Unit - 2 - Network Classification

1. Local area network (LAN)

A local area network, or LAN, is the most common network type. It allows users to connect within a short distance in a common area. Once they connect, users have access to the same resources. For example, you might use a LAN when you connect your laptop to the internet at your home and print a document from a printer on the same network.

2. Personal area network (PAN)

A personal area network, or PAN, is a small-scale network that revolves around one person or device. A PAN connects just a few devices in a small localized area. Rather than including many devices, PANs usually operate from one or two main devices. For example, if you use the Bluetooth functionality on your smartphone to share a photo with a nearby device, you're using a PAN.

3. Metropolitan area network (MAN)

A metropolitan area network, or a MAN, is a medium-sized network that's larger than a CAN. While a MAN is a costly network, it provides efficient connectivity between devices across a wide geographical range. For example, a city government might operate with a MAN if it has offices across the entire metropolitan area.

4. Wide area network (WAN)

A wide area network, or a WAN, is an extensive network that's not confined to geographical space. Corporations and international companies may use WANs to provide a common network with far-reaching connectivity. For example, remote workers who use the internet to access information from their company make use of a WAN.

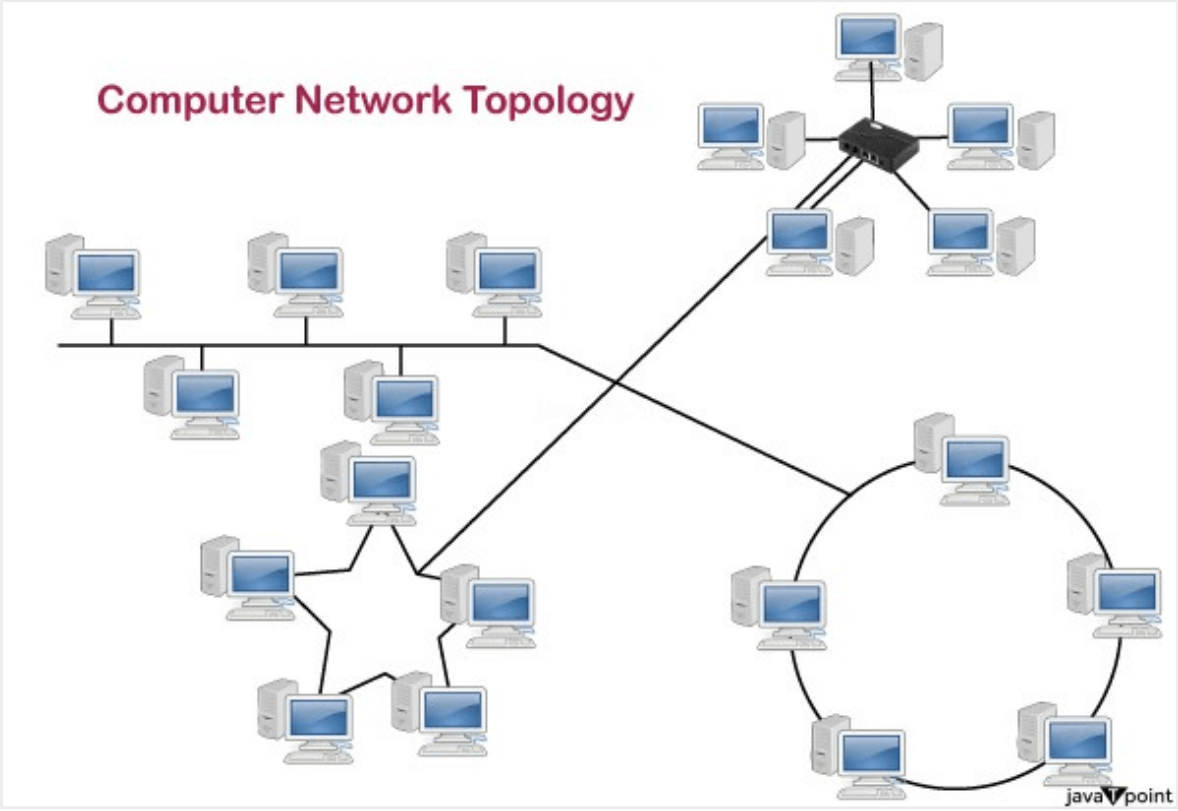
