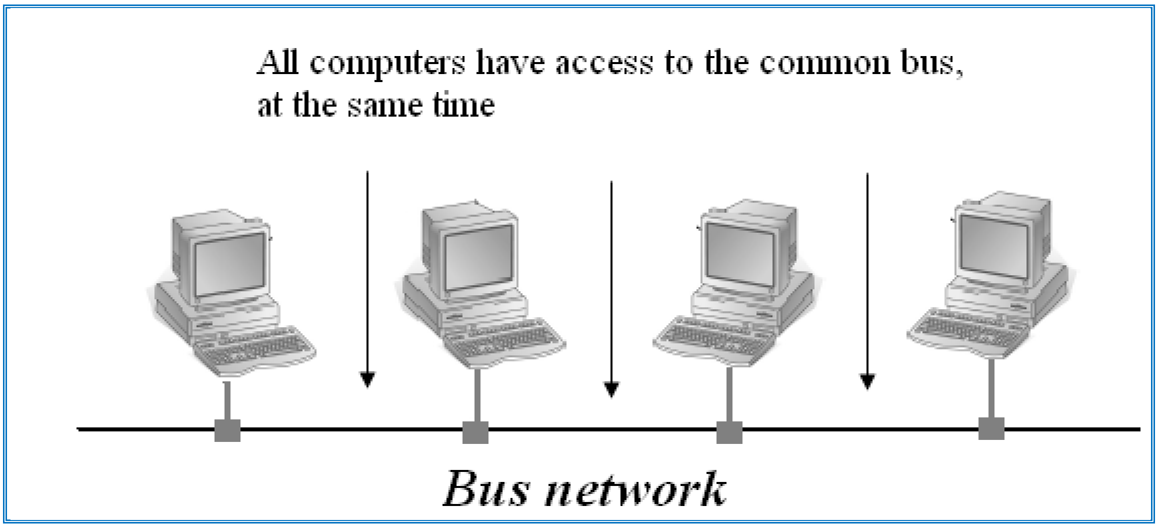


Figure 10. Bus topology

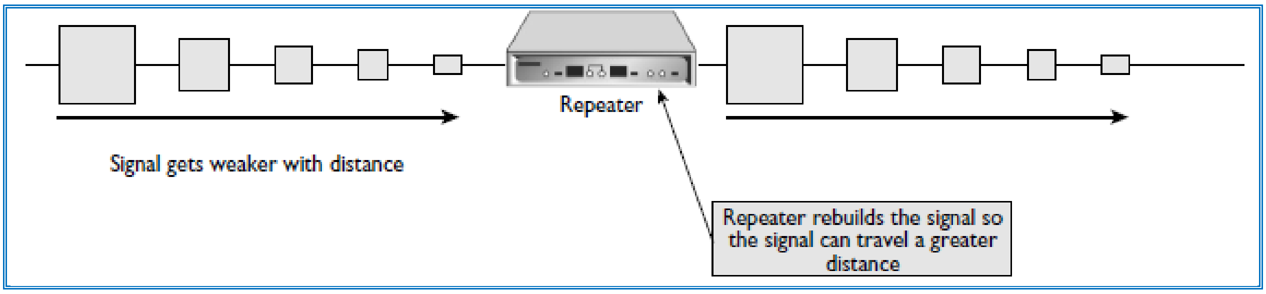
1.8 Routers, bridges and repeaters

Networks connect to other networks through repeaters, bridges or routers. A repeater corresponds to the physical layer of the OSI model and always routes data from one network segment to another. Bridges, on the other hand, route data using the data link layer(using the MAC address). Routers direct data using the network layer(that is, using the network address, such a s the IP address). Normally at the data link layer, transmitted data are known as a data frame, while at the network layer it is referred to as a data packet. Figure 11 illustrates the three interconnection types.

