Network Types

Ethernet

Ethernet is the most common network. It offers support for a variety of protocols and computer platforms. The Ethernet standard was developed by the IEEE Committee. Ethernet has been successful due to its varied support for cabling and its relatively low cast.

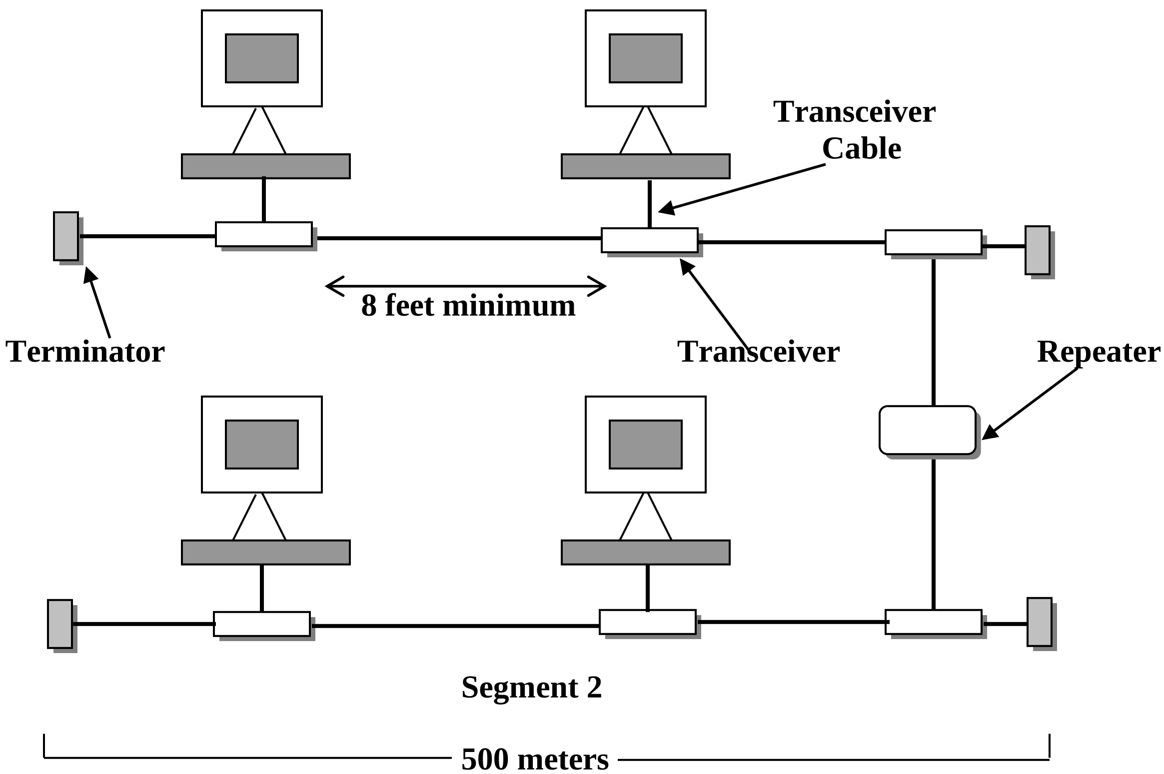
Ethernet is available in different standards.

- 10Base-5:
- 10Base-2:
- 10Base-T:
- 10Base-F:
- 100Base-FX (Fast Ethernet at 100Mbps)
- 1000Base-X (Gigabit Ethernet over fiber at 1Gbps (1998))
- 10GBase-EW (10Gbps Ethernet over fiber (2003))

10Base-5

10Mbps using RG-8 or RG-11 coaxial cable to transmit signals in 500-meter segments. This is also known as Thick Ethernet. Ethernet access the network with the CSMA/CD (Carrier sense multiple access with collision detection) media access method. This means that only one workstation can use the network at a time.

10Base-5 Ethernet has the following specifications:



10Base-5 Network

- **Topology:** Bus
- **Media Access method:** CSMA/CD
- **Cable Types:** 50-ohm Thick net coax cable.
- **Transmission speed**: 10Mbps.
- **Maximum number of network nodes:** 300-500
- **Maximum number of nodes per segment:** 100
- **Maximum number of segments:** 5, 3 of which can have connected nodes.
- **Minimum distance between the nodes:** 2.5 meters (8 feet).

- **Maximum network length:** 2500 meters.
- **Maximum segment length:** 500 meters.
- **Protocol used:** IPX/SPX (Internet work Packet Exchange/Sequenced Packet Exchange) or TCP/IP.

CSMA/CD Carrier Sense Multiple Access/Collision Detection

The transmission sequence on a CSMA/CD network goes as follows:

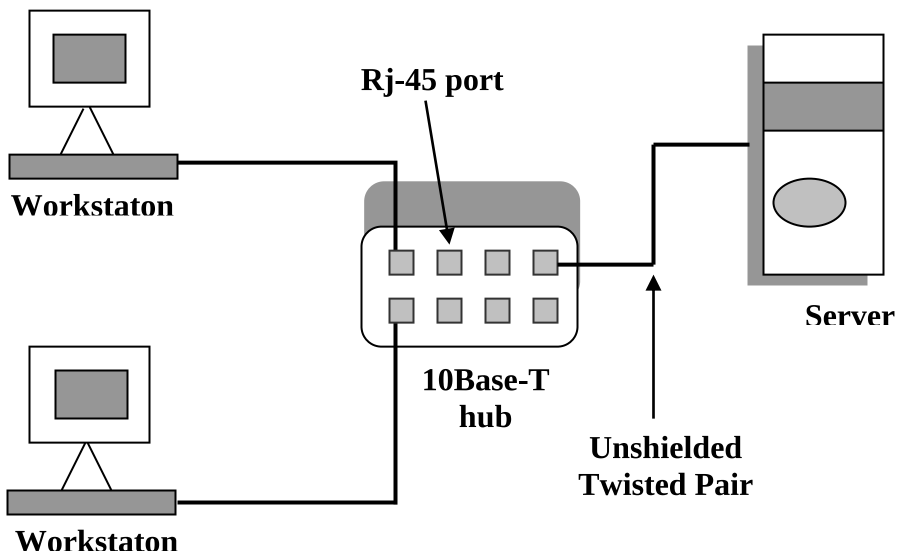
1. The device “listens” to the media for any other transmissions.
2. If the network media is quite, then the device proceeds to start transmitting its data.
3. After the device transmits its data, it listens to the network media to detect any collision.
4. If the device detects a collision, it will send out a signal for all other devices to receive. This signal tells the other devices to keep from sending data for a small period to clear all signals from the media.
5. The transmitting stations will then wait a random amount of time before sending their data.