Network Topology

Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

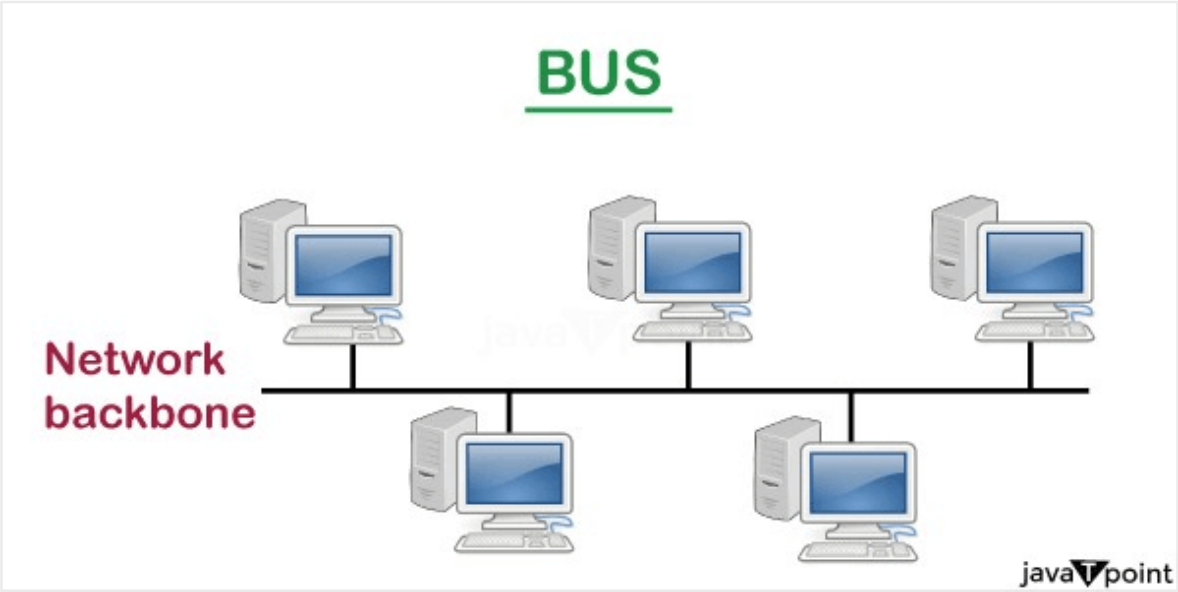
Types of Network Topology

Physical topology is the geometric representation of all the nodes in a network. There are six types of network topology which are Bus

Topology, Ring Topology, Tree Topology, Star Topology, Mesh Topology, and Hybrid Topology.



1) Bus Topology



- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in

the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

CSMA: It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

- **CSMA CD:** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
- **CSMA CA: CSMA CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

Advantages of Bus topology:

- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

2) Ring Topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.
    - **Token passing:** It is a network access method in which token is passed from one node to another node.

    - **Token:** It is a frame that circulates around the network.

Working of Token passing

- A token moves around the network, and it is passed from computer to computer until it reaches the destination.
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- In a ring topology, a token is used as a carrier.

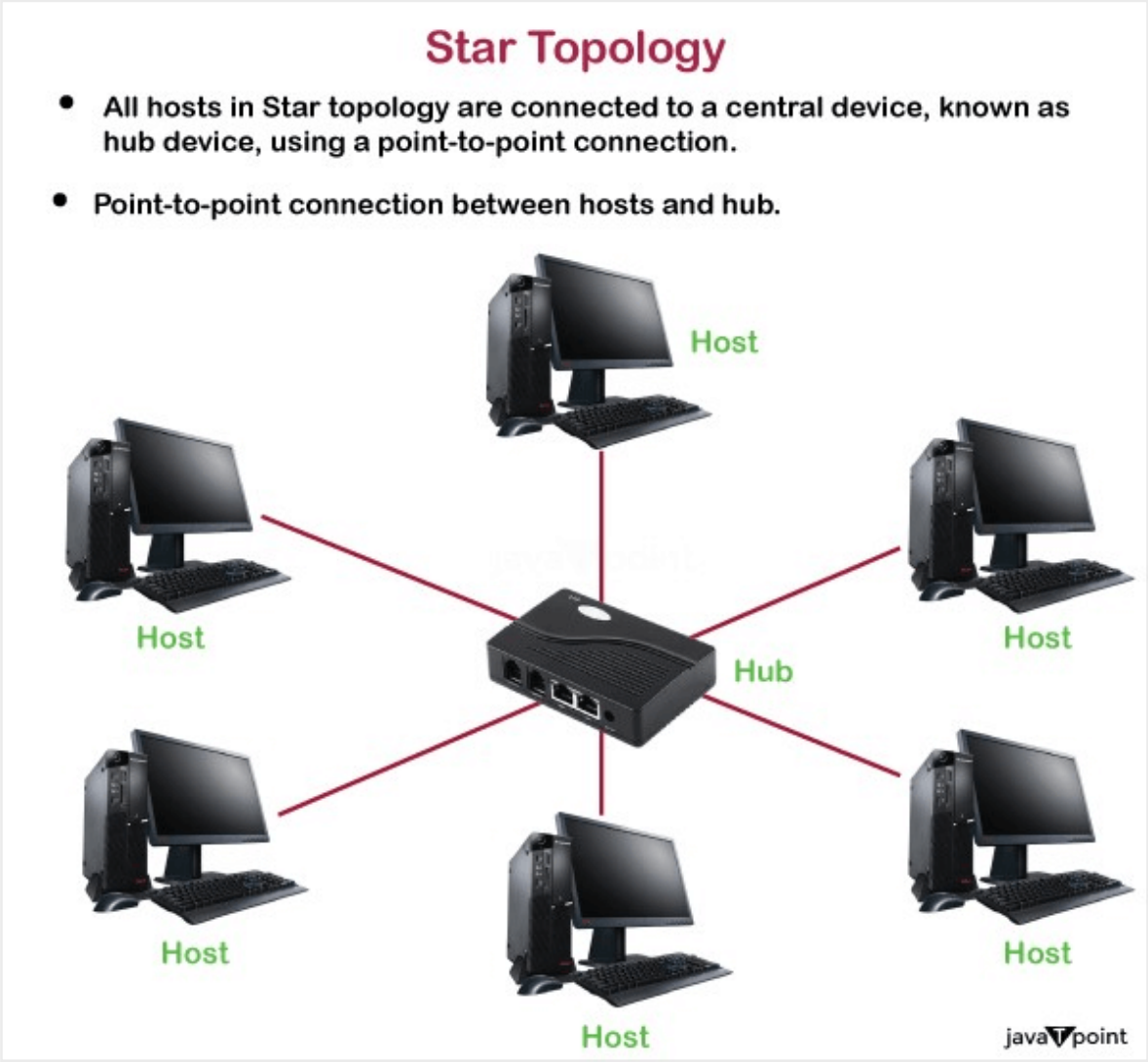
Advantages of Ring topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

3) Star Topology



- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

Advantages of Star topology

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable.

