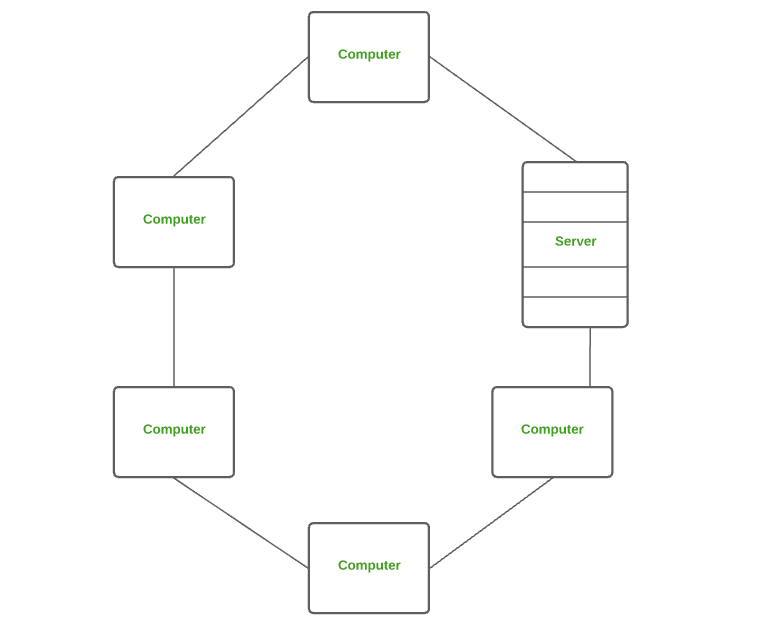
Computer Networking

UNIT-3 NOTES

A Local Area Network (LAN) is the backbone of modern connectivity, seamlessly linking computers and devices within a confined geographic area such as an office, campus, or building. Functioning as an intricate web of interconnected nodes, a LAN enables the efficient sharing of resources, information, and services among its connected devices. This localized network infrastructure facilitates collaborative work environments, streamlined communication, and resource optimization, thereby fostering productivity and connectivity on a small-scale level. Whether in homes, businesses, or educational institutions, LANs play a pivotal role in shaping the landscape of contemporary digital communication, offering a reliable and swift means for devices to interact and exchange data within designated proximity. As technology continues to evolve, the importance of LANs remains paramount, providing the foundation for numerous applications and innovations that drive the interconnected world we inhabit today.



## 1.1 What is Local Area Network (LAN)?

A Local Area Network (LAN) is a computer network that connects devices within a relatively small geographic area, such as a building, office, or campus. It is a communication infrastructure allowing computers, printers, servers, and storage devices to share resources and exchange information seamlessly. LANs can be established using wired technologies like Ethernet cables or wireless technologies like Wi-Fi. They are commonly used in homes, offices, schools, and other localized environments to facilitate efficient data transfer, resource sharing, and collaboration among network users. LANs are characterized by high data transfer rates, localized administration and management, the ability to share resources, and security features to protect the network and its data. Components of Local Area Network

**Some key features and characteristics of LANs include:**

* Limited geographic area: LANs cover a relatively small area, such as a building, office, or campus.
* High data transfer rates: LANs provide fast communication and data sharing between devices within the network.
* Shared resources: LANs allow devices to share resources like printers, storage devices, and internet connections.
* Local administration and management: LANs are managed by local administrators for maintenance, security, and user management.
* Ethernet and TCP/IP: Ethernet is the common technology used for wired LAN connections, while TCP/IP is the standard protocol suite for LAN communication.
* Security measures: LANs incorporate security measures like firewalls, access control, encryption, and VPNs to protect against unauthorized access and data breaches.

LANs are crucial in facilitating local communication and resource sharing, making them essential for various applications, including home networking, office environments, educational institutions, and small to medium-sized businesses.

## **1.2 Using a Local Area Network (LAN) offers several benefits:**

1. LANs allow for efficient sharing of network resources such as printers, scanners, and storage devices. Multiple users can access these resources, eliminating the need for individual devices and reducing costs.
2. LANs facilitate seamless communication and collaboration among users. Users can easily share files, exchange information, and communicate through instant messaging, email, or video conferencing tools. This promotes teamwork, knowledge sharing, and efficient workflow.
3. LANs provide fast data transfer rates within the network. This enables quick access to shared files, applications, and network resources, enhancing productivity and reducing delays in data transmission.
4. LANs can be centrally managed, allowing administrators to monitor and control network operations efficiently. This simplifies tasks such as user management, security configurations, and software updates, improving network stability and making troubleshooting easier.
5. LANs can implement security measures to protect against unauthorized access and data breaches. Firewalls, access controls, and encryption protocols can be deployed to safeguard sensitive information, ensuring the privacy and integrity of network communications.
6. By sharing resources and centralizing management, LANs can result in cost savings. Organizations can reduce hardware and software expenses by utilizing shared devices and applications, and network administrators can efficiently allocate resources and monitor network usage to optimize costs.
7. LANs can be easily expanded or reconfigured to accommodate changing network needs. New devices can be added, and [network](https://www.lisedunetwork.com/networking-in-library/) settings can be adjusted to adapt to growth or changes in organizational requirements.

## 1.3 Components of Local Area Network (LAN)

A local Area Network (LAN) is made up of three essential elements:

1. Hardware Components
2. Software Components; and
3. The Users.

### 1.3.1 Hardware Components:

The hardware components of a Local Area Network (LAN) include:

* **Devices:** LANs connect various devices such as computers, laptops, servers, printers, switches, routers, network-attached storage (NAS) devices, and other network-enabled devices. These devices are interconnected to facilitate communication and resource sharing within the LAN.
* **Network Interface Cards (NICs)**: Each device connected to the LAN requires a Network Interface Card or network adapter. A NIC is responsible for establishing a physical connection to the LAN. It allows the device to send and receive data packets over the network.
* **Cables and Connectors**: LANs use cables and connectors to establish wired connections between devices. Ethernet cables, such as Cat5e or Cat6, are commonly used. These cables provide the physical medium through which data is transmitted between devices within the LAN.
* **Switches:** Switches are networking devices that connect multiple devices within the LAN. They provide multiple ports to which devices can be connected using Ethernet cables. Switches manage data flow by forwarding data packets to the intended recipient device. They ensure efficient communication between devices within the LAN.
* **Routers:** In larger LANs or networks that require internet connectivity, routers play a vital role. Routers connect different networks, allowing data to be transmitted between the LAN and other networks or the internet. They analyze and route data packets based on the destination IP addresses.
* **Wireless Access Points (WAPs):** In addition to wired connections, LANs can include wireless connectivity through Wireless Access Points (WAPs). WAPs enable devices to connect to the LAN wirelessly using Wi-Fi technology. They provide wireless coverage and allow devices to communicate with each other and access network resources without the need for physical cables.
* **Network Cabinets and Racks:** LANs often utilize network cabinets or racks to house and organize networking equipment. These cabinets provide a centralized location for devices like switches, routers, and servers, ensuring proper cable management, ventilation, and physical security.