10Base-2

10Mbps using RG-58 coaxial cable to transmit signals on 200-meter segments. This is also known as Thin Ethernet.

10Base-T

10Mbps using UTP cabling with RJ-45 jacks arranged in a star configuration to transmit signals on 100-meter segments. This is also known as Twisted-Pair Ethernet. This configuration eliminates the single point of failure problem associated with the bus topology. Each device has a separate UTP cable connecting it to the hub.



10Base-T network

The10Base-T Ethernet has the following specifications:

- **Topology:** Star
- **Media Access method:** CSMA/CD
- **Cable Types:** Categories 3-5 UTP cable.
- **Transmission speed**: 10Mbps.
- **Maximum number of network nodes:** 1024
- **Maximum number of nodes per segment:** 1
- **Maximum number of segments:** 1024
- **Minimum distance between the nodes:** 2.5 meters (8 feet).

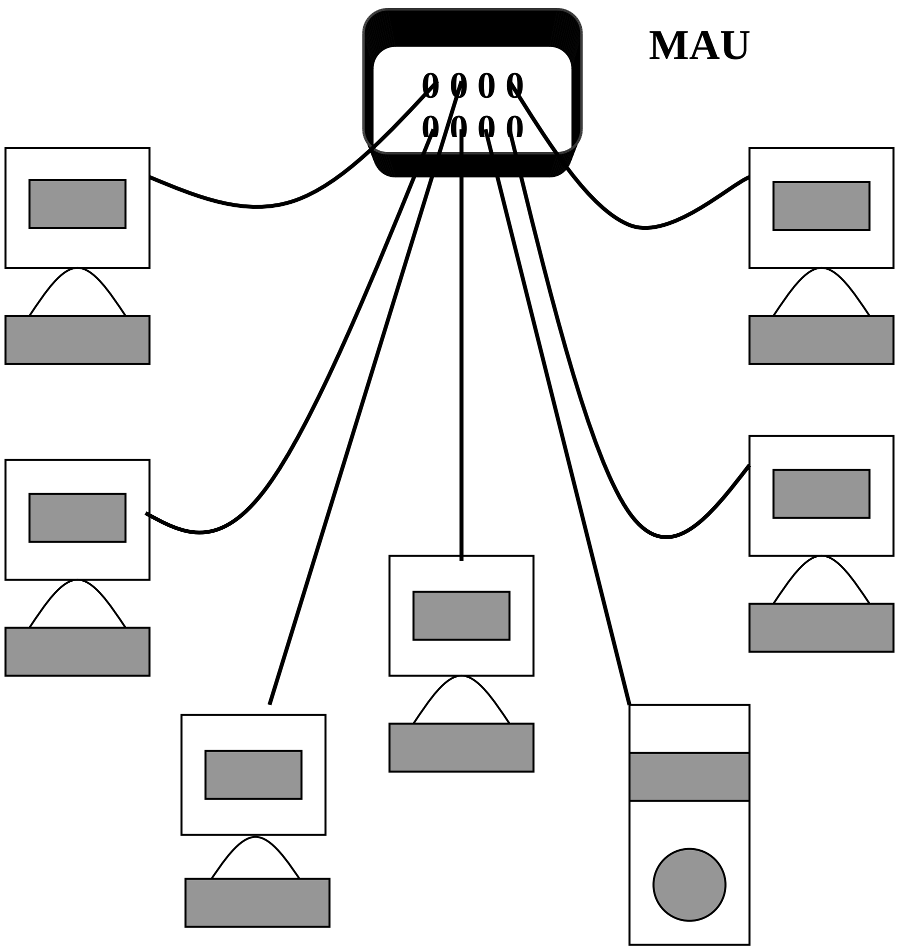
- **Maximum network length:** No maximum length.
- **Maximum segment length:** 100 meters.
- **Protocol used:** IPX/SPX (Internet work Packet Exchange/Sequenced Packet Exchange) or TCP/IP.

Fast Ethernet (100Base-Fx: Fiber optic)

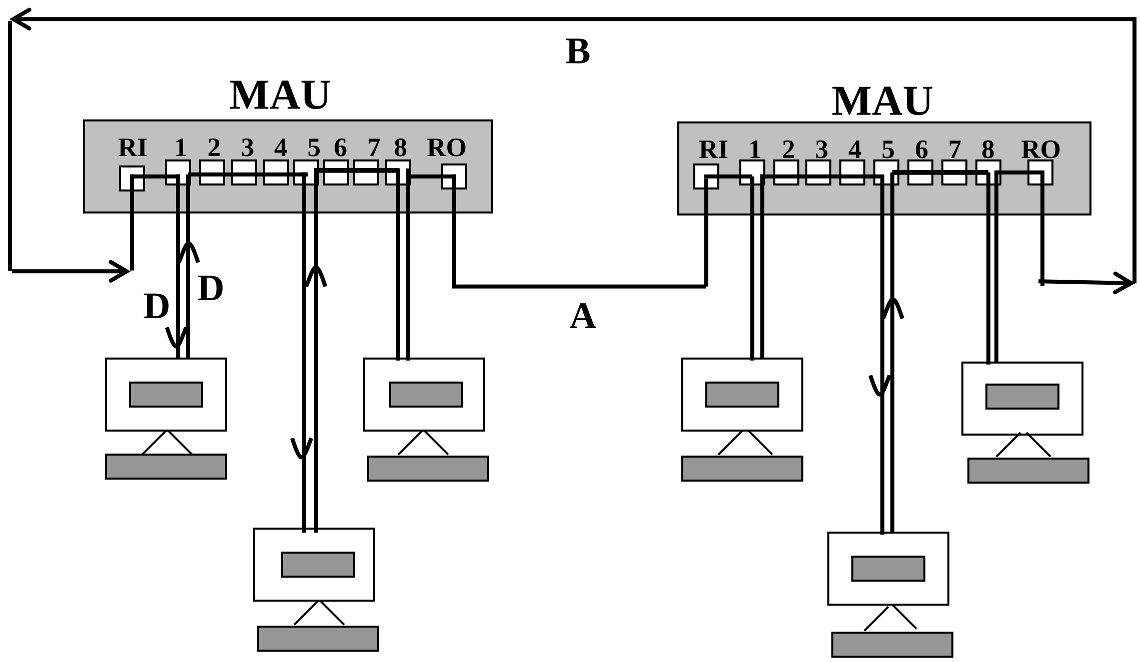
Token Ring

Token Ring uses token passing in a physical star configuration connected in a ring using hubs. For this reason, Token Ring holds up well under heavy network traffic. This standard was developed by IBM and was certified by the IEEE Committee. Token Ring is much more expensive network than Ethernet and ARCNET.