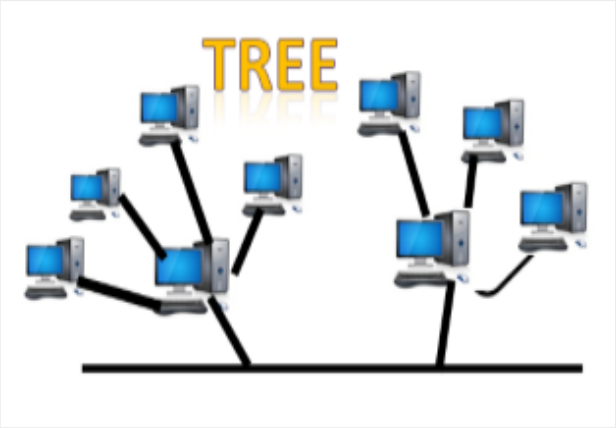
In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.

- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

4) Tree topology



- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.

- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

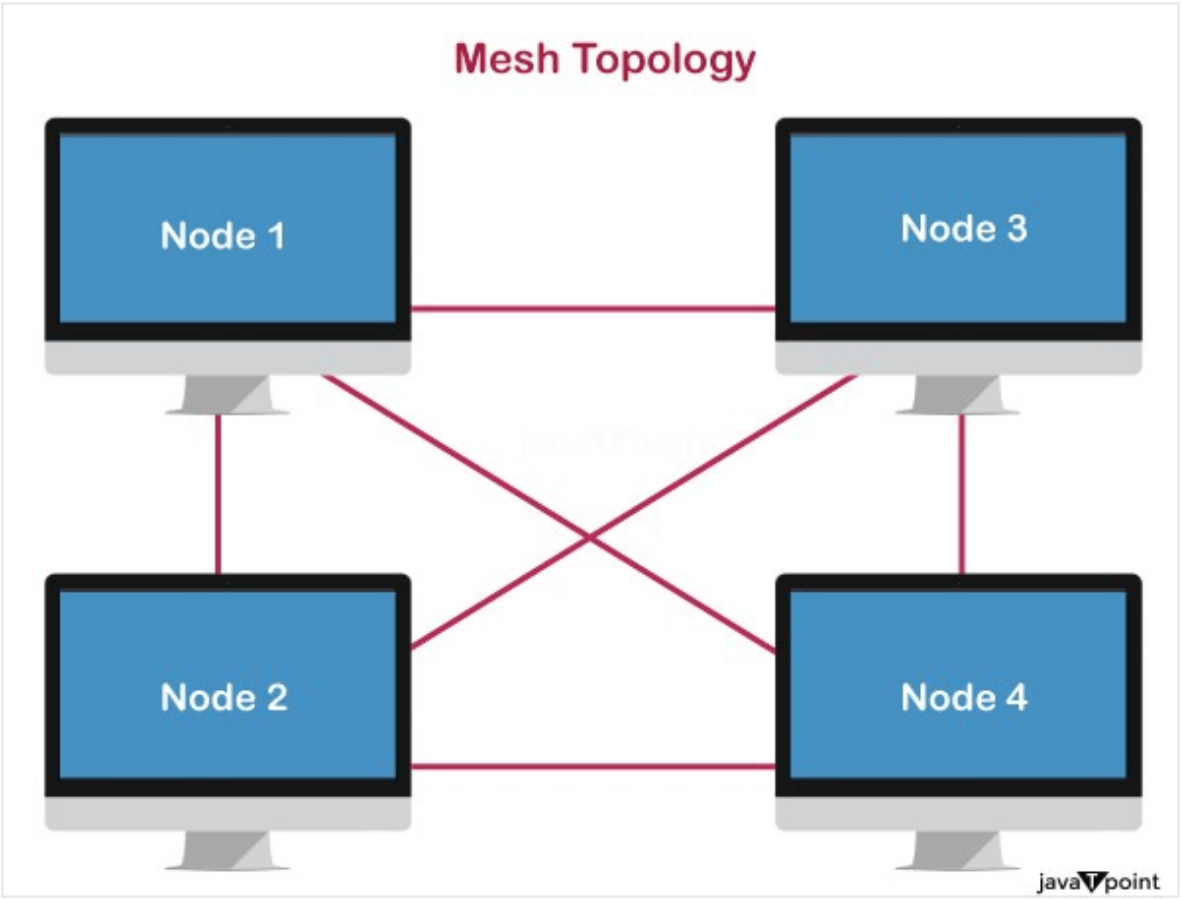
Advantages of Tree topology

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

5) Mesh topology

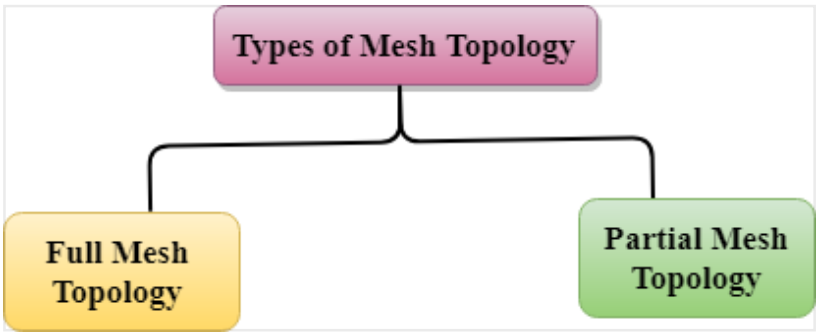


- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula: **Number of cables = (n*(n-1))/2;**

Where n is the number of nodes that represents the network.