These hardware components work together to establish the physical infrastructure of a LAN, enabling devices to communicate, share resources, and access network services within a local area.

## 1.3.2 Software Components:

The software components of a Local Area Network (LAN) include:

* **Network Operating System (NOS):** A LAN may have a dedicated network operating system installed on servers or specialized network devices. The NOS provides the foundation for managing and controlling the network. It allows administrators to configure network settings, manage user accounts, allocate resources, and provide network services such as file sharing, printing, and email.
* **Network Protocols:** LANs rely on network protocols to govern how data is transmitted, addressed, and managed within the network. Common LAN protocols include Ethernet for wired connections and Wi-Fi for wireless connections. TCP/IP (Transmission Control Protocol/Internet Protocol) is the fundamental protocol suite used in LANs, providing the rules and standards for data transmission and addressing.
* **Network Management Software:** LANs often employ network management software to monitor, control, and troubleshoot network performance and configurations. This software lets network administrators view network activity, track device status, manage network security, and analyze network traffic. It facilitates network monitoring, performance optimization, and configuration management.
* **Network Security Software:** LANs implement various software components to enhance network security. This includes firewalls, which control network traffic and protect against unauthorized access; antivirus software, which scans for and prevents malware; intrusion detection/prevention systems (IDS/IPS) that monitor for suspicious network activity; and encryption tools to secure data transmission over the LAN.
* **Application Software:** LANs support a wide range of application software that operates on devices connected to the network. This includes productivity software such as word processors, spreadsheets, presentation tools, and specialized applications for specific purposes like database management, design software, or collaboration tools. Application software enables users to perform tasks and utilize network resources efficiently.
* **Network Services:** LANs provide network services that enhance communication, resource sharing, and collaboration. These services can include file sharing, printing services, email, web browsing, instant messaging, video conferencing, and remote access to network resources. Network services allow users to utilize shared resources and communicate seamlessly within the LAN efficiently.

These software components work in conjunction with the hardware components of a LAN to provide a comprehensive networking environment. They enable network management, secure data transmission, support application functionality, and deliver network services to users within the local area network.

#### The Users:

The users component of a Local Area Network (LAN) refers to the individuals or entities who utilize the network to access resources, communicate, and collaborate within the LAN environment. Here are some key aspects of the users component:

* **Network Users:** These are the individuals or groups of people who connect their devices to the LAN. Network users can include employees within an organization, students in an educational institution, or residents in a residential community. Each user typically has a device, such as a computer or a laptop, to access the LAN.
* **Network Administrator:** The network administrator oversees the LAN’s operations, configurations, and maintenance. This individual or team is typically knowledgeable about network technologies and has the expertise to manage and troubleshoot network-related issues. The network administrator’s tasks can include:

i. **Network Setup and Configuration:** The network administrator is responsible for setting up and configuring the LAN, including installing and configuring network devices such as switches, routers, and wireless access points. They define network settings, IP addressing schemes, and network protocols.

**ii. User Management:** The network administrator manages user accounts, permissions, and access rights within the LAN. They create and delete user accounts, assign user roles and group memberships, and enforce security policies and restrictions.

**iii. Network Security:** Network administrators implement and manage network security measures to protect the LAN from unauthorized access, data breaches, and security threats. This includes setting up firewalls, implementing intrusion detection/prevention systems, managing access controls, and ensuring compliance with security policies and standards.

**iv. Network Monitoring and Performance Optimization:** Network administrators monitor the LAN’s performance, analyze network traffic, and identify potential issues or bottlenecks. They use network monitoring tools to detect and resolve network problems, optimize network performance, and ensure efficient data transmission within the LAN.

**v. Network Maintenance and Upgrades:** The network administrator performs regular maintenance tasks such as firmware updates, device configurations, and network backups. They also plan and execute network upgrades or expansions when necessary, ensuring the LAN infrastructure remains up-to-date and capable of meeting the organization’s needs.

**vi. Troubleshooting and Technical Support:** In the event of network issues or user connectivity problems, the network administrator troubleshoots and resolves the issues. They provide technical support to network users, diagnose network-related problems, and implement solutions to ensure smooth network operation.

A Local Area Network (LAN) is a computer network that connects devices within a localized area, such as a building or campus, facilitating efficient communication, resource sharing, and collaboration among network users. LANs comprise various components that work together to create a functional network infrastructure. The hardware components include computers, servers, switches, routers, NICs, cables, and wireless access points. These components establish physical connections, manage data transmission, and provide network connectivity. On the software side, LANs rely on network protocols, network operating systems, network management software, and security software to govern data transmission, manage network resources, monitor network performance, and ensure network security. Additionally, LANs incorporate the user component, including network users who connect their devices to the LAN, user accounts and roles, collaboration and communication tools, and network administrators who manage and maintain the LAN infrastructure. The integration of these components enables LANs to support efficient data transfer, resource sharing, secure communication, and collaboration within a localized network environment.

in 1977.

uses of LAN

Local Area Networks (LANs) are used for a variety of purposes, including:

1. File Sharing: LANs allow users to share files and resources within a local area, making it easier to collaborate and access shared documents.
2. Printer Sharing: Multiple users within a LAN can share a single printer, reducing the need for individual printers in an office or home environment.
3. Internet Sharing: LANs can be used to share a single internet connection among multiple devices, reducing costs and improving network efficiency.
4. Communication: LANs facilitate communication through email, instant messaging, and other forms of digital communication within a local area.
5. Resource Sharing: LANs enable the sharing of software, databases, and other resources, allowing efficient use of resources within a local environment.
6. Gaming: LANs are commonly used for multiplayer gaming, allowing players to connect and compete in a local network environment.
7. Networked Appliances: LANs can be used to connect and control networked appliances, such as smart home devices and security systems.

These are just a few examples of the many uses of LAN networks.

LAN STANDARDS

LAN STANDARDS

## What are IEEE 802 wireless standards?

IEEE 802 is a collection of networking standards that cover the physical and data link layer specifications for technologies such as Ethernet and wireless. These specifications apply to local area networks ([LANs](https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN)) and metropolitan area networks ([MANs](https://www.techtarget.com/searchnetworking/definition/metropolitan-area-network-MAN)). IEEE 802 also aids in ensuring multivendor interoperability by promoting standards for vendors to follow.

Essentially, the IEEE 802 standards help make sure internet services and technologies follow a set of recommended practices so that network devices can all work together smoothly.

IEEE 802 is divided into different parts that cover the physical and [data link](https://www.techtarget.com/searchnetworking/definition/Data-Link-layer) aspects of networking. The family of standards is developed and maintained by the Institute of Electrical and Electronics Engineers (IEEE) 802 LAN/MAN Standards Committee, also called the LMSC.

The set of standards started in 1979 with a proposed standard called Local Network for Computer Interconnection, which was approved a year later. The LMSC has made more than 70 standards for IEEE 802.