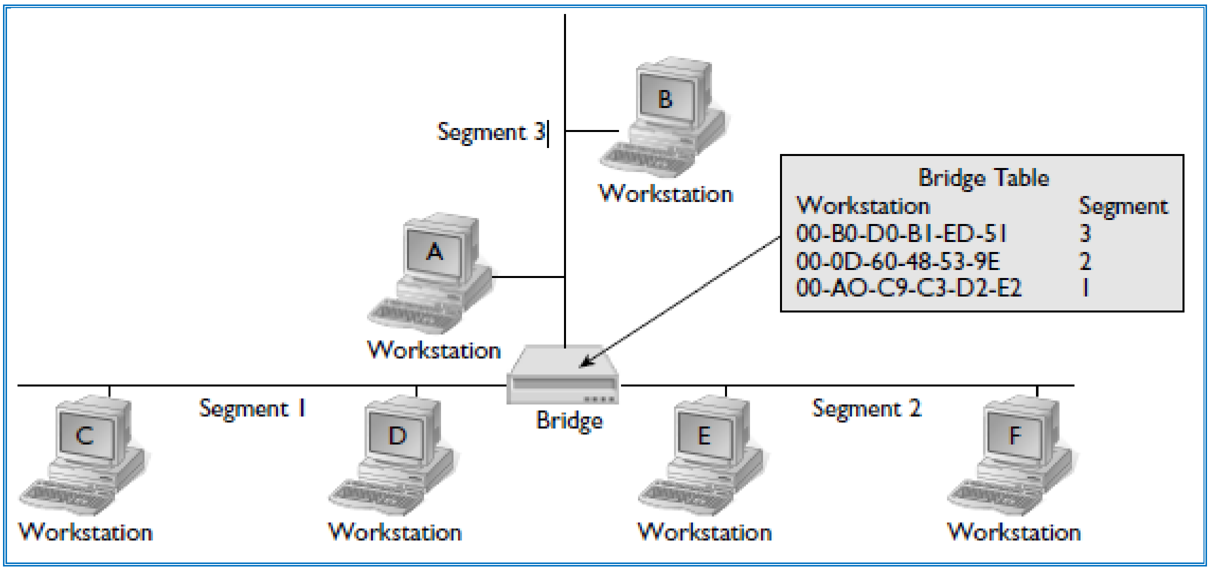
1.8.1 Repeaters

All network connections suffer from a reduction in signal strength(attenuation) and digital pulse distortion. Thus, for a given cable specification and bit rate, each connection will have a maximum length of cable that can be used to transmit the data reliably. Repeaters can be used to increase the maximum interconnection length, and may do the following:

- Clean signal pulses.
- Pass all signals between attached segments.
- Boost signal power.
- Possibly translate between two different media types (such as fibre to twisted-pair cable.)


Repeater
Signal gets weaker with distance
Repeater rebuilds the signal so the signal can travel a greater distance