Token ring uses a physical star to connect systems in a logical ring, as shown in fig. The systems are connected to a central device using separate cables. This is called the physical star configuration. Inside the central device, the ports are connected in a ring as shown in fig.



Physical Token Ring Star



A + B = Total main ring length
D = Lobe cable length (330 feet)
RI = Ring in
RO = Ring out

Token Ring has the following specifications:

- **Topology:** Physical Star, Logical Ring.
- **Media Access method:** Token Passing.
- **Cable Types:** STP, UTP, and fiber optic.
- **Transmission speed**: 4 or 16Mbps.
- **Maximum number of network nodes:**
  - UTP: 72
  - STP: 260
- **Maximum number of segments:** 33

- **Maximum network length connecting all MAUs:** 400 feet with UTP cables; fiber-optic cabling can span several kilometers.
- **Maximum distance between node and MAU (segment length):** 150 feet for UTP cable; up to 330 feet for STP.
- **Maximum patch cable distance connecting MAUs:** 45.5 meters with UTP; 200 meters with STP; 1 kilometer with fiber-optic.

Hubs.

Multistation Access Unit (MAU) is a Token Ring hub. The MAU internally links the workstation into a ring. MAUs have special ring-in and ring-out ports used to connect several MAUs to the ring.

Cables.

The seven types of cable that can be used with IBM Token Ring:- (UTP, STP, Fiber-Optic)

How Token Ring Works?

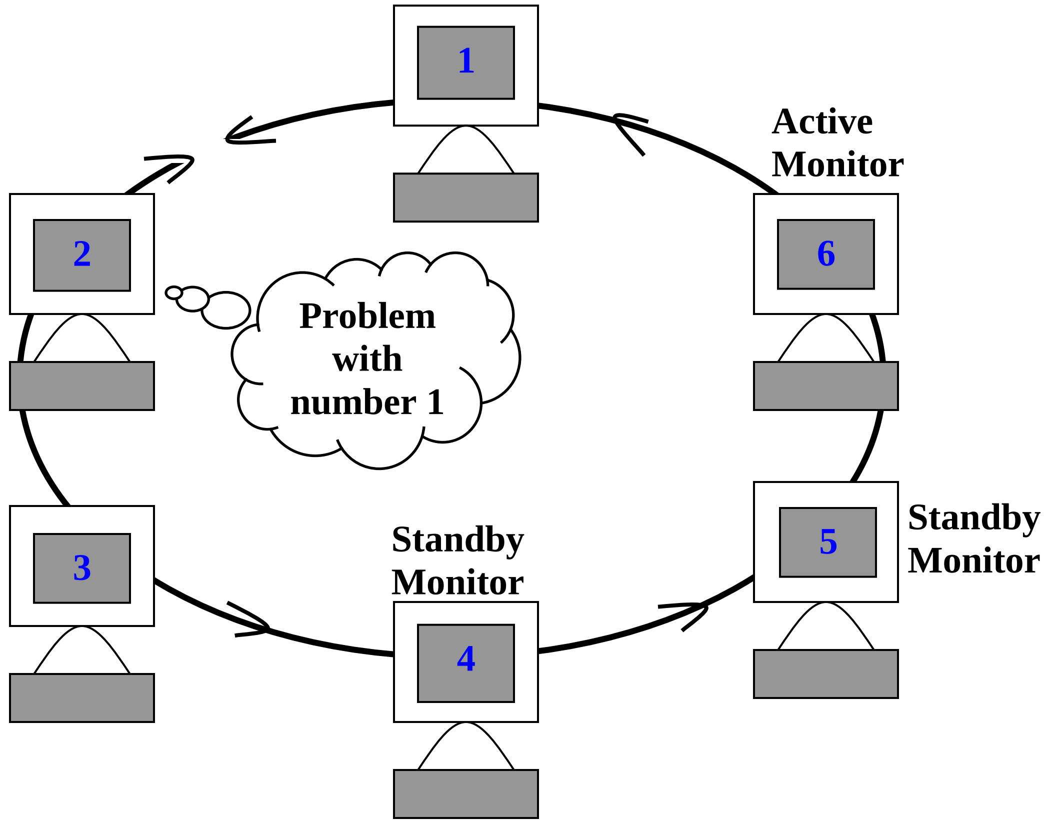
The ring passes a free token (a small frame with a special format) around the ring in one consistent direction. A node receives the token from its nearest active upstream neighbor (NAUN) and passes it to its nearest active downstream neighbor (NADN). If a station receives a free token, it knows it can attach data and send it on down the ring.

Each station in the ring receives the data from the busy token with data attached and repeats the token and data, exactly as it received them. The address station keeps the data and passes it to its upper-layer. It then switches two bits of the frame.

Active Monitors and Standby Monitors.

The station that has been up the longest normally becomes the active monitor. Token Ring allows only one active monitor on a ring at a time. All other stations on the ring become stand by monitors. The active monitor does a sort of system check every seven seconds. In this check, the active monitor sends out a token to the next station on the ring. This token informs the station of the active monitor's address.

If a station does not hear from its upstream neighbor in the seven seconds, it assumes something bad has happened and acts on its own. It sends a message down the ring announcing three basic pieces of information: its network address, the station it has not heard from in the allotted time, and the type of beacon (the condition being indicated, such as no response from the node). This action is called beaconing. It occurs when the Nearest Active Upstream Neighbor notification fails, as illustrated in fig.