Mesh topology is divided into two categories:

- Fully connected mesh topology
- Partially connected mesh topology

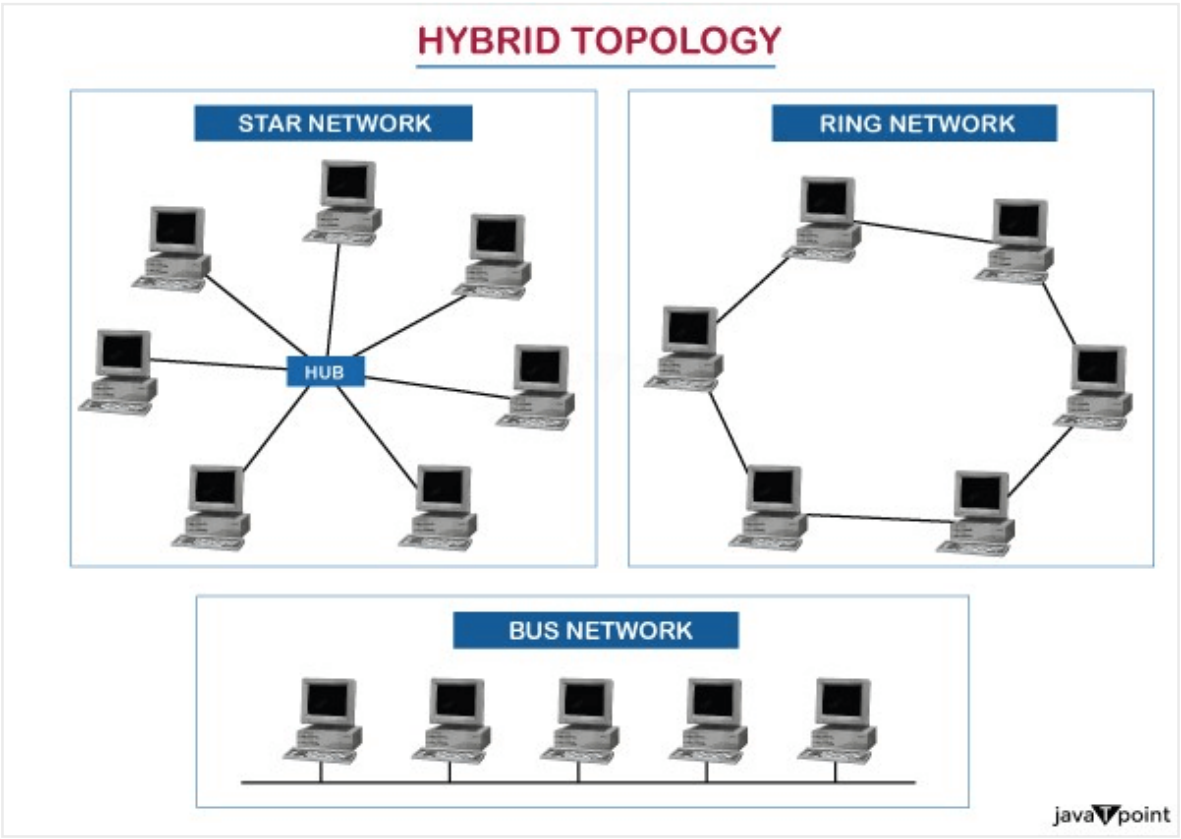


- **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
- **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

Advantages of Mesh topology:
Reliable: The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.
Fast Communication: Communication is very fast between the nodes.
Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices.
Disadvantages of Mesh topology

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

6) Hybrid Topology



- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages of Hybrid topology

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

Next TopicTransmission modes

Difference between Internet, Intranet and Extranet

Networks are crucial in today's globalized world because they allow the acquisition, exchange, and organization of knowledge. Of all the first order networks the Internet, Intranet, and Extranet are commonly utilized for various applications. Every network type meets specific roles that are required in connecting the global population, and internal organization, and secure communication with external subjects. About these networks, this article will aim at identifying their fundamental and specific applications.

What is the Internet?

The Internet is a huge network of millions of computers and related devices from all corners of the globe through which users are able to communicate, exchange information, and partake in general resources. Its mechanism is more decentralized and does not have a specific owner; it works only as a common idea shared by various institutions, governments, and users. The Internet is the tool that links people, companies, and organizations, offering various opportunities for cooperation and development, as well as offering various possibilities to find the necessary information, using Internet resources, such as websites and services, research data, and social networks.

What is an Intranet?

An Intranet is a local area network that has been designed for use within an organization by its employees to share information as well as work together. An Intranet is also constructed from the technologies of the Internet from TCP/IP, HTTP, and web browsers but exist behind a security firewall and has only a limited number of authorized users. Its use is to enhance the cooperation internally, control the distribution of facilities and to work more effectively. These include company news that include the latest updates posted internally to and including personnel directories, project management applications and access to databases all of which assist the organization in enhancing its efficiency.

What is Extranet ?

An Extranet is an extended form of an Intranet that enables secure communication and collaboration between an organization and external entities, such as suppliers, partners, or clients. While it uses Internet protocols to facilitate connectivity, an Extranet is controlled and accessible only to authorized users with login credentials. The primary purpose of an Extranet is to extend the reach of internal resources to trusted external users while maintaining security through firewalls, encryption, and access control measures.

Difference between Internet, Intranet and Extranet

Point of difference	Internet	Intranet	Extranet
Accessibility of network	Public	Private	Private
Availability	Global system.	Specific to an organization.	To share information with suppliers and vendors it makes the use of public network.

Coverage	All over the world.	Restricted area upto an organization.	Restricted area upto an organization and some of its stakeholders or so.
Accessibility of content	It is accessible to everyone connected.	It is accessible only to the members of organization.	Accessible only to the members of organization and external members with logins.
No. of computers connected	It is largest in number of connected devices.	The minimal number of devices are connected.	The connected devices are more comparable with Intranet.
Owner	No one.	Single organization.	Single/ Multiple organization.
Purpose of the network	It’s purpose is to share information throughout the world.	It’s purpose is to share information throughout the organization.	It’s purpose is to share information between members and external, members.
Security	It is dependent on the user of the device connected to network.	It is enforced via firewall.	It is enforced via firewall that separates internet and extranet.