Using a repeater to regenerate the signal

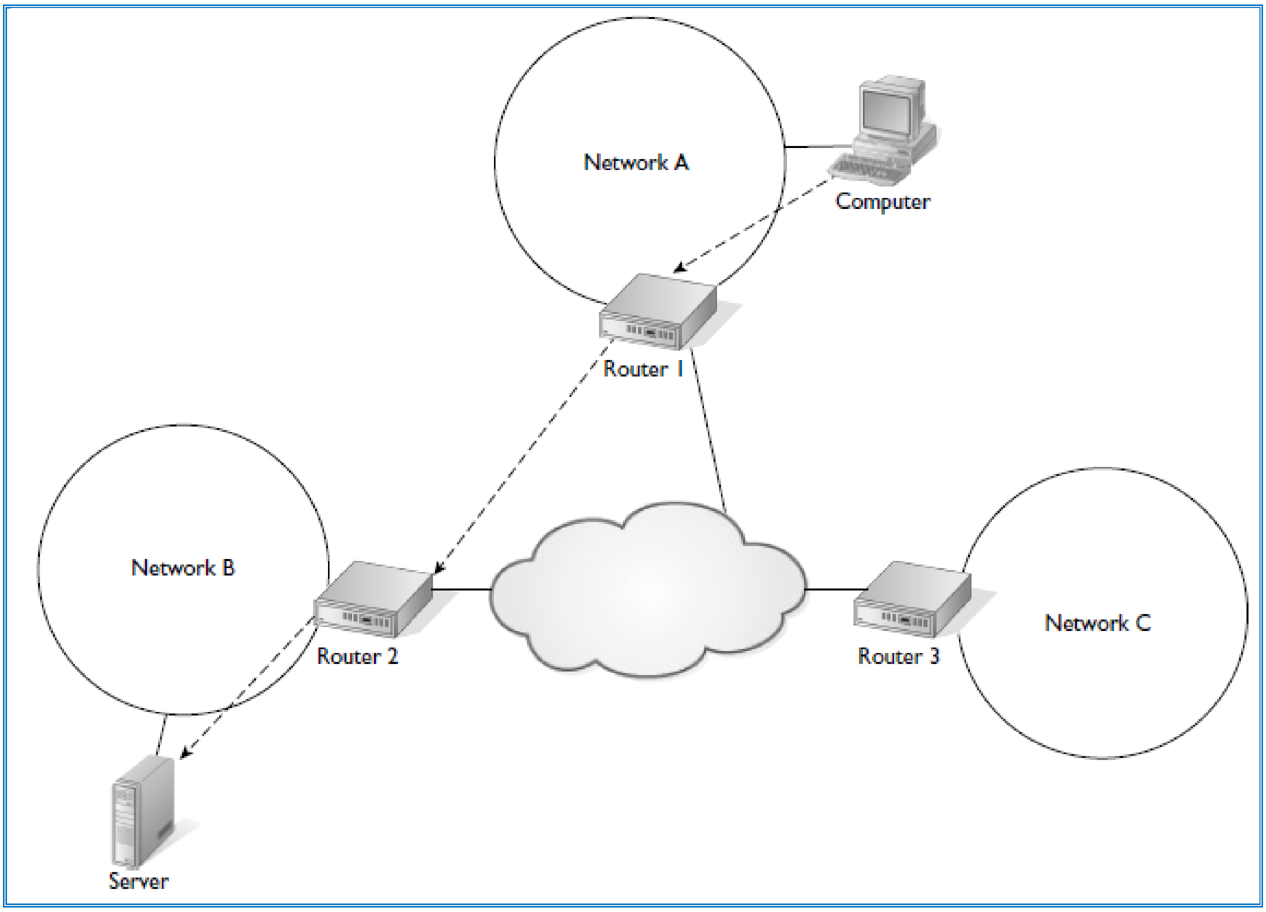


Bridge Table

Workstation	Segment
00-B0-D0-B1-ED-51	3
00-0D-60-48-53-9E	2
00-AO-C9-C3-D2-E2	1

A bridged network with three segments

Figure 11



Router connecting LANs and WANs

Figure 11 (continuation**)**

1.8.2 Bridges

Bridges filter input and output traffic so that only data frames distended for a network are actually routed into that network and only data frames destined for the outside are allowed out of the network.

The performance of a bridge is governed by two main factors:

- **The filtering rate.** A bridge reads the MAC address of the Ethernet/Token ring/FDDI node and then decides if it should forward the packet into the network. Filter rates for bridges range from around 5000 to 70000 pps (packets per second).
- **The forward rate.** Once the bridge has decided to route the frame into the internetwork then the bridge must forward the frame onto the Internet

network media. Forwarding rates range from 500 to 140 000 pps and a typical forwarding rate is 90 000 pps.

A typical Ethernet bridge has the following specifications:	
Bit rate:	10 Mbps
Filtering rate:	17 500 pps
Forwarding rate:	11 000 pps
Connectors:	2 DB15 AUI(female), DB9male console port, 2 BCN (for 10BASE2) or 2 RJ-45(for 10BASE-T)
Algorithm:	Spanning tree protocol. It automatically learns the addresses of all devices on both interconnected networks and builds a separate table for each network

Spanning tree architecture (STA) bridges

The spanning tree algorithm has been defined by the standard IFFF 802.1.It is normally implemented as software on STA-compliant bridges. On power-up they automatically learn the addresses of all nodes on both interconnected networks an build up a separate table for each network. They can also have two connections between two LANs so that when the primary path becomes disabled, the spanning tree algorithm can re-enable the previously disabled redundant link.

Source route bridging

With source route bridging a source device, not the bridge, is used to send special explorer, which are then used to determine the best path to the destination. Explorer packets are sent out from the source routing bridges until they reach their destination workstation. Then each source routing bridge along the route enters its address in the routing information field (RIF) of the explorer packet. The destination node then sends back the completed RIF field to the source node. When the source device has determined the best path to the destination, it sends the data message along with the path instructions to the local bridge. If then forwards the data message according to the received path instructions.

1.8.3. Routers

Routers examine the network address field and determine the best route for the packet. They have great advantage in that they normally support several different types of network layer protocols.