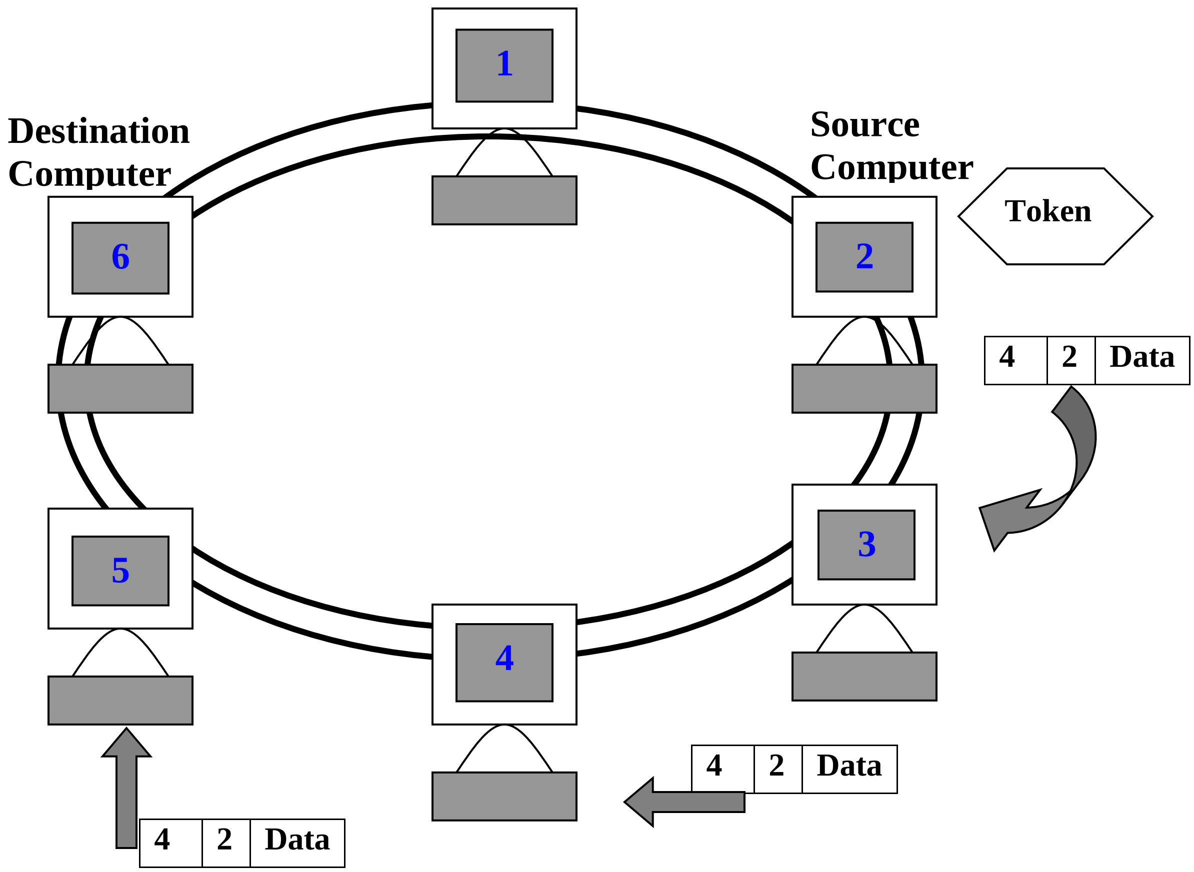
During the beaconing process, each Token Ring card takes itself out of the ring and does an internal diagnostic to determine whether it has a problem. If it can, it repairs itself without administrator intervention.

Here are some of the advantages:

1. Unlike Ethernet, Token Ring continues to operate reliably under heavy loads.
2. Built-in diagnostic and recovery mechanisms, such as beaconing and auto-reconfiguration, make the protocols more reliable.
3. High-speed network capable of 4 to 20Mbps.
4. Expensive, Difficult to troubleshoot.

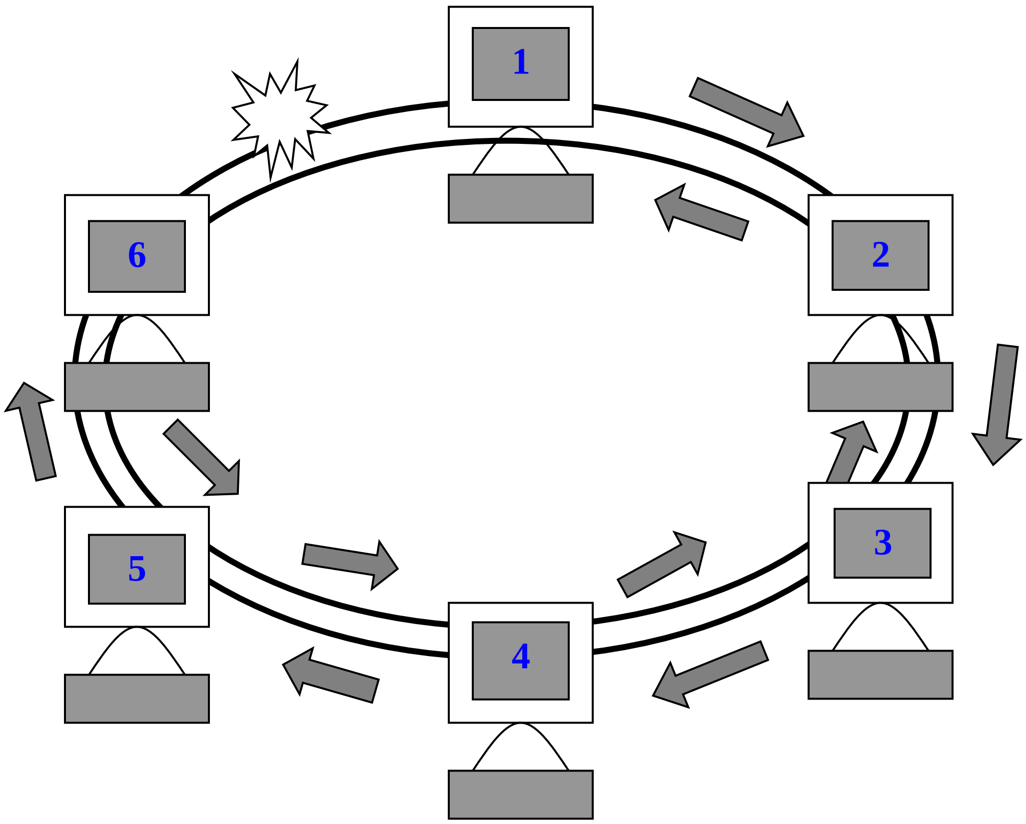
FDDI (Fiber Distributed Data Interface)

FDDI is another ring-based network; FDDI uses fiber-optic cables to implement very fast, reliable networks.
Like Token Ring, a token is passed around the ring, and the possessor of the token is allowed to transmit FDDI frames. Unlike Token Ring, a FDDI network may have several frames simultaneously circulating on the network. This is possible because the possessor of the token may send multiple frames, without waiting for the first frame to circulate all the way around the ring before sending the next frame.
The possessor of the FDDI token is also allowed to release the token and send it to the next station in the ring as soon as it is through transmitting frames, rather than having to wait for the frames to make it all the way around the ring. This means that the next station may begin transmitting while the frames from the first station are still circulating, as shown in fig.
Some FDDI networks also have a method of reserving regular transmission times for certain stations; only those stations may transmit at those regular intervals, and those stations are not required to capture a token to transmit. Frames sent in such a manner are called *synchronous frames*.



Dual Counter-Rotating Rings.

Another feature that sets FDDI apart from Token Ring is that it uses two counter-rotating rings as shown in fig. Since there is no central device to bypass network failures, another method must be used to ensure that a single failure does not take down the whole network, FDDI does this by implementing two links in each device, one for the primary ring, the other for the secondary ring. In the event of a device or a cable failure, a single ring would be broken, and the token (and the data frames) would not be able to proceed around the ring. In FDDI, the data is then routed to the secondary ring, and the data travels back around the ring, in the opposite direction from the way it originally traveled. When it reaches the other side of the break in the network and is able to proceed no farther, it is routed back to the primary ring and proceeds normally.