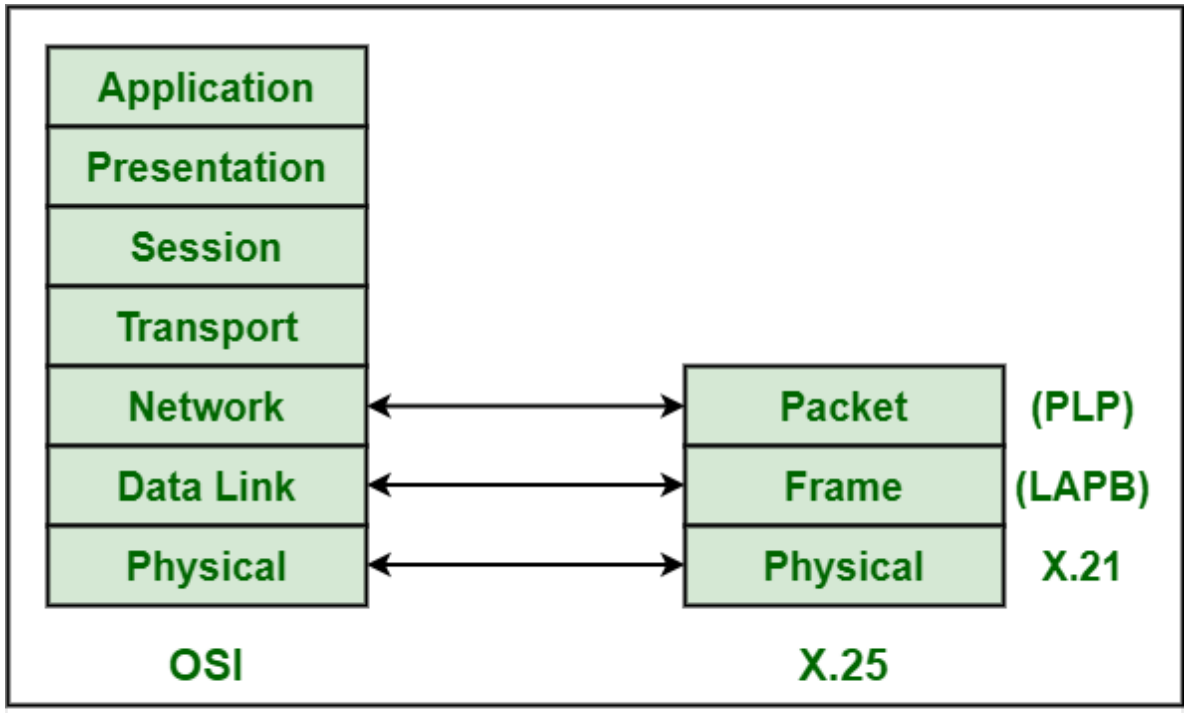
Users	General public.	Employees of the organization.	Employees of the organization which are connected.
Policies behind setup	There is no hard and fast rule for policies.	Policies of the organization are imposed.	Policies of the organization are imposed.
Maintenance	It is maintained by ISP.	It is maintained by CIO. HR or communication department of an organization.	It is maintained by CIO. HR or communication department of an organization.
Economical	It is more economical to use.	It is less economical.	It is also less economical.
Relation	It is the network of networks.	It is derived from Internet.	It is derived from Intranet.
Example	What we are normally using is internet.	WIPRO using internal network for its business operations.	DELL and Intel using network for its business operations.

X.25

X.25 is generally a protocol that was developed by Telecommunication Standardization Sector (ITU-T) of International Telecommunication Union. It usually allows various logical channels to make use of same physical line. It basically defines a series of documents particularly issued by ITU. These documents are also known as X.25 Recommendations. X.25 also supports various conversations by multiplexing packets and also with the help of virtual communication channels. X.25 basically encompasses or suits to the lower three layers of the Open System Interconnection (OSI)

reference model for networking. These three protocol layers are :

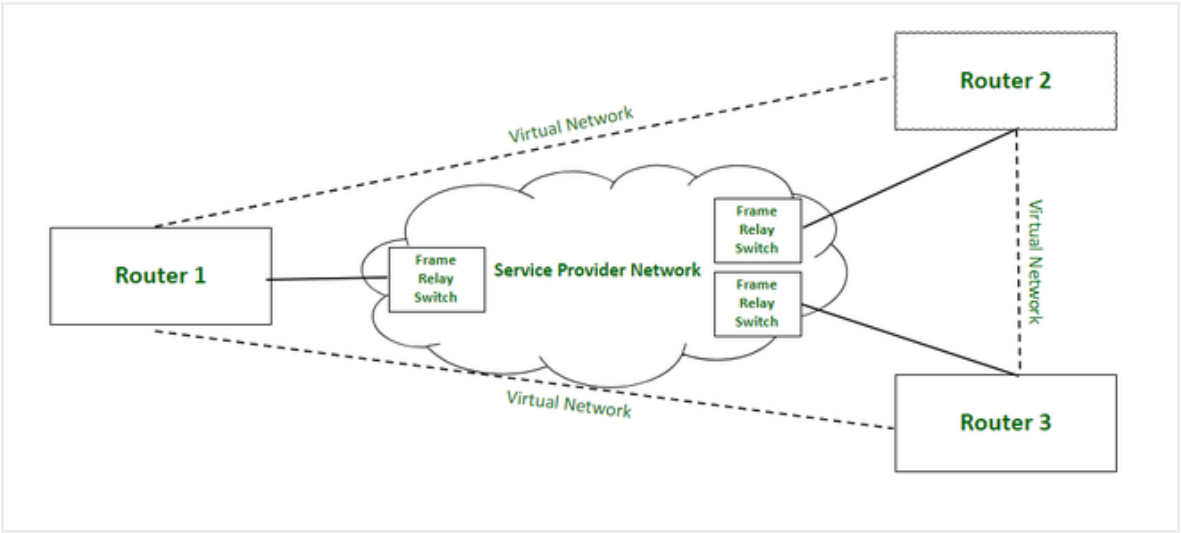
1. Physical Layer
2. Frame Layer
3. Packet Layer



X.25 Layer Mapping with OSI Model

Frame Relay Work

Frame Relay is a packet-switching network protocol that is designed to work at the data link layer of the network. It is used to connect Local Area Networks (LANs) and transmit data across Wide Area Networks (WANs). It is a better alternative to a point-to-point network for connecting multiple nodes that require separate dedicated links to be established between each pair of nodes. It allows transmission of different size packets and dynamic bandwidth allocation. Also, it provides a congestion control mechanism to reduce the network overheads due to congestion. It does not have an error control and flow management mechanism.