Routers need to communicate with other routers so that they can exchange routing information. Most network operating systems have associated routing protocols which support the transfer of routing information. Typical routing protocols used in Internet communications are:

- BGP (border gateway protocol).
- EGP (exterior gateway protocol).
- OSPF (open shortest path first).
- RIP (routing information protocol).

Most routers support RIP and EGP. In the past, RIP was the most popular router protocol standard. Its widespread use is due to no small part to the fact that it was distributed along with the Berkerley Software Distribution(BSD) of UNIX(from which most commercial versions of UNIX are derived). It suffers from several disadvantages and has been largely replaced by OSFP and EGB. These protocols have the advantage over the RIP in that they can handle large internetworks as well as reducing routing table update traffic.

RIP uses a distance vector algorithm which measures the number of network jumps(known as hops),up to a maximum of 16, to the destination router. This has the disadvantage that the smallest number of hops is not always the best route from source to destination. The OSPF and EGB protocol use a link state algorithm, which can decide between multiple paths to the destination router. These are based not only on hops but also on other parameters such as delay, capacity, reliability and throughput.

With distance vector routing each router maintains a table by communicating with neighbouring routers. The number of hops in its own table are then computed as it knows the number of hops to local routers. Unfortunately, the routing table can take some time to be updated when changes occur, because it takes time for all the routers to communicate with each other(known as slow convergence).

2.1. Local Area Networks (Ethernet)

Most of the computers on the Internet connect through a LAN and the most commonly used LAN is Ethernet. DEC,Intel and Xerox Corporation initially developed Ethernet and the IEEE 802 committee has since defined standards for it, the most common of which are Ethernet 2.0 and IEEE 802.3 . This chapter discusses Ethernet technology and the different types of Ethernet.

In itself Ethernet cannot make a network and needs some other protocol such as TCP/IP to allow nodes to communicate. Unfortunately, Ethernet in its standard form does not cope well with heavy traffic, but this is outweighted by the following:

- Ethernet networks are easy to plan and cheap to install.
- Ethernet network components, such as network cards and connectors, are cheap and well supported.
- It is a well-proven technology, which is fairly robust and reliable.
- It is simple to add and delete computers on the network.
- It is supported by most software and hardware systems.

A major problem with Ethernet is that, because computers must contend to get access to the network, there is no guarantee that they will get access within a given time. This contention also causes problems when two computers try to communicate at the same time then they must both back'off and no data can be transmitted. In its standard form it allows a bit rate of 10 Mbps, but new standards for fast Ethernet systems minimize the problems of contention and also increase the bit rate to 100 Mbps. Ethernet uses coaxial or twisted-pair cable.

Ethernet uses a shared-media, bus-type network topology where all nodes share a common bus. These nodes must then contend for access to the network as only one node can communicate at a time. Data are transmitted in frames which contain the MAC(media access control) source and destination addresses of the sending and receiving node, respectively. The local shared-media is known as a segment. Each node on the network monitors the segment and copies any frames addressed to itself.

Ethernet uses carrier sense, multiple access with collision detection(CSMA/CD). On a CSMA/CD network, nodes monitor the bus(or Ether) to determine if it is busy. A node wishing to send data waits for an idle condition then transmits its message. Unfortunately collision can occur when two nodes transmit at the same time, thus nodes must monitor the cable when they transmit. When this happens both nodes stop transmitting frames and transmit a jamming signal. This informs all nodes on the network that a collision has occurred. Each of the nodes then waits a random period of time before attempting a re-transmission. As each node has a random delay time then there can be a prioritization of the nodes on the network. Nodes thus contend for the network and are not guaranteed access to it. Collisions generally slow down the network. Each node on the network must be able to detect collisions and be capable of transmitting and receiving simultaneaously.These nodes either connect onto a common Ethernet connection or can connect to an Ethernet hub, as illustrated in **Figure**