There are two types of stations: Class A and Class B. Class A stations are also called *dual-attached stations* because they can be attached to both rings at the same time. Class A stations are extremely stable. They can survive a break in one or both rings. Class B stations are called *single-attached stations* because they attach to only one ring.

FDDI network has the following specifications:

- **Topology:** Ring
- **Media Access method:** Token Ring
- **Cable Types:** Optical Fiber.
- **Transmission speed**: 100Mbps.
- **Maximum network length:** 4 Kilometers.
- **Maximum number of network nodes:**
- **Maximum number of nodes per segment:**
- **Maximum number of segments:**
- **Minimum distance between the nodes:**
- **Maximum segment length:**

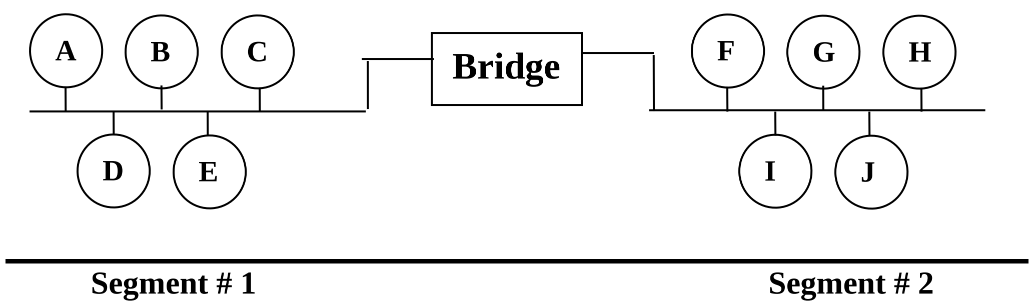
Bridges

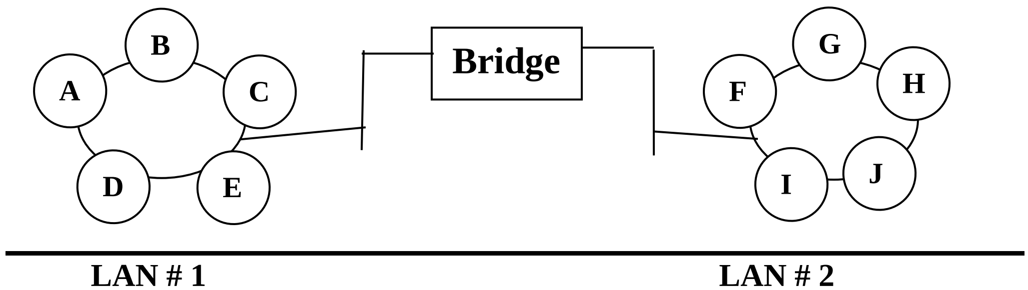
Where repeaters do not do any type of filtering of traffic that they pass, bridges do.

A bridge can connect two or more networks that use a similar data communication scheme, and specifically, the same addressing method.

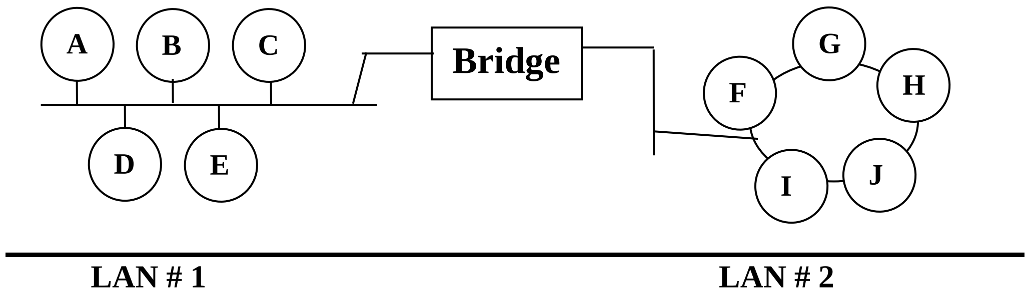
Bridges work at the data link Layer of the OSI model and like a repeater, attach two different network segments and pass data.

Bridges use MAC addresses to filter traffic b/w segments. (e.g) Two Ethernet LAN's can be interconnected by a bridge. As shown.





In fact, the Ethernet and Token Ring both use the similar addressing (MAC), so they can be connected to each other with a bridge.



Functions of Bridges

When a bridge receives a frame from one segment, it verifies that the frame arrived, there was no electrical interference on the LAN during transmission, and then forwards a copy of the frame to the other segment if necessary.

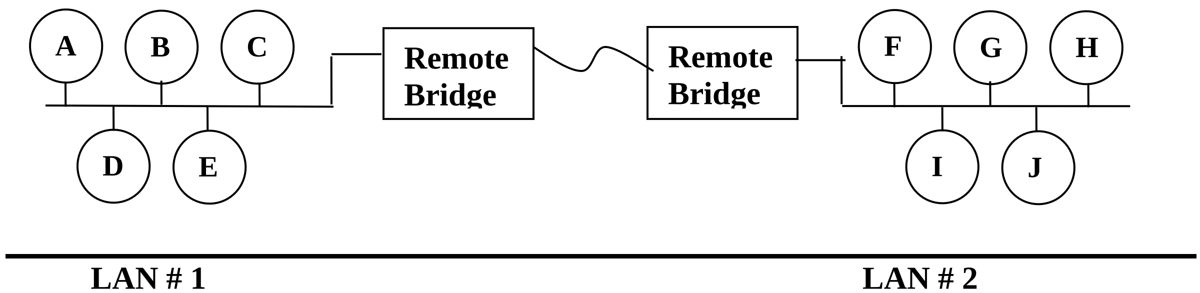
To determine whether to forward a frame, a bridge uses the physical address found in the frame's header. The bridge knows the location of each computer attached to the LAN's, it connects. When a frame arrives on a segment, the bridge extracts and checks the destination address. If the destination computer is attached to the segment over which the frame arrived, the destination and bridge receive the same transmission, and the bridge discards the frame without forwarding a copy. If the destination does not lie on the segment over which the frame arrived, the bridge sends a copy of the frame on the other segment.