Some commonly used standards include those for Ethernet, bridging and virtual bridged LANs, [wireless LANs, wireless MANs, wireless personal area networks](https://www.techtarget.com/searchnetworking/tip/The-4-different-types-of-wireless-networks) (PANs) and radio access networks, as well as media independent handover services.

Better-known specifications include [802.3 Ethernet](https://www.techtarget.com/searchnetworking/definition/8023), [802.11](https://www.techtarget.com/searchmobilecomputing/definition/80211) Wi-Fi and 802.15 Bluetooth/Zigbee. However, some of these standards have been labeled as disbanded or hibernating, and are either superseded by newer standards or being reworked. Using an open process, the LMSC advocates for these standards globally.

Individual working groups are decided on and assigned to each area so that each segment receives an acceptable amount of focus. IEEE 802 specifications also split the data link layer into two different layers -- a logical link control layer and a media access control (MAC) layer.

LMSC provides a PDF of standards for up to six months after they have been published. All standards stay in place until they are replaced with another document or withdrawn.

## Why IEEE 802 standards are important

LMSC was formed in 1980 to standardize [network protocols](https://www.techtarget.com/searchnetworking/definition/protocol) and provide a path to make compatible devices across numerous industries.

Without these standards, equipment suppliers could manufacture network hardware that would only connect to certain computers. It would be much more difficult to connect to systems not using the same set of networking equipment. Standardizing protocols helps ensure multiple types of devices can connect to multiple network types. It also helps make sure network management isn't the challenge it could be if standards weren't in place.

IEEE 802 also coordinates with other international standards, such as the International Organization for Standardization or ISO, to help maintain international standards.

The 802 in IEEE 802 does not stand for anything of significance; 802 was the next numbered project.

## Examples of IEEE 802 uses

Commercial organizations can use the IEEE 802 specifications to ensure their products maintain any newly specified standards. So, for example, the 802.11 specification that applies to Wi-Fi could be used to make sure Wi-Fi devices work together under one standard. In the same way, IEEE 802 can help maintain LAN standards.

These specifications also define what connectivity infrastructure will be used for -- individual networks or those at a larger organizational scale.

The IEEE 802 specifications apply to hardware and software products. So that manufacturers don't have any input on the standards, there is a voting protocol in place. This ensures one organization does not influence the standards too much.

## Working groups

The working groups are the different areas of focus within the 802 specifications. They are numbered from 802.1 onward.

| 802 | Overview | Basics of physical and logical networking concepts |
| --- | --- | --- |
| 802.1 | Bridging | * LAN/MAN bridging and management. * Covers management and the lower sublayers of OSI Layer 2, including MAC-based bridging, virtual LANs and port-based access control. * Also contains the Time-Sensitive Networking Task Group. |
| 802.2 | Logical link control | Disbanded |
| 802.3 | [Ethernet](https://www.techtarget.com/searchnetworking/definition/Ethernet) | * The grandfather of the 802 specifications. * Provides asynchronous networking using carrier sense, multiple access with collision detect (CSMA/CD) over coax, twisted-pair copper and optical fiber media. * Current speeds range from 10 Mbps to 10 Gbps. |
| 802.4 | Token bus | Disbanded |
| 802.5 | Token ring | Disbanded |
| 802.6 | Distributed queue dual bus | * Superseded. * Revision of 802.1D, superseded by 802.1D-2004. |
| 802.7 | Broadband LAN practices | Disbanded |
| 802.8 | Fiber optic practices | Disbanded |
| 802.9 | Integrated services LAN | Disbanded |
| 802.10 | Interoperable LAN security | Disbanded |
| 802.11 | [Wi-Fi](https://www.techtarget.com/searchmobilecomputing/definition/Wi-Fi) |  |
| 802.11a |  |  |
| 802.11b |  |  |
| 802.11d |  |  |
| 802.11e |  |  |
| 802.11g |  |  |
| 802.11h |  |  |
| 802.11i |  |  |
| 802.11j |  |  |
| 802.11k |  |  |
| 802.11m |  |  |
| 802.11n |  |  |
| 802.11x |  |  |
| 802.12 | Demand priority |  |
| 802.13 | Not used |  |
| 802.14 | Cable modems |  |
| 802.15 | Wireless PANs |  |
| 802.15.1 | [Bluetooth](https://www.techtarget.com/searchmobilecomputing/definition/Bluetooth) |  |
| 802.15.3a | Ultra wideband |  |
| 802.15.4 | [Zigbee](https://www.techtarget.com/iotagenda/definition/ZigBee) |  |
| 802.15.5 | [Mesh network](https://www.techtarget.com/iotagenda/definition/mesh-network-topology-mesh-network) |  |
| 802.16 | Wireless MANs |  |
| 802.17 | Resilient packet ring |  |
| 802.18 | Radio Regulatory Technical Advisory Group |  |
| 802.19 | Wireless coexistence |  |
| 802.20 | Mobile broadband wireless access |  |
| 802.21 | Media independent handover |  |
| 802.22 | Wireless regional area network |  |
| 802.23 | Emergency Services Working Group |  |
| 802.24 | Vertical Applications Technical Advisory Group |  |

# Channel Access Method

Channel access method (CAM) is used in telecommunications and computer networks to allow network terminals to share media capacity through a multipoint transmission medium. CAM examples include bus, hub, wireless and ring networks.

Advertisements

A channel access scheme is based on a multiplexing method, which allows several data streams or signals to share the same communication channel or physical medium. Furthermore, it is also based on a multiple access protocol and control mechanism known as media access control (MAC).

Channel access method is also know as multiple access method.

**Channel Access Method**

CAM is based on the following protocol features:

* Physical layer multiplexing
* The media access control layer, which handles addressing and collision prevention
* Token passing
* Polling, a continuous slave/master data querying process
* Contention or node network access competition

Channel access methods in computer networking refer to the protocols and techniques used for devices to access and share a communication channel efficiently. In networking, a communication channel can be any medium through which data is transmitted, such as wired Ethernet cables or wireless radio frequencies. The choice of channel access method depends on factors like the network topology, the medium used for communication, and the required performance.

There are several channel access methods, but two of the most common ones are:

1. **Carrier Sense Multiple Access (CSMA)**:
   * In CSMA, before transmitting data, a device listens to the channel to check if it's idle. If the channel is busy, the device waits for a random period before attempting to transmit again (this is known as the backoff algorithm).
   * There are different variants of CSMA:
     + CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is used in wired Ethernet networks. If a collision is detected during transmission, the device stops transmitting, waits for a random amount of time, and then retries.
     + CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is used in wireless networks like Wi-Fi. Devices wait for a random backoff time to avoid collisions due to hidden terminals.
2. **Time Division Multiple Access (TDMA)**:
   * TDMA divides the communication channel into time slots. Each device is allocated a specific time slot for transmission.
   * Unlike CSMA, where devices contend for the channel when it's idle, in TDMA, devices are assigned specific time slots, reducing the chances of collisions.
   * TDMA is commonly used in cellular networks and satellite communication systems.