Frame Relay Network

Working:

Frame relay switches set up virtual circuits to connect multiple LANs to build a WAN. Frame relay transfers data between LANs across WAN by dividing the data in packets known as frames and transmitting these packets across the network. It supports communication with multiple LANs over the shared physical links or private lines.

Frame relay network is established between Local Area Networks (LANs) border devices such as routers and service provider network that connects all the LAN networks. Each LAN has an access link that connects routers of LAN to the service provider network terminated by the frame relay switch. The access link is the private physical link used for communication with other LAN networks over WAN. The frame relay switch is responsible for terminating the access link and providing frame relay services.

For data transmission, LAN's router (or other border device linked with access link) sends the data packets over the access link. The packet sent by LAN is examined by a frame relay switch to get the Data Link Connection Identifier (DLCI) which indicates the destination of the packet. Frame relay switch already has the information about addresses of the LANs connected to the network hence it identifies the destination LAN by looking at DLCI of the data packet. DLCI basically identifies the virtual circuit (i.e. logical path between nodes that doesn't really exist) between source and destination network. It configures and transmits the packet to frame relay switch of destination LAN which in turn transfers the data packet to destination LAN by sending it over its respective access link. Hence, in this way, a LAN is connected with multiple other LANs by sharing a single physical link for data transmission.

Frame relay also deals with congestion within a network. Following methods are used to identify congestion within a network:

1. **Forward Explicit Congestion Network (FECN) –**
   FECN is a part of the frame header that is used to notify the destination about the congestion in the network. Whenever a frame experiences congestion while transmission, the frame relay switch of the destination network sets the FECN bit of the packet that allows the destination to identify that packet has experienced some congestion while transmission.
2. **Backward Explicit Congestion Network (BECN) –**
   BECN is a part of the frame header that is used to notify the source about the congestion in the network. Whenever a frame experiences congestion while transmission, the destination sends a frame back to the source with a set BECN bit that allows the source to identify that packet that was transmitted had experienced some congestion while reaching out to the destination. Once, source identifies congestion in the virtual circuit, it slows down to transmission to avoid network overhead.
3. **Discard Eligibility (DE) –**
   DE is a part of the frame header that is used to indicate the priority for discarding the packets. If the source is generating a huge amount of traffic on the certain virtual network then it can set DE bits of less significant packets to indicate the high priority for discarding the packets in case of network overhead. Packets with set DE bits are discarded before the packets with unset DE bits in case of congestion within a network.

Types:

1. **Permanent Virtual Circuit (PVC) –**
   These are the permanent connections between frame relay nodes that exist for long durations. They are always available for communication even if they are not in use. These connections are static and do not change with time.
2. **Switched Virtual Circuit (SVC) –**
   These are the temporary connections between frame relay nodes that exist for the duration for which nodes are communicating with each other and are closed/ discarded after the communication. These connections are dynamically established as per the requirements.

Advantages:

1. High speed
2. Scalable
3. Reduced network congestion
4. Cost-efficient
5. Secured connection

Disadvantages:

1. Lacks error control mechanism
2. Delay in packet transfer
3. Less reliable

Fast Ethernet

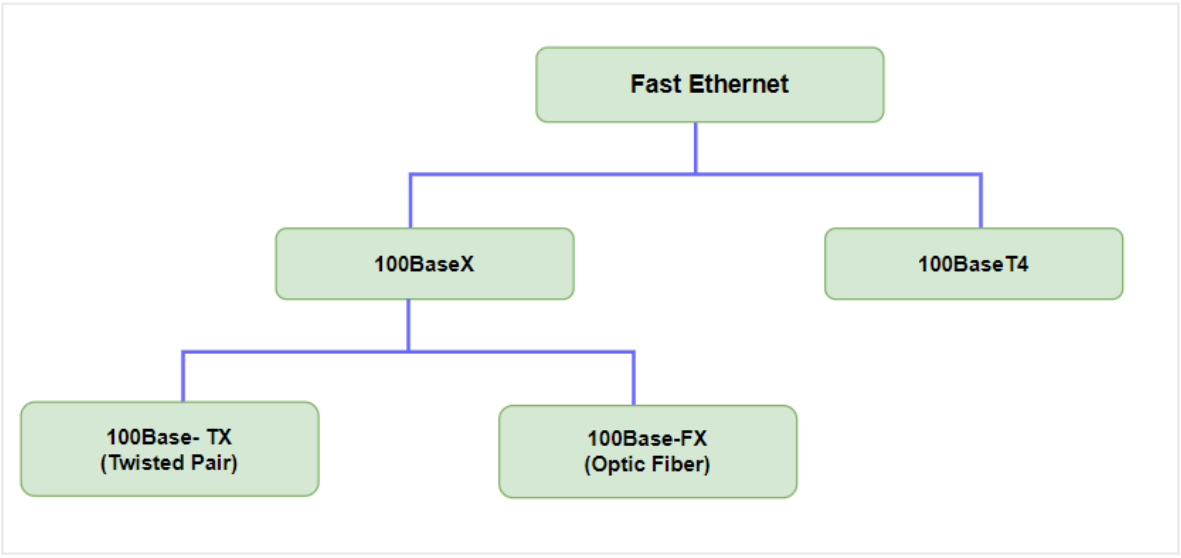
Fast Ethernet is a networking technology which is enhancement of traditional ethernet by increasing the data transfer rates. Fast Ethernet represents a huge development over traditional Ethernet, addressing the growing demand for better data transfer rates in networking environments. The original Ethernet standard, defined by means of the Institute of Electrical and Electronics Engineers (IEEE) 802.3 specification, operated at a speed of 10 Mbps. However, because the call for faster network speeds grew, the need for an advanced Ethernet standards became apparent.