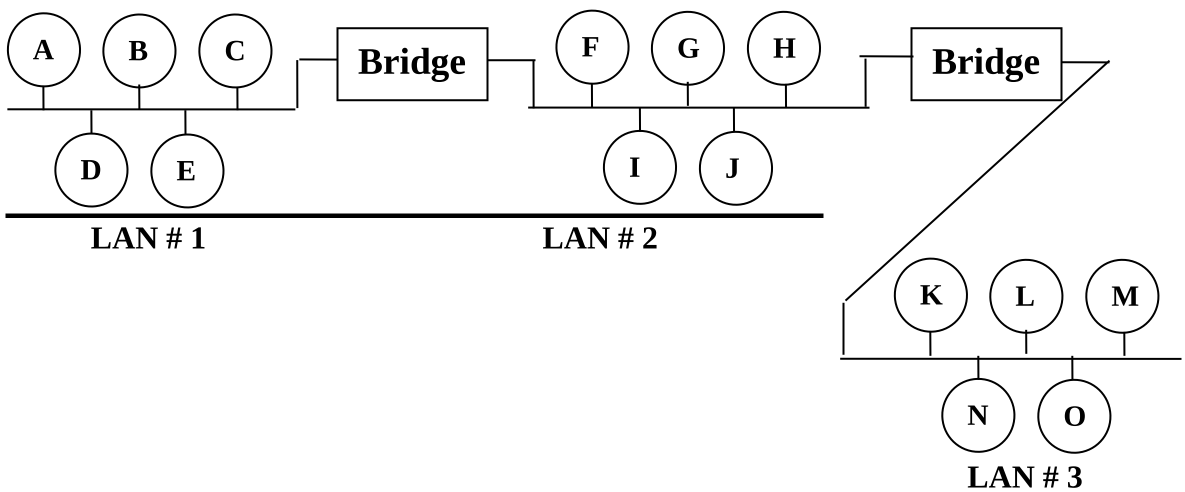
How can a bridge know which computers are attached to which segments? The bridges learn the locations of computers automatically.

Event	Segment 1 List	Segment 2 List
Bridge boots	--------	--------
A sends to B	A,	--------
B sends to A	A, B	-------

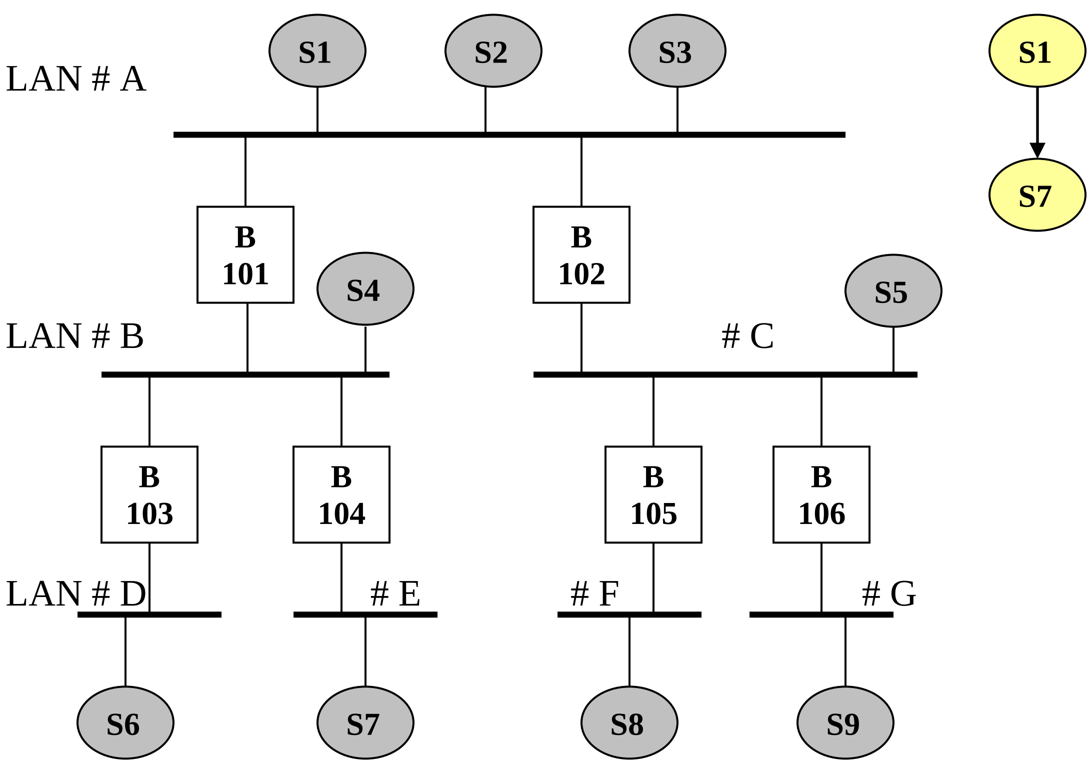
Advantages of Bridges

1. Bridges extend Network segments by connecting them together to make one logical Network.
2. Bridges segment traffic b/w networks by filtering data if it does not need to pass.
3. Like repeaters, they can connect similar network types with different cabling.
4. Special bridges can connect different network types together.

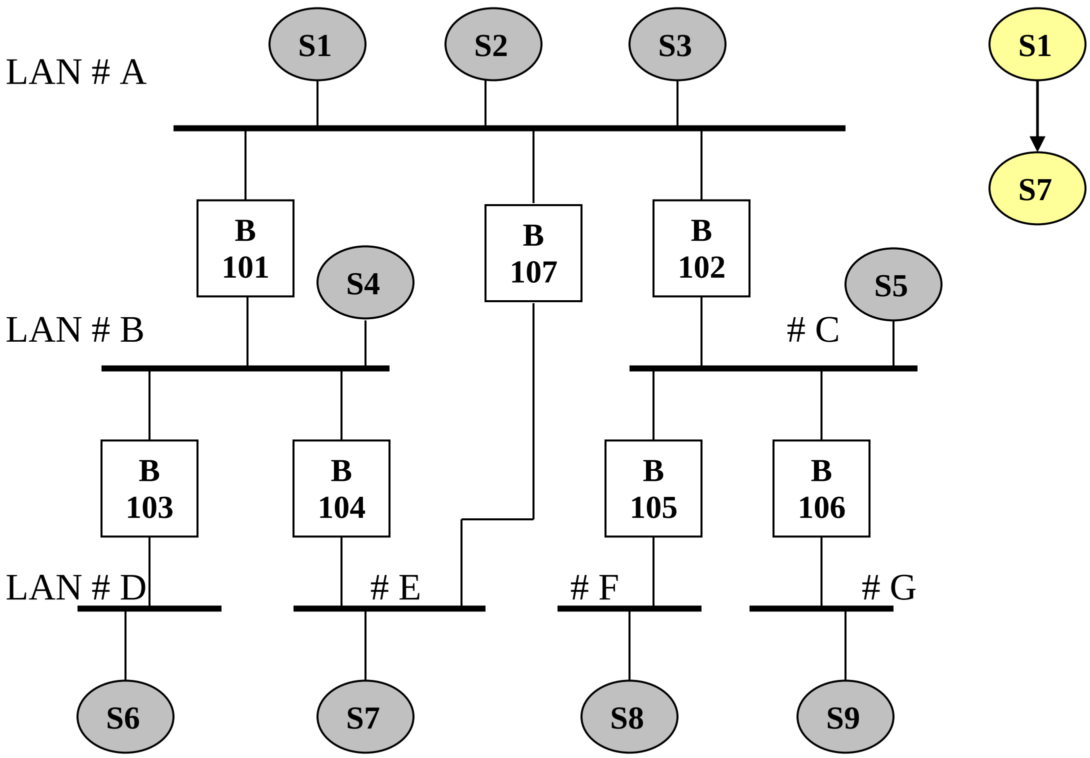




<u>Routing with Bridges: (a)</u>



(b)