Here's a more in-depth explanation of CSMA:

**Carrier Sense Multiple Access (CSMA)**:

CSMA is a contention-based access method where devices contend for access to the channel. Before transmitting data, a device using CSMA listens to the channel to detect if it's busy or idle. If the channel is idle, the device can transmit its data. However, if the channel is busy (indicating that another device is transmitting), the device waits for a random period of time before attempting to transmit again. This random wait period is known as the backoff algorithm and helps reduce the probability of collisions between devices attempting to transmit simultaneously.

**CSMA Variants**:

1. **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**:
   * Used in wired Ethernet networks.
   * In addition to sensing the channel before transmitting, devices also listen to the channel while transmitting to detect collisions.
   * If a collision is detected, devices stop transmitting immediately, wait for a random amount of time, and then retry transmission.
   * CSMA/CD is effective in detecting collisions in wired networks and ensures fair access to the channel among multiple devices.
2. **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**:
   * Used in wireless networks like Wi-Fi.
   * Wireless networks have issues with hidden terminals, where two devices cannot directly detect each other's signals.
   * CSMA/CA employs a mechanism where devices contend for the channel based on virtual carrier sensing, estimating the busy state of the channel from indirect indications.
   * Before transmitting, devices wait for a random backoff time to reduce the chances of collisions.
   * CSMA/CA aims to avoid collisions rather than detecting them after they occur.

**Advantages of CSMA**:

* Simple and widely implemented.
* Adaptive to network load variations.
* Supports dynamic network topologies.

**Disadvantages of CSMA**:

* Vulnerable to collisions, especially in high-traffic environments.
* The backoff mechanism can lead to inefficient channel utilization, especially when there are many devices contending for access.
* Doesn't guarantee fairness in access, as devices with higher transmission priority might monopolize the channel.

In summary, channel access methods like CSMA play a crucial role in managing access to communication channels in computer networks, ensuring efficient and reliable data transmission. The choice of method depends on factors like network topology, medium characteristics, and performance requirements.

**Aloha**

Aloha is a computer networking protocol developed in the 1970s at the University of Hawaii as a way to allow multiple users to share a single communication channel. It's one of the earliest forms of multiple access protocols, which enable multiple devices to access a shared communication medium, like a radio channel or a network cable.

There are two main versions of the Aloha protocol: pure Aloha and slotted Aloha.

1. **Pure Aloha**:
   * In pure Aloha, each station can transmit data whenever it has something to send.
   * When a station wants to transmit, it simply sends the data.
   * After sending the data, the station waits for an acknowledgment from the receiver.
   * If no acknowledgment is received within a certain time window, the station assumes that there was a collision with another station's transmission and resends the data after a random backoff period.
2. **Slotted Aloha**:
   * Slotted Aloha divides time into discrete slots, with each slot corresponding to the time it takes to transmit one packet.
   * Stations are only allowed to transmit at the beginning of a time slot.
   * This eliminates the possibility of collisions that occur due to transmissions overlapping partially.
   * If a station has data to send, it waits for the beginning of the next time slot and then transmits its data.
   * Like pure Aloha, if a station doesn't receive an acknowledgment, it will retry transmission after a random back off period.

**Advantages of Aloha:**

* Simplicity: Aloha is straightforward and easy to implement.
* Decentralization: It does not require central coordination, making it suitable for distributed systems.
* Robustness: It can handle a variable number of users and is resilient to changes in network topology.

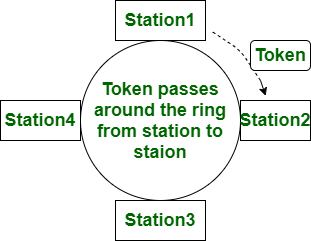
**Disadvantages of Aloha:**

* Low Efficiency: Both pure and slotted Aloha suffer from low efficiency, especially as the network becomes more congested.
* Vulnerability to Collisions: Collisions occur frequently, leading to wasted bandwidth and retransmissions.
* Limited Scalability: As the number of users increases, the probability of collisions also increases, reducing overall network throughput.

While the original Aloha protocol is not widely used in modern networks due to its limitations, its concepts have influenced the development of more sophisticated multiple access protocols such as Carrier Sense Multiple Access (CSMA) and its variants (e.g., CSMA/CD, CSMA/CA), which are fundamental to Ethernet and Wi-Fi networks.

**Token ring and Ethernet**

**1.**[**Token Ring**](https://www.geeksforgeeks.org/token-ring-frame-format/)**:**   
In the token ring a token ring passes over a physical ring. Token ring is defined by IEEE 802.5 standard. In token ring, there is a station and a special frame called token. A station in token ring can transmit data frame if it contains a token. After the successful transmission of data frame token are pointed(issued). Token ring is a Star shaped topology and handles priority in which some nodes may give priority to the token.



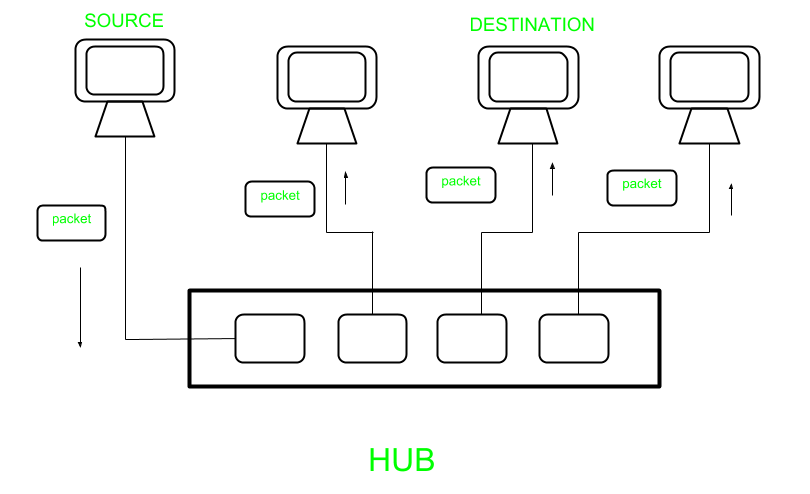
**2.**[**Ethernet**](https://www.geeksforgeeks.org/local-area-network-lan-technologies/)**:**   
IEEE 802.3 defines the Ethernet. It uses CSMA/CD mechanism. It means that if many stations exist at the same time to talk, all stations will be closed. To resume them, wait for a random time. Unlike token ring it doesn’t employ any priorities. And it is less costly than token ring network.