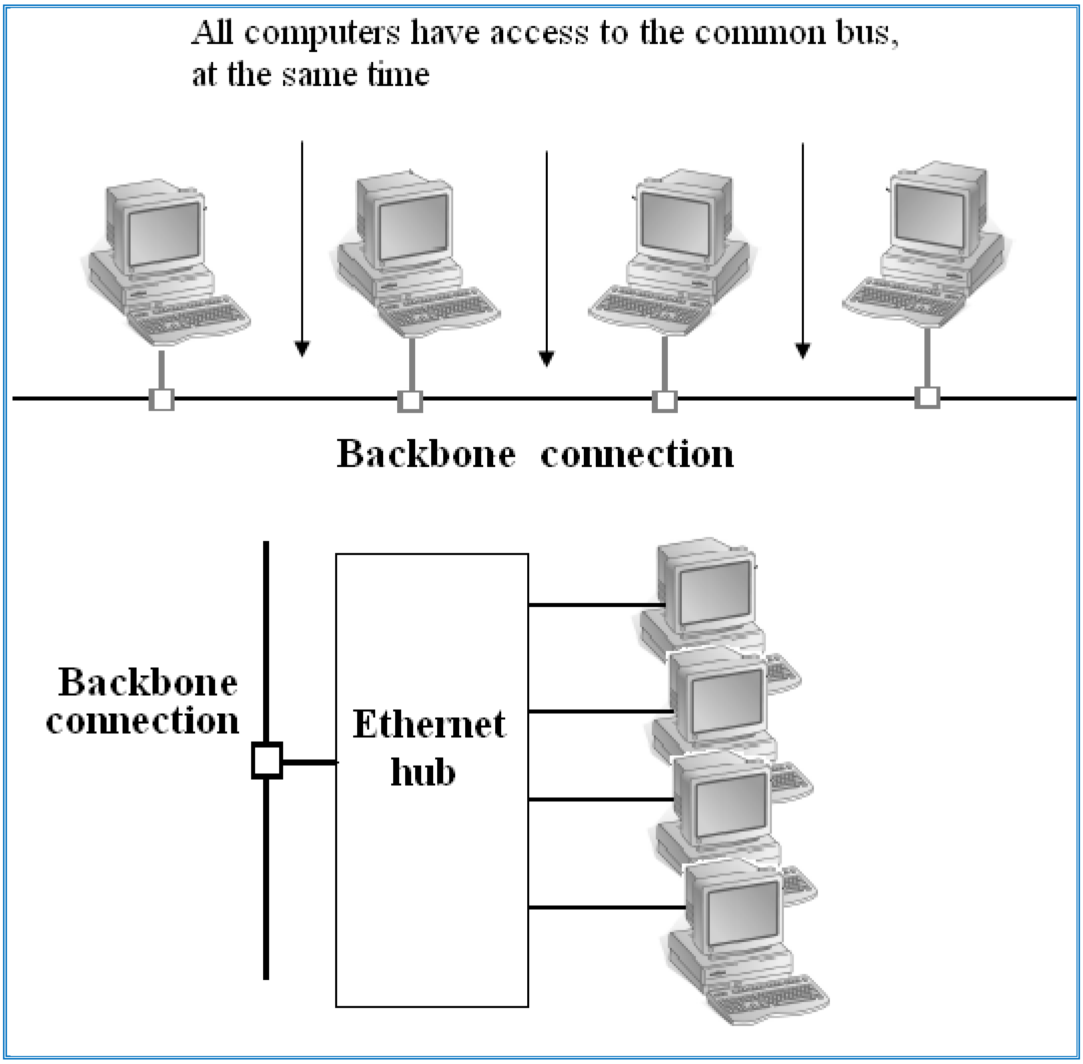

All computers have access to the common bus, at the same time
Backbone connection
Backbone connection
Ethernet hub

Figure 12

2.2 IEEE standards

The IEEE are the main standards organization for LANs and they refer to the standard for Ethernet as CSMA/CD(carrier sense multiple access/collision detect). **Figure 13** shows how the IEEE standards for CSMA/CD fit into the OSI model. The two layers of the IEEE standards correspond to the physical and data link layers of the OSI model. On Ethernet networks, most hardware will comply with IEEE 802.3 standard. The object of the MAC layer is to allow many nodes to share a single communication channel. IT also adds start and end frame delimiters, error detection bits, access control information and source and destination addresses. Each Ethernet data frame has an error detection scheme known as cyclic redundancy check (CRC).