Disadvantages of Bridges

1. Bridges process information about the data they receive, which can slow performance.
2. Bridges pass all broadcasts.
3. They cost more than repeaters due to extra intelligence.

Routing

The Network layer is responsible for routing packets across a network. For packets to be correctly routed there needs to be a table setup to show the shortest routes between two networks. These tables can either be dynamic or static.

Static routing tables are set up manually by administrators.

Dynamic routing protocols use one of two methods to define the shortest route without administrator support.

Distance Vector
Link State

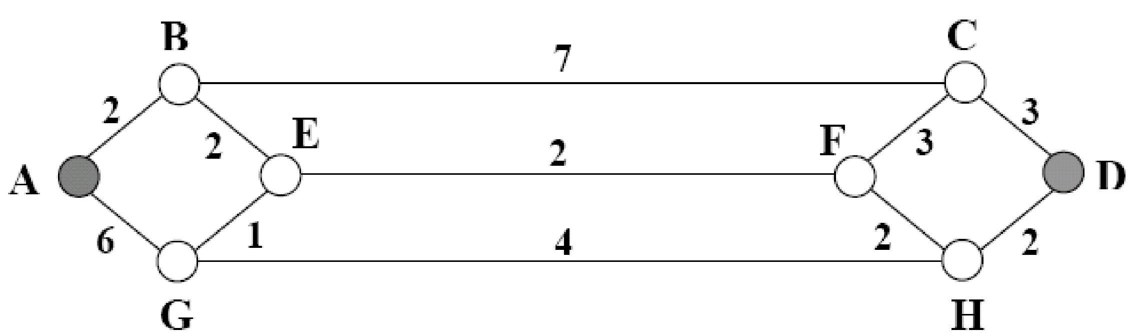
Routing Algorithms

(a) Shortest Path Routing

The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph representing a communication line. To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.

One-way of measuring path length is the number of hops.

There are also other metrics to find out the shortest path Routing. Physical distance and time delay in milliseconds.



Distance Vector Routing

Modern computer networks generally use dynamic routing algorithms. Two dynamic algorithms in particular, distance vector routing and link state routing, are the most popular.

Distance Vector Routing algorithms operate by having each router maintain a table giving the best-known distance to each destination and which line to use to get there. These tables are updated by exchanging information with the neighbors. Each router maintains a routing table indexed by, and containing one entry for each router in the subnet. If the metric is delay, the router can measure it directly with special ECHO packets that the receiver just timestamps and sends back as fast as it can.

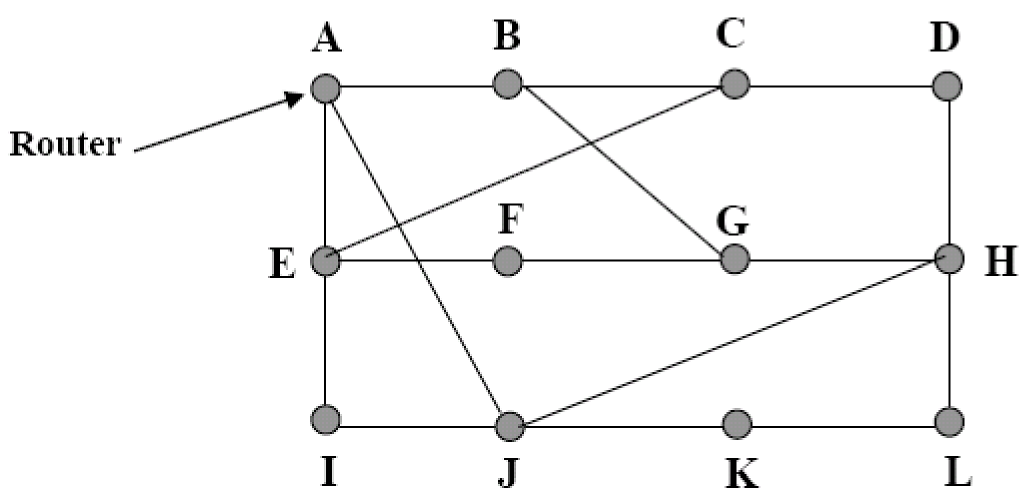
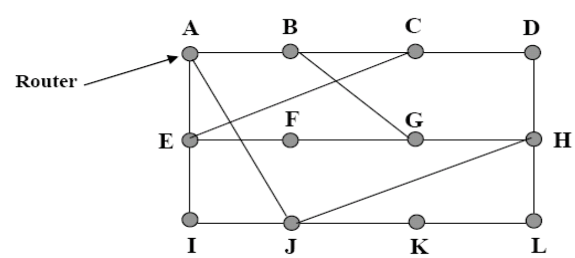


Figure shows the delay vectors received from the neighbors of router ***J***. ***A*** claims to have a 12-msec delay to ***B***, a 25-msec delay to ***C*** etc. Suppose that ***J*** has measured or estimated its delay to its neighbors, ***A***, ***I***, ***H*** and ***K*** as 8, 10, 12 and 6-msec.

Consider how ***J*** computes its new route to router *G*.

	A	I	H	K		Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	-
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is **8**	**JI** delay is **10**	**JH** delay is **12**	**JK** delay is **6**	New Routing table for **J**	

Vector Table received from J's four neighbors.

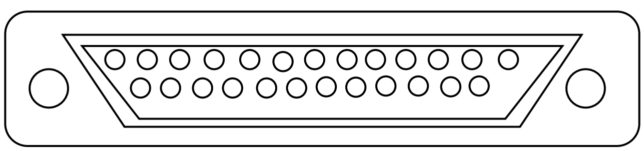


Interface Standards

The point at which one device connects to another is known as an interface. An interface standard defines exactly which electronics signals are required for communication between two devices.