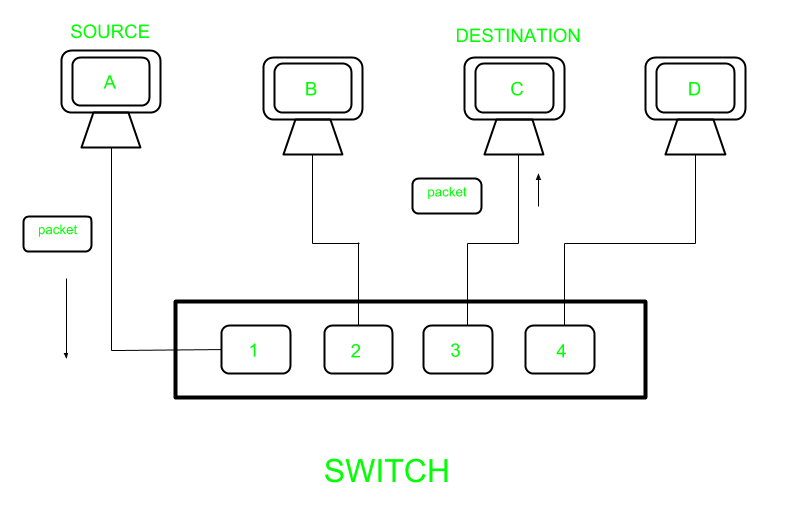
Let’s see the difference between the token ring and Ethernet:-

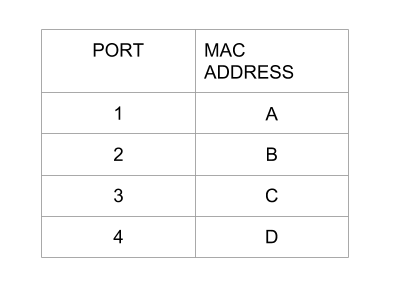
| **S. No.** | **TOKEN RING** | **ETHERNET** |
| --- | --- | --- |
| 1. | In the token ring, the token passing mechanism is used. | While Ethernet uses CSMA/CD(Carrier-Sense Multiple Access/Collision Detection) mechanism. |
| 2. | Token ring is defined by IEEE 802.5 standard. | Whereas Ethernet is defined by IEEE 802.3 standard. |
| 3. | Token ring is deterministic. | While it is non-deterministic. |
| 4. | A token ring is a Star shaped topology. | While Ethernet is a Bus shaped topology. |
| 5. | The token ring handles priority in which some nodes may give priority to the token. | While Ethernet does not employ priority. |
| 6. | Token ring costs more than Ethernet. | While Ethernet cost seventy percent less than token ring. |
| 7. | In the token ring telephone wire is used. | While in Ethernet coaxial cable(wire) is used. |
| 8. | The token ring contains routing information. | While Ethernet does not contain routing information. |
| 9. | The transmission speed of token ring is slower (generally operates at 4 Mbps to 16 Mbps). | Its transmission speed is faster (generally operates at 10 Mbps to up to 100 Mbps). |
| 10. | In token ring, flow of data is unidirectional as data is passed from one workstation to another only when the token is received by the workstation. | In Ethernet, no such directional flow of data takes place. Instead, data frames can be transmitted by any of the workstation if the network is idle. |
| 11. | Token ring uses a token passing system so only 1 workstation is active at a time. | Ethernet uses CSMA/CD so here more than one workstation stays active at a time. |

# Difference between layer-2 and layer-3 switches

[Network Devices](https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/)   
A **switch** is a device which sends a data packet in a local network. What is advantage over hub? A hub floods the network with the packet and only destination system receives that packet while others just drop due to which the traffic increases a lot. To solve this problem switch came into the picture. A switch first learns, by flooding network just like hub to fill MAC- address table, on which port a particular device is connected. After learning it sends packets to that particular host only.







Layer 2 switch work on layer 2 of OSI model i.e. data link layer and sends a “Frames” to destination port using MAC address table which stores the mac address of a device associated with that port. Layer 3 switch work on layer 3 of OSI model i.e. network layer where it route packet by using IP address, it is used widely on VLANs.

| **Layer 2 Switch** | **Layer 3 Switch** |
| --- | --- |
| Operate on layer 2 (Data link) of OSI model. | Operate on layer 3 (Network Layer) of OSI model. |
| Send “frames” to destination on the basis of MAC address. | Route Packet with help of IP address |
| Work with MAC address only | Can perform functioning of both 2 layer and 3 layer switch |
| Used to reduce traffic on local network. | Mostly Used to implement VLAN (Virtual Local area network) |
| Quite fast as they do not look at the Layer 3 portion of the data packets. | Takes time to examine data packets before sending them to their destination |
| It has single broadcast domain | It has multiple broadcast domain. |
| Can communicate within a network only. | Can communicate within or outside network. |

# What is Ethernet?

A local Area Network (LAN) is a data communication network connecting various terminals or computers within a building or limited geographical area. The connection between the devices could be wired or wireless. [Ethernet](https://www.geeksforgeeks.org/what-is-ethernet/), [Token rings](https://www.geeksforgeeks.org/efficiency-of-token-ring/), and [Wireless LAN](https://www.geeksforgeeks.org/difference-between-lan-and-wlan/) using [IEEE 802.11](https://www.geeksforgeeks.org/ieee-802-11-mac-frame/) are examples of standard [LAN technologies](https://www.geeksforgeeks.org/lan-switching/).

## What is Ethernet?

Ethernet is the most widely used LAN technology and is defined under IEEE standards 802.3. The reason behind its wide usability is that Ethernet is easy to understand, implement, and maintain, and allows low-cost network implementation. Also, Ethernet offers flexibility in terms of the topologies that are allowed. Ethernet generally uses a bus topology. Ethernet operates in two layers of the [OSI model](https://www.geeksforgeeks.org/layers-of-osi-model/), the physical layer and the [data link layer](https://www.geeksforgeeks.org/data-link-layer/). For Ethernet, the protocol data unit is a frame since we mainly deal with DLLs. In order to handle collisions, the Access control mechanism used in [Ethernet](https://www.geeksforgeeks.org/what-is-ethernet/)is[CSMA/CD.](https://www.geeksforgeeks.org/collision-detection-csmacd/)

Although Ethernet has been largely replaced by wireless networks, wired networking still uses Ethernet more frequently. [Wi-Fi](https://www.geeksforgeeks.org/what-is-wi-fiwireless-fidelity/) eliminates the need for cables by enabling users to connect their smartphones or laptops to a network wirelessly. The 802.11ac Wi-Fi standard offers faster maximum data transfer rates when compared to Gigabit Ethernet. However, wired connections are more secure and less susceptible to interference than wireless networks. This is the main justification for why so many companies and organizations continue to use Ethernet.

There are different types of Ethernet networks that are used to connect devices and transfer data.

Let’s discuss them in simple terms:

**1. Fast Ethernet:**This type of Ethernet network uses cables called twisted pair or CAT5. It can transfer data at a speed of around 100 Mbps (megabits per second). Fast Ethernet uses both fiber optic and twisted pair cables to enable communication. There are three categories of Fast Ethernet: 100BASE-TX, 100BASE-FX, and 100BASE-T4.