Fast Ethernet, standardized below the IEEE 802.3u specification, brought several enhancements to get its higher data transfer rates. One of the key improvements changed into the use of different signaling methods and media types compared to traditional Ethernet. Fast Ethernet helps both twisted pair and fiber optic cabling.

Types of Fast Ethernet

Fast Ethernet is mainly of several types or standards, each having their own specifications, implementations and characteristics. The two most common types of Fast Ethernet are:

- 100Base-TX
- 100Base-FX



1. 100Base-TX

- 100Base-TX utilizes twisted pair copper cabling specified as Cat5e cables for the ease of data transmission.
- It is mainly used in Local Area Networks(LANs)
- It works on both Full duplex and Half Duplex Modes and it supports data transfer rates up to 100 Mbps.
- This is used in the connecting devices like computers. printers and LAN environment.

2. 100Base-FX

- 100Base-FX is another type of Fast Ethernet that is in different cabling which is fiber optic cabling for Data transmission
- It is mainly used in long run cables of range 120 Kms and it requires electro magnetic interference.
- It supports up to 100 Mbps of DTR and it also offers the higher bandwidth.
- This is used commonly in connecting devices across different buildings or in the environment where copper cabling is out of reach.

Significance of Fast Ethernet

The Significance of Fast Ethernet lies in the impact on networking capabilities, performance and Efficiency. Some Key points mentioned are the significance of Fast Ethernet below:

- Increased Data Transfer Rates
- Enhanced Network Performance
- Cost Effectiveness
- Scalability
- Flexibility

- Support for Bandwidth intensive applications (Video Conferencing, Multimedia streaming, Large File Transfers).

Applications of Fast Ethernet

The applications of Fast Ethernet are diverse in various industries and scenarios. The following are some of the applications for Fast Ethernet:

- **Data Centers:** Fast Ethernet is commonly deployed in data center environments to connect servers, storage devices, and networking equipment. It facilitates rapid data transfer between servers and storage arrays, supporting mission-critical applications and services hosted in the data center.
- **Surveillance Systems:** Fast Ethernet is utilized in surveillance systems for transmitting high-definition video feeds from IP cameras to monitoring stations or recording devices. It ensures real-time monitoring and recording of surveillance footage, enhancing security and surveillance capabilities.
- **Educational Institutions:** Fast Ethernet is employed in educational institutions, such as schools and universities, to support networked learning environments. It enables access to online educational resources, collaborative tools, and e-learning platforms, enriching the educational experience for students and educators.
- **Telecommunications:** Fast Ethernet is used in telecommunications networks for backhaul connections between central offices, cell towers, and network aggregation points. It enables the efficient transfer of voice, data, and video traffic over large-scale telecommunications networks.

Narrowband ISDN (N-ISDN) and Broadband ISDN (B-ISDN)

Are two types of Integrated Services Digital Network (ISDN), a set of communications standards for transmitting voice, data, and video over digital lines.

Narrowband ISDN (N-ISDN):

- Designed for voice and low-speed data transmission.
- Uses a basic rate interface (BRI) with two 64 kbps B-channels and one 16 kbps D-channel.

- Primarily used for traditional phone services and low-speed data connections.

Broadband ISDN (B-ISDN):

- Designed for high-speed data, video, and multimedia applications.
- Uses a much higher bandwidth than N-ISDN.
- Relies on Asynchronous Transfer Mode (ATM) technology for efficient data transfer.
- Offers a wide range of services, including video conferencing, teleconferencing, and high-speed internet access.

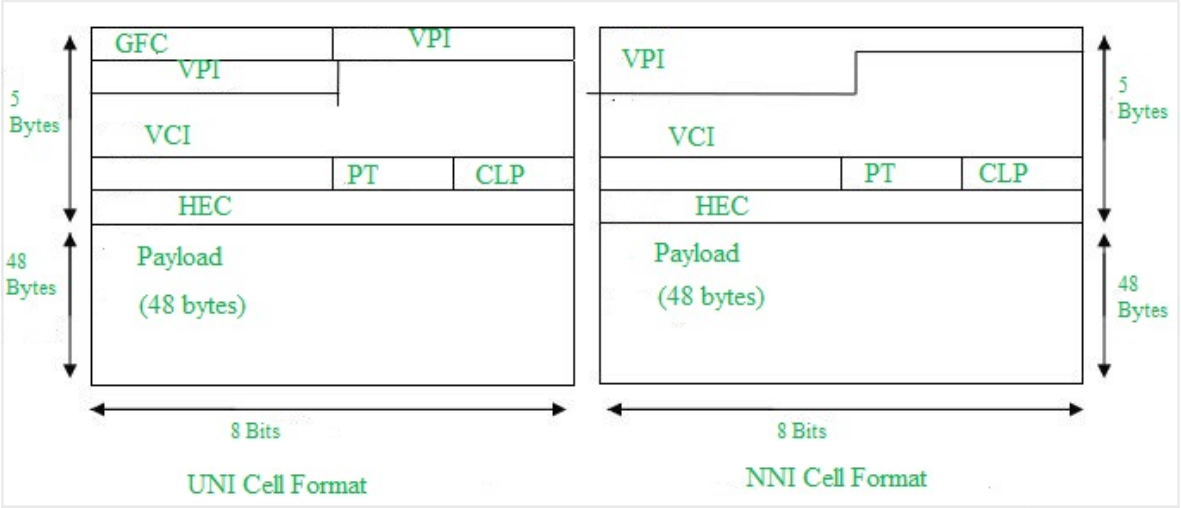
Key Differences:

Feature	Narrowband ISDN (N-ISDN)	Broadband ISDN (B-ISDN)
Bandwidth	Low	High
Technology	Circuit-switched	Cell-switched (ATM)
Applications	Voice, low-speed data	High-speed data, video, multimedia
Infrastructure	Existing copper networks	Fiber-optic networks

Export to Sheets

Asynchronous Transfer Mode (ATM) in Computer Network

-> It usually used in multimedia transfer in televisions etc
-> It has 32 bit local header and 20bytes global NASP header
-> It established a connection before transferring the data
-> It sends packets in a sequence one by one.
-> It also have pic (permamnent virtual connection) w can use that too for data transfer.
-> Its packets are of fixed or small size
-> It packets are transferred in form of cell of total size 53 bytes
-> 4 header bytes & 48 data bytes .
-> It can transmit videos and images data
-> Cause it uses asynchronous time division multiplexing that why we called it asynchronous transfer mode.



1. Driven by the integration of services and performance requirements of both telephony and data networking: “broadband integrated service vision” (B-ISON).

2. Telephone networks support a single quality of service and are expensive to boot.

3. Internet supports no quality of service but is flexible and cheap.

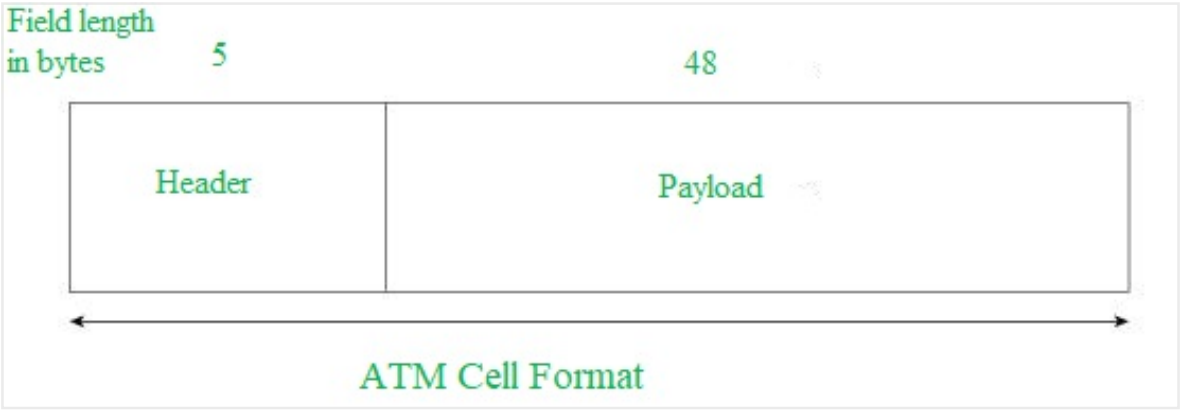
4. ATM networks were meant to support a range of service qualities at a reasonable cost- intended to subsume both the telephone network and the Internet.

Asynchronous Transfer Mode (ATM):
It is an International Telecommunication Union- Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video, or voice which is conveyed in small fixed-size packets called cells. Cells are transmitted asynchronously and the network is connection-oriented.
ATM is a technology that has some event in the development of broadband ISDN in the 1970s and 1980s, which can be considered an evolution of packet switching. *Each cell is 53 bytes long* – 5 bytes header and 48 bytes payload. Making an ATM call requires first sending a message to set up a connection.
Subsequently, all cells follow the same path to the destination. It can handle both constant rate traffic and variable rate traffic. Thus it can carry multiple types of traffic with **end-to-end** quality of service.
ATM is independent of a transmission medium, they may be sent on a

wire or fiber by themselves or they may also be packaged inside the payload of other carrier systems. ATM networks use “Packet” or “cell” Switching with virtual circuits. Its design helps in the implementation of high-performance multimedia networking.

ATM Cell Format –

As information is transmitted in ATM in the form of fixed-size units called **cells**. As known already each cell is 53 bytes long which consists of a 5 bytes header and 48 bytes payload.



Asynchronous Transfer Mode can be of two format types which are as follows:

1. **UNI Header:** This is used within private networks of ATMs for communication between ATM endpoints and ATM switches. It includes the Generic Flow Control (GFC) field.

2. **NNI Header:** is used for communication between ATM switches, and it does not include the Generic Flow Control(GFC) instead it includes a Virtual Path Identifier (VPI) which occupies the first 12 bits.

Working of ATM:

ATM standard uses two types of connections. i.e., Virtual path connections (VPCs) which consist of Virtual channel connections (VCCs) bundled together which is a basic unit carrying a single stream of cells from user to user. A virtual path can be created end-to-end across an ATM network, as it does not rout the cells to a particular virtual circuit. In case of major failure, all cells belonging to a particular virtual path are routed the same way through the ATM network, thus helping in faster recovery.

Switches connected to subscribers use both VPIs and VCIs to switch the cells which are Virtual Path and Virtual Connection switches that can have different virtual channel connections between them, serving

the purpose of creating a *virtual trunk* between the switches which can be handled as a single entity. Its basic operation is straightforward by looking up the connection value in the local translation table determining the outgoing port of the connection and the new VPI/VCI value of connection on that link.

ATM vs DATA Networks (Internet) –

- ATM is a “virtual circuit” based: the path is reserved before transmission. While Internet Protocol (IP) is connectionless and end-to-end resource reservations are not possible. RSVP is a new signaling protocol on the internet.
- ATM Cells: Fixed or small size and Tradeoff is between voice or data. While IP packets are of variable size.
- Addressing: ATM uses 20-byte global NSAP addresses for signaling and 32-bit locally assigned labels in cells. While IP uses 32-bit global addresses in all packets.