The RS-232-C Standard

One of the most common interface standards for data communications in use today is EIA's *Recommended Standard* is RS-232-C. RS-232-C defines exactly how ones and zeros are to be electronically transmitted.



DB25 male connector

RS-232-C Voltage Level

RS-232-C defines "sending a 1," known as mark, as an electronic signal between –3 and –15 volts. It defines "sending a 0," known as a space, as an electronic signal between +3 and +15 volts.
Signals outside these ranges are considered undefined, neither a one nor a zero, and are ignored by the receiver.

DTEs and DCEs in RS-232-C

RS-232-C assumes that there are two types of interfaces. The first, known as *data terminal equipment* (DTE), is the interface most often found on terminals, host computers and printers. The second known

as *data circuit-terminating equipment* (DCE), is the interface usually used on devices known as modems and multiplexers.
RS-232-C specifies the signals exchanged between DTEs and DCEs, by using a certain type of physical connector. For most applications, the DB25 connector. There are two versions of the DB25 connector, male and female. The male connector contains the 25 pins, and the female connector contains 25 small sockets for these pins. Each of the pins and their corresponding sockets are numbered from 1 to 25.

Pin	Abbreviation	Name
1	GND	Protective Ground.
2	TD	Transmitted Data.
3	RD	Received Data.
4	RTS	Request to send.
5	CTS	Clear to send.
6	DSR	Data set ready.
7	SG	Signal Ground.
8	DCD	Data Carrier Detect.
9		Positive Test Voltage.
10		Negative Test Voltage.
11		Unassigned.
12	SDCD	Secondary Data Carrier Detect.
13	SCTS	Secondary Clear to Send.
14	STD	Secondary Transmitted Data.
15	TC	Transmit Clock.
16	SRD	Secondary Received Data.
17	RC	Receive Clock.
18		Unassigned.
19	SRTS	Secondary request to Send.
20	DTR	Data Terminal Ready.
21	SQ	Signal Quality Detect.
22	RI	Ring Indicator.
23	DRS	Data Rate Select.
24	XTC	External Transmit Clock.
25		Unassigned.

RS-232-C data signal definitions

DTE sends data on the TD (Transmitted Data Pin). It is found on pin number 2 of the DB25 connector.
DTE receives data on the RD (Received Data Pin). Notice that the pins are named with respect to the DTE. The DCE receives data from the DTE on the TD pin, and sends data to the DTE on the RD pin. DTE usually uses the male connector with pins. RD is found on pin number 3.

RS-232-C ground signal definitions

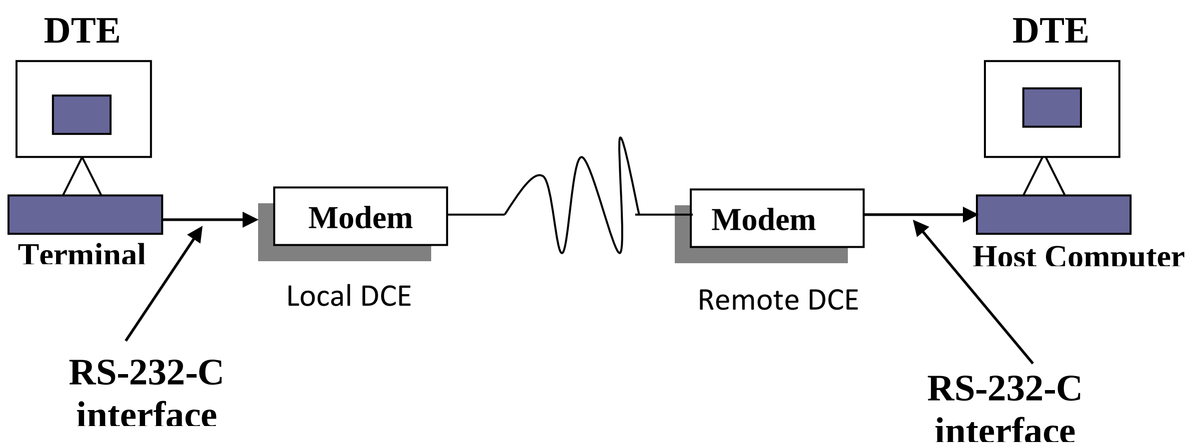
This signals acts as a zero volt reference for all the other signals. When a DTE sends a signal on the TD pin, the DCE compares this voltage to the SG pin to determine whether the data sent was a 1 or a 0. SG is found on pin number 7.
GND is protective ground used to reduce interference and electronic noise. It is found on pin number 1.

RS-232-C control signal definitions

Using the TD, RD and SG pins data could be transmitted between DTEs and DCEs.
When a DTE device is powered on and placed on line, it asserts the DTR (Data terminal ready) signal, this is an announcement to the DCE that a DTE is attached and ready to begin communications. DTR is found on pin number 20.
The DSR (Data set ready) is asserted by the DEC in response to RTS (Request to send) on pin 4 when the DCE is able to accept data from the DTE. CST is found on pin number 5.
The RI (Ring indicator) signal is asserted by the DCE to alert the DTE that a remote device wants to initiate communications. RI is found on pin number 22 of DB25 connector.

RS-232-C HANDSHAKING

Assume that we have a terminal (DTE) connected to a DCE, which we refer to as the local DCE as shown in fig. This DCE communicates with another DCE, known as remote DCE, which is in turn connected to a host computer (DTE).



Connecting DTEs and DCEs with RS-232-C

The terminal is powered up and immediately asserts the DTR (Data terminal ready) signal. The local DCE responds by asserting the DSR (Data set ready) signal, and establishes communications with the remote DCE. The remote DCE alert the host computer that another party would like to communicate with it by asserting RI (Ring indicator) signal. The host computer, if powered on and ready, then asserts the DTR (Data terminal ready) signal. The remote DCE responds by dropping the RI (Ring indicator) signal and asserting the DTR (Data set ready) signal, completing the connection between the terminal and host computer.

After receiving the DSR (Data set ready) signal from the DCE, they almost immediately would have asserted the RTS (Request to send) signal. The purpose of the RTS signal is to request a transmission path. The DCEs would then respond with the CTS (Clear to send) and DCD (Data carrier detect) signals as soon as communications were established between the DCEs. The CTS signal confirms that a transmission path is available for the DTE to send data to the DCE. The DCD signal confirms that a transmission path is established in the other direction, from the DCE to DTE.

An inserting function is performed by the DCEs during the connection. The terminal transmit data on the TD

(Transmitted data) pin to the local DCE, which sends the data to the remote DCE. The remote DCE sends this data to the host computer on the RD (Receive data) pin. The DCEs have performed *crossover* of the data signal, much as telephone do for us.

Typically, a DTE ends the connection by dropping its DTR and RTS signals.