**2. Gigabit Ethernet:** This is an upgrade from Fast Ethernet and is more common nowadays. It can transfer data at a speed of 1000 Mbps or 1 Gbps (gigabit per second). Gigabit Ethernet also uses fiber optic and twisted pair cables for communication. It often uses advanced cables like CAT5e, which can transfer data at a speed of 10 Gbps.

**3.10-Gigabit Ethernet:** This is an advanced and high-speed network that can transmit data at a speed of 10 gigabits per second. It uses special cables like CAT6a or CAT7 twisted-pair cables and fiber optic cables. With the help of fiber optic cables, this network can cover longer distances, up to around 10,000 meters.

**4. Switch Ethernet:**This type of network involves using switches or hubs to improve network performance. Each workstation in this network has its own dedicated connection, which improves the speed and efficiency of data transfer. Switch Ethernet supports a wide range of speeds, from 10 Mbps to 10 Gbps, depending on the version of Ethernet being used.

In summary, Fast Ethernet is the basic version with a speed of 100 Mbps, Gigabit Ethernet is faster with a speed of 1 Gbps, 10-Gigabit Ethernet is even faster with a speed of 10 Gbps, and Switch Ethernet uses switches or hubs to enhance network performance.

The [Manchester Encoding](https://www.geeksforgeeks.org/manchester-encoding-in-computer-network/) Technique is used in [Ethernet](https://www.geeksforgeeks.org/what-is-ethernet/).

Using Manchester encoding, data can be transmitted over a physical medium in communication systems. It is a type of line coding where the signal transitions, as opposed to the absolute voltage levels, serve as the data representation.

| **S.NO** | **Fast Ethernet** | **Gigabit Ethernet** |
| --- | --- | --- |
| 1. | [Fast Ethernet](https://www.geeksforgeeks.org/local-area-network-lan-technologies/) provides 100 Mbps speed. | [Gigabit Ethernet](https://www.geeksforgeeks.org/introduction-of-gigabit-ethernet/) offers 1 Gbps speed. |
| 2. | Fast Ethernet is simple configured. | While Gigabit Ethernet is more complicated than Fast Ethernet. |
| 3. | Fast Ethernet generate more delay comparatively. | Gigabit Ethernet generates less delay than Fast Ethernet. |
| 4. | The coverage limit of Fast Ethernet is up to 10 km. | While the coverage limit of Gigabit Ethernet is up to 70 km. |
| 5. | The round-trip delay in Fast Ethernet is 100 to 500 bit times. | While the round-trip delay in Gigabit Ethernet is 4000 bit times. |
| 6. | Fast Ethernet is the Successor of 10-Base-T Ethernet. | While Gigabit Ethernet is the successor of Fast Ethernet. |
| 7. | Fast ethernet is less scalable than Gigabit ethernet. | Gigabit ethernet is more scalable than Fast ethernet. |

# Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways)

**Network Devices:** Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, and NIC, etc.

**1. Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

**2. Hub** –  A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.  In other words, the [collision domain](https://en.wikipedia.org/wiki/Collision_domain) of all hosts connected through Hub remains one.  Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

**Types of Hub**

Top VS Code Extensions for Web Developer in 2024!! GeeksforGeeks

* **Active Hub:-**These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
* **Passive Hub:-**These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.
* **Intelligent Hub:-**It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

**3. Bridge** – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

**Types of Bridges**

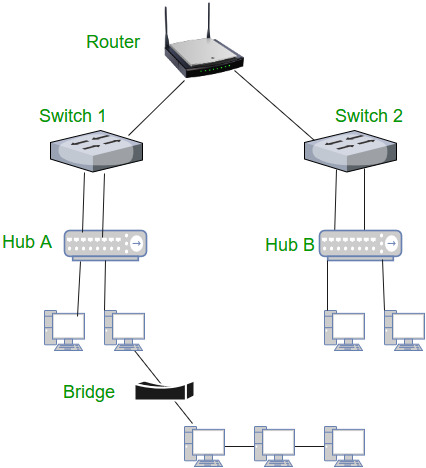
* **Transparent Bridges:-**These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
* **Source Routing Bridges:-**In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

**4. Switch** – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.  In other words, the switch divides the collision domain of hosts, but the [broadcast domain](https://en.wikipedia.org/wiki/Broadcast_domain) remains the same.

#### ****Types of  Switch****

1. **Unmanaged switches:** These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.
2. **Managed switches**: These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.
3. **Smart switches:** These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.
4. **Layer 2 switches:** These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.
5. **Layer 3 switches**: These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks..
6. **Gigabit switches:** These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.

**5. Routers** – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.



**6. Gateway** – A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.

.

**7. NIC**– NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN.  It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

# WAN Full Form

A WAN (Wide Area Network) is to connect multiple smaller Local Area Networks (LANs). It is a computer network designed. WANs can help in communication, the sharing of information, and much more between systems or devices from around the world through a WAN provider.

## What is a WAN?

**WAN** stands for **Wide Area Network**. It is a [computer network](https://www.geeksforgeeks.org/what-is-computer-networking/) that covers a large geographical area consisting of two or more [LANs or MANs](https://www.geeksforgeeks.org/difference-between-lan-and-man/). These networks are established with leased [telecommunication](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-telecommunication/) circuits, in which two sides which are connected have routers that connect the LAN of both sides together in a network to facilitate communication.



*WAN Full Form*

## History of WAN

The roots of WAN are connected to the U.S Department of defense which developed ARPANET to let researchers communicate and share computer resources remotely. The connection can be circuit-switched telephone lines, radio wave transmission or [optical fiber](https://www.geeksforgeeks.org/fiber-optics-and-types/) transmission. It is used to exchange data with users all over the world, they can be client, employee, buyer, seller, student, etc. WAN has the ability to transmit data, image, audio data, video data over large distances.

## What is a WAN Router?

An organisation can access a carrier network by using a WAN [router](https://www.geeksforgeeks.org/introduction-of-a-router/), sometimes referred to as an edge router or border router, which routes data packets between WAN locations. Packet over SONET/SDH (PoS), [Multiprotocol Label Switching (MPLS)](https://www.geeksforgeeks.org/multi-protocol-label-switching-mpls/),[ATM, and Frame Relay](https://www.geeksforgeeks.org/difference-between-frame-relay-and-atm/) are many WAN protocol were developed.



*WAN Network*

## What is Software-Defined WAN (SD-WAN)?

* It is a technique for making WAN architectures easier to construct, run, and administer is [software-defined](https://www.geeksforgeeks.org/software-defined-networking/) WAN (SD-WAN). It relies on virtualization, overlay networks, application-level policies and onsite SD-WAN devices and [software](https://www.geeksforgeeks.org/software-and-its-types/) platforms.
* SD-WAN improves the efficiency of data transfer across a WAN by shifting traffic to less expensive network links to replace more expensive leased or MPLS lines.

## Types of WAN Technologies

There are mainly two technologies that are used in the WAN network design.