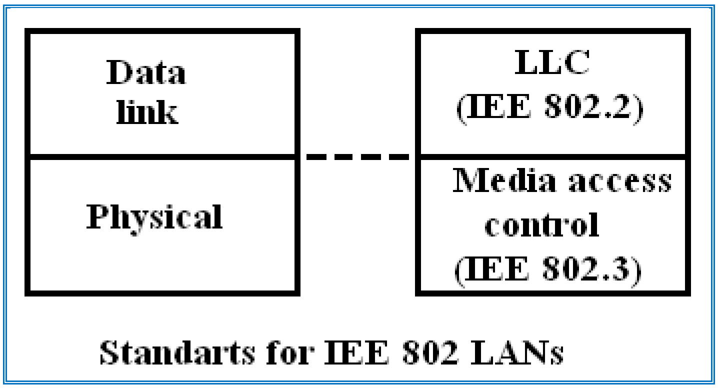


Figure 13

2.3 Ethernet – media access control (MAC) layer

When sending data the MAC layer takes the information from the LLC link layer. **Figure 14** shows the IEEE 802.3 frame format. It contains two or six bytes for the source and destination addresses(16 or 48 bits each), four bytes for the CRC(32 bits) and two bytes for the LLC length(16 bits). The LLC part may by up to 1500 bytes long. The preamble and delay components define the start and of the frame. The initial preamble and start delimiter are, in total, eight bytes long and the delay component is a minimum of 96 bytes long.

A seven-byte preamble precedes the Ethernet 802.3 frame. Each byte of the preamble has a fixed binary pattern of 10101010 and each node on the network uses it to synchronise its clocks and transmission timigs. It also informs nodes that a frame is to be sent and for them to check the destination address in the frame.

The end of the frame is a 96-byte delay period, which provides the minimum delay between two frames. This slot time delay allows for the worst-case network propagation delay.

The smart delimiter field(SDF) is a single byte (or octet) of 10101011. It follows the preamble and identifies that there is a valid frame being transmitted. Most Ethernet systems use a 48-bit MAC address for the sending and receiving node. Each Ethernet node has a unique MAC address, which is normally defined as hexadecimal digits, such as:

4C – 31 – 22 – 10 - F1 – 32

or 4C31 : 2210 : F132

A 48-bit address field allows 2^{48} different addresses(or approximately 281 474976710 000 different addresses).

The LLC length field defines whether the frame contains information ок it can be used to define the number of bytes in the logical link field. The logical link field can contain up to 1500 bytes of information and has a minimum of 46 bytes, its format is given in **Figure 14**. If the information is greater than the upper limit then multiple frames are sent. In addition, if the field is less than the lower limit then it is padded with extra redundant bits.

The 32-bit frame check sequence (or АСЫ) is an error detection scheme. It is used to determine transmission errors and is often referred to as a cyclic redundancy check (CRC) or simply as checksum.

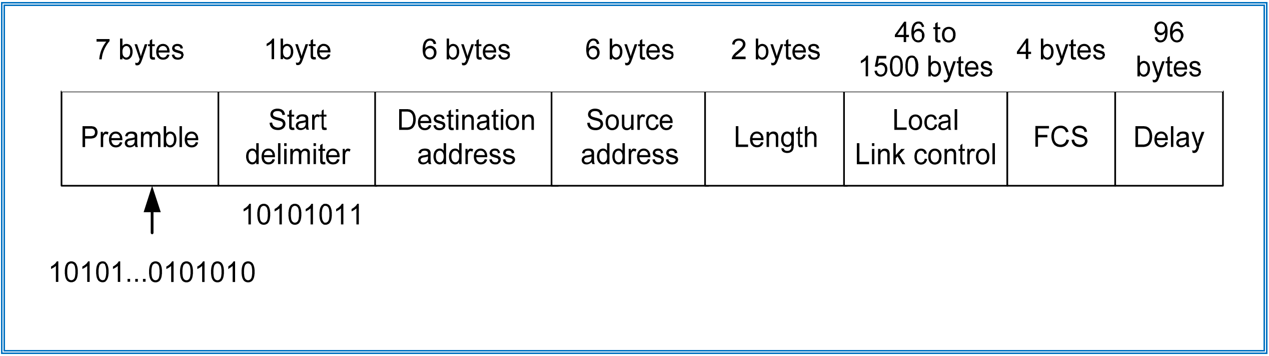


Figure 14

2.4 Ethernet transceivers

Ethernet requires a minimal amount of hardware. The cables used to connect it are either unshielded twisted pair cable(UTP) ок coaxial cables. These cables must be terminated with their characteristic impedance, which is 50Ω for coaxial cables and 100Ω for UTP cables.