* **Circuit switching**: [Circuit switched](https://www.geeksforgeeks.org/circuit-switching-in-computer-network/)networks operate on the virtual connection principle, which dictates that all messages will take the same way and that resources along this path are set aside for this connection.
* **Packet Switching:**The size of a packet in a [packet switched](https://www.geeksforgeeks.org/packet-switching-and-delays-in-computer-network/)network is dictated by the outgoing link, and these packets may follow different route. These packets are ready to collected and reassembled at the destination.
* **TCP/IP protocol suite**: [TCP/IP](https://www.geeksforgeeks.org/tcp-ip-in-computer-networking/) is a protocol suite of foundational of the internet protocols used to interconnect devices on Internet and other computers networks or device network. Full form of TCP/IP is Transmission Control Protocol/Internet Protocol.
* **Router:**A [router](https://www.geeksforgeeks.org/introduction-of-a-router/) is a networking device which transfers data packets between device networks and also we can say it is used to interconnect LANs to form a wide area network (WAN).
* **Packet over SONET/SDH (PoS):** Packet over [SONET and SDH](https://www.geeksforgeeks.org/difference-between-sonet-and-sdh/) is a communication protocol used for WAN transport. When using optical fiber and SONET or SDH communication protocol used to defines how point-to-point links communicate.
* **Multiprotocol Label Switching (MPLS):** [Multi Protocol Label Switching (MPLS)](https://www.geeksforgeeks.org/multi-protocol-label-switching-mpls/) is an IP packet routing technique and also a network routing optimization technique that routes IP packet through paths via labels instead of looking at complex routing tables of routers.

## Characteristics of WAN

* **Broader Reach:**The reach of WAN in terms coverage of geographical area is very high which can be a region, country or the world itself.
* **Higher Capacity:**The capacity of WAN in terms of number of [LANs or WANs](https://www.geeksforgeeks.org/difference-between-lan-and-wan/) connected in a network is very high, which results in connection of large number of user over different location all around the globe.
* **Use of Public Carrier:**WAN uses [telephone network](https://www.geeksforgeeks.org/introduction-to-telephone-network/), cabled system, satellites etc for connection and transmission purpose which are easily available.
* **Resource Sharing:**WAN enables its users to share data and information over large area. Computer resources can be accessed remotely which makes transmission and exchange of data very easy.

## Advantages of WAN

* It covers large geographical area which enhances the reach of organisation to transmit data quickly and cheaply.
* The data can be stored in centralised manner because of remote access to data provided by WAN.
* The travel charges that are needed to cover the geographical area of work can be minimised.
* WAN enables a user or organisation to connect with the world very easily and allows to exchange data and do business at global level.

## Disadvantages of WAN

* Traffic congestion in Wide Area Network is very high.
* The fault tolerance ability of WAN is very less.
* Noise and error are present in large amount due to multiple connection point.
* The data transfer rate is slow in comparison to [LAN](https://www.geeksforgeeks.org/lan-full-form/) because of large distances and high number of connected system within the network.

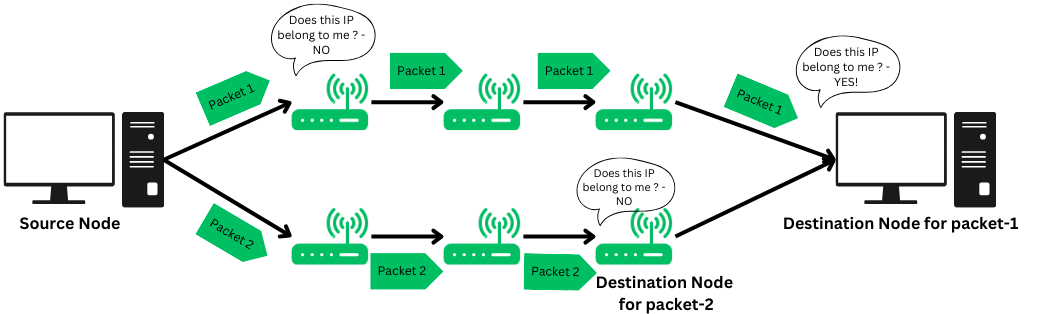
# What is Routing?

The process of choosing a path across one or more networks is known as network routing. Any kind of network, including public transit and phone networks, can use the routing principles. Routing chooses the routes along which Internet Protocol (IP) packets get from their source to their destination in packet-switching networks, such as the Internet. Routers are specialized pieces of network hardware that make these judgments about Internet routing.

## What is Routing?

Routing refers to the process of directing a data packet from one node to another. It is an autonomous process handled by the network devices to direct a data packet to its intended destination. Note that, the node here refers to a [network device](https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/)called – ‘[Router](https://www.geeksforgeeks.org/introduction-of-a-router/)‘. Routing is a crucial mechanism that transmits data from one location to another across a network (Network type could be any like [LAN, WAN, or MAN](https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/)). The process of routing involves making various routing decisions to ensure reliable & efficient delivery of the data packet by finding the shortest path using various routing metrics which we will be discussing in this article.

Routing of a data packet is done by analyzing the destination IP Address of the packet. Look at the below image:



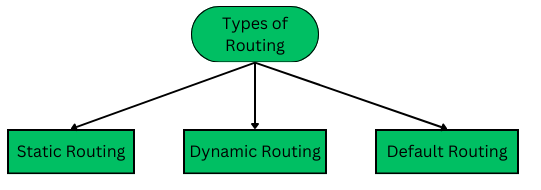
*Routing of packets*

* Source Node (Sender) sends the data packet on the network, embedding the IP in the header of data packet.
* The nearest router receives the data packet, and based on some metrics, further routes the data packet to other routers.
* Step-2 occurs recursively till the data packet reaches its intended destination.

**Note:** There are limits to how many hop counts a packet can do if its exceeded, the packet is considered to be lost.

## Types of Routing

Routing is typically of 3 types, each serving their own purpose and offering different functionalities.



*Types of Routing*

### 1. Static Routing

Static routing is also called as “non-adaptive routing”. In this, routing configuration is done manually by the network administrator. Let’s say for example, we have 5 different routes to transmit data from one node to another, so the network administrator will have to manually enter the routing information by assessing all the routes.

* Network administrator has full control over the network, routing the data packets to their concerned destinations
* Routers will route packets to the destination configured manually the network administrator.
* Although this type of routing gives a fine-grained control over the routes, it may not be suitable for large scale enterprise networks.

### 2. Dynamic Routing

Dynamic Routing is another type of routing in which routing is an autonomous procedure without any human intervention. Packets are transmitted over a network using various shortest path algorithms and pre-determined metrics. This type of routing is majorly preferred in modern networks as it offers more flexibility and versatile functionality.

* It is also known as adaptive routing.
* In this, the router adds a new routes to the routing table based on any changes made in the topology of the network.
* The autonomous procedure of routing helps in automating every routing operation from adding to removing a route upon updates or any changes made to the network.