Each node has transmission and reception hardware to control access to the cable and also to monitor network traffic. The transmission/reception hardware is called a transceiver (short for *trans*mitter/re*ceiver*) and a controller builds up and strips down the frame. The transceiver builds the transmitted bits at a rate of 10 Mbps – thus the time for one bit is 1/10 × 10^6, which is 0.1 µs

The Ethernet transceiver transmits onto a single ether. When none of the nodes are transmitting then the voltage on the line is +0.7 V. This provides a carrier sense signal for all nodes on the network, it is also known as the heart-beat. If a node detects this voltage then it knows that the network is active and there are no nodes currently transmitting.

Thus when a node wishes to transmit a message it listens for a quite period. Then if two or more transmitters transmit at the same time then a collision results. When they detect the collision then each node transmits a 'jam' signal. The nodes involved in the collision then wait for a random period of time (ranging from 10 to 90 ms) before attempting to transmit again. Each node on a network also awaits a retransmission. Thus collisions are inefficient in network as they stop nodes from transmitting. Transceivers normally detect collisions by monitoring the DC(or average) voltage on the line.

When transmitting, a transceiver unit transmits the preamble of consecutive 1s and 0s. The coding used is a Manchester code which represents a 0 as a high to a low voltage transition and a 1 as a low to high voltage transition. A low voltage is -0.7 V and a high is + 0.7 V. Thus when the preamble is transmitted the voltage will change between +0.7 and -0.7 V, this is illustrated in **Figure 15.** If after the transmission of the preamble no collisions are detected then the rest of the frame is sent.

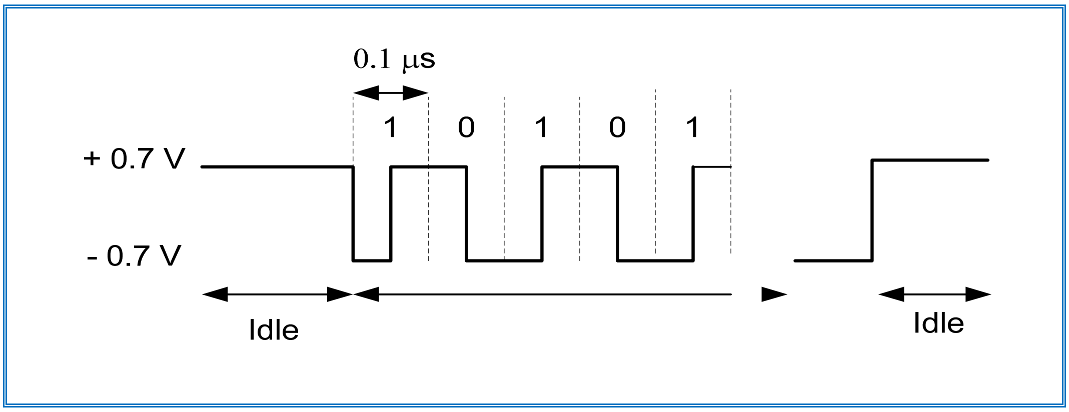


Figure15

2.5 Ethernet types

The five main types of standard Ethernet are:

- Standard, or thick-wire, Ethernet(10BASE5).
- Thinnet, or thin-wire Ethernet, or Cheapernet (10BASE2).
- Twisted-pair Ethernet(10BASE-T).
- Optical fibre Ethernet(10BASE-FL).
- Fast Ethernet(100BASE-TX ot 100VG-Any LAN).

The thin- and thick-wire types connect directly to and Ethernet segment, these are shown in **Figure16** and **Figure17**. Standard Etherne, 10BASE%, uses a high specification cable(RG-50)and N-type plugs to connect the transceiver to the Ethernet segment. A node connects to the transceiver using a 9-pin D Type connector. A vampire(or bee-sting)connector can be used to clamp the transceiver to the backbone cable.

Thin-wire, or Cheapernet, uses a lower specification cable (it has a lower inner conductor diameter). The cable connector required is also of a lower specification, that is, BNC rather than N-type connectors. In standard Ethernet the transceiver unit is connected directly onto the backbone tap. On a Cheapernet network the transceiver is integrated into the node.

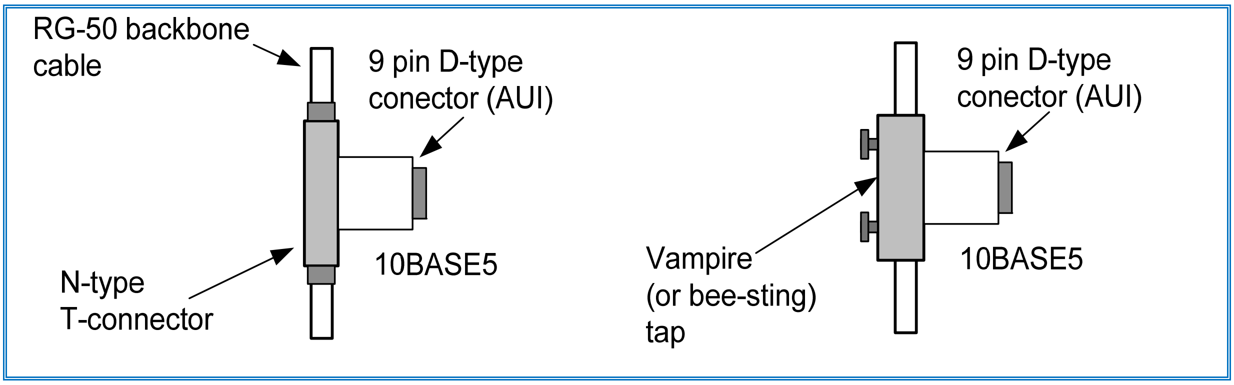

RG-50 backbone cable
9 pin D-type conector (AUI)
10BASE5
N-type T-connector
9 pin D-type conector (AUI)
Vampire (or bee-sting) tap
10BASE5

Figure16

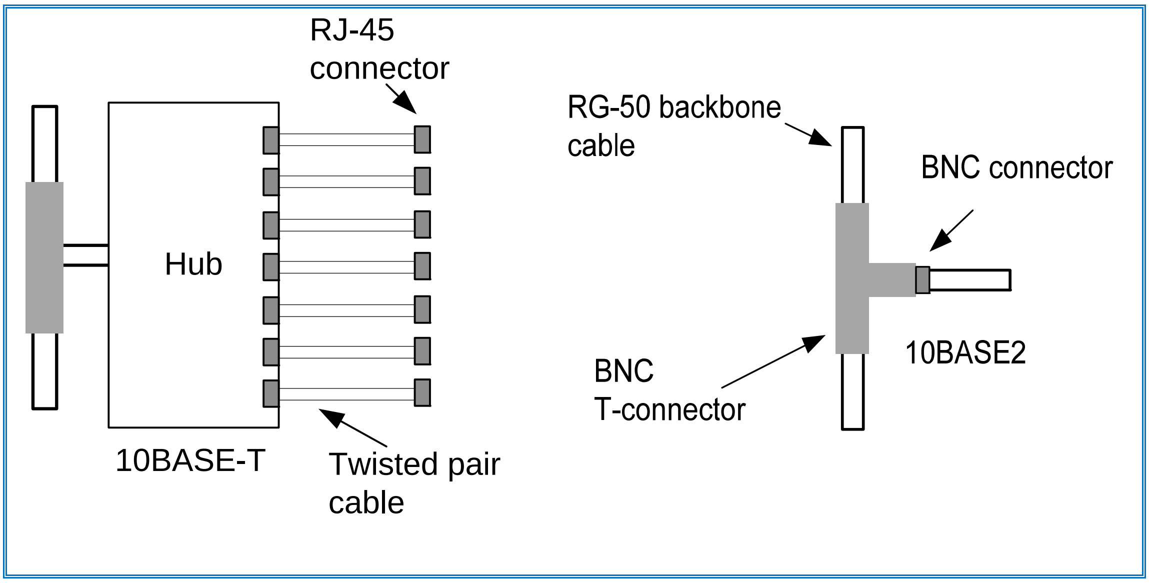


Figure17

Many modern Ethernet connections are to a 10BASE –T hub which connects UTP cables to the Ethernet segment. An RJ-45 connector is used for 10BASE – T. The fibre optic type, 10BASE-FL, allows long lengths of interconnected lines, typically up to 2 km. They use either SMA connectors or ST connectors. SMA connectors are screw-on types while ST connectors are push-on. **Table** shows the basic specifications for the different types.