### 3. Default Routing

Default Routing is a routing technique in which a router is configured to transmit packets to a default route that is, a gateway or next hop device if no specific path is defined or found. It is commonly used when the network has single exit point. The IP Router has the following address as the default route : 0.0.0.0/0.

## Working Principle of Routing

Routing works by finding a shortest path from the source node to the destination node across a network. Here’s step-by-step working of routing:

### ****Step1: Communication initiation****

The first step that typically happens is, one node (client or server) initiates a communication across a network using [HTTP](https://www.geeksforgeeks.org/http-full-form/)protocols.

### ****Step2: Data Packets****

The source device now breaks a big chunk of information into small data packets for reliable and efficient transmission. This process is called is called de-assembling and encapsulating the data payload. And then each data packet is labelled with the destination node’s IP address.

### ****Step3: Routing Table****

[Routing table](https://www.geeksforgeeks.org/routing-tables-in-computer-network/)is a logical [data structure](https://www.geeksforgeeks.org/data-structure-meaning/) used to store the IP addresses and relevant information regarding the nearest routers. The source node then looks up for the IP addresses of all the nodes that can transmit the packet to its destination and selects the shortest path using the shortest path algorithm and then routes accordingly.

Routing Table is stored in a router, a network device that determines the shortest path and routes the data packet.

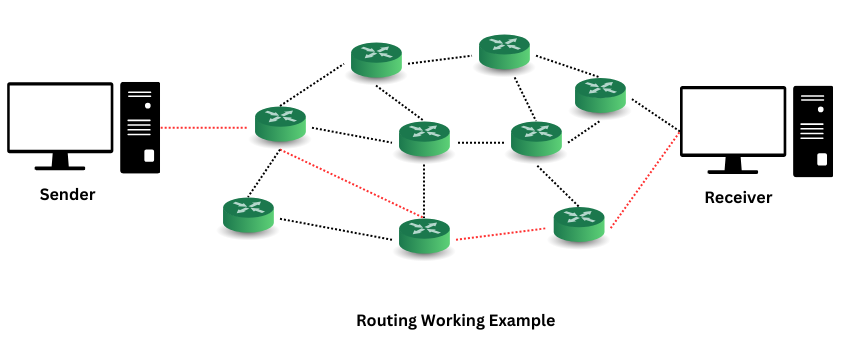
### Step4: Hopping procedure

In the procedure or routing, the data packet will undergo many hops across various different nodes in a network till it reaches its final destination node. Hop-count is defined as the number of nodes required to traverse through to finally reach the intended destination node. This hopping procedure has a certain criteria defined for every data packet, there’s a limited number of hops a packet can take if the packet exceeds that, then its considered to be lost and it is retransmitted.

### Step5: Reaching the destination node

Once all the data packets reach their intended destination node, they re-assemble and transform into complete information that was sent by the sender (source node). The receiver will perform various [error checking](https://www.geeksforgeeks.org/error-detection-in-computer-networks/) mechanism to verify the authenticity of the data packets.

Overall, the data packet will be transmitted over least hop-count path as well as the path on which there is less traffic to prevent packet loss.



**Congestion Control in Computer Networks**

What is **congestion**?

A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

**Effects** of Congestion

* As delay increases, performance decreases.
* If delay increases, retransmission occurs, making situation worse.

**Congestion control algorithms**

* Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.
* Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.
* There are two congestion control algorithm which are as follows:
* **Leaky Bucket Algorithm**
* The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting.
* A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms.
* This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.
* The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources.
* The large area of network resources such as bandwidth is not being used effectively.

Let us consider an example to understand

Imagine a bucket with a small hole in the bottom.No matter at what rate water enters the bucket, the outflow is at constant rate.When the bucket is full with water additional water entering spills over the sides and is lost.

[](https://media.geeksforgeeks.org/wp-content/uploads/leaky.jpg)

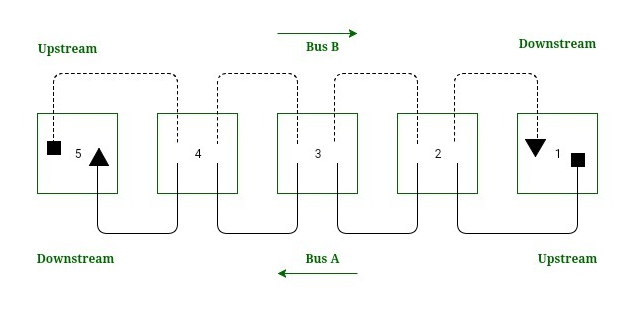
Similarly, each network interface contains a leaky bucket and the following **steps** are involved in leaky bucket algorithm:

1. When host wants to send packet, packet is thrown into the bucket.
2. The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
3. Bursty traffic is converted to a uniform traffic by the leaky bucket.
4. In practice the bucket is a finite queue that outputs at a finite rate.

* **Token bucket Algorithm**
* The leaky bucket algorithm has a rigid output design at an average rate independent of the bursty traffic.
* In some applications, when large bursts arrive, the output is allowed to speed up. This calls for a more flexible algorithm, preferably one that never loses information. Therefore, a token bucket algorithm finds its uses in network traffic shaping or rate-limiting.
* It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket.
* The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.
* When tokens are shown, a flow to transmit traffic appears in the display of tokens.
* No token means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket.

# IEEE 802.6 (DQDB)

IEEE 802.6 standard i.e. DQDB(Distributed Queue Dual Bus) is a [MAN(Metropolitan Area Network)](https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/) protocol. It can be defined as a high speed shared medium access control protocol that is used over a bus network. It has two unidirectional buses, for controlling purposes, where the bus can carry data, video, and voice over a network with bandwidth being allocated as per time slots. The advantage of using the paired bus is that it is used to tackles failure configuration. It can be extended up to 30 miles at 34-55 Mbps.

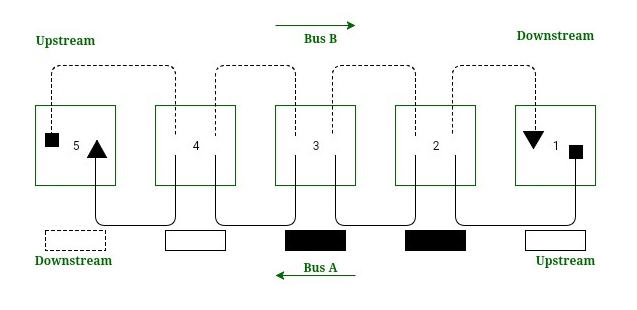


**Fig.1:-** Working of DQDB

**Directional Traffic:**  
Each bus support traffic in only one direction and are opposite to one another. The start of the bus being represented as a square and the end of the bus being represented as a triangle (Fig.1). Bus A traffic moves from right to left (i.e. from station 1 to 5) whereas the bus B traffic moves from left to right (i.e. from station 5 to 1).

**Upstream and Downstream:**  
The relationship of stations of the DQDB network depends on the directional flow of traffic of the buses.  
Considering bus A in Fig.1, which has station 1 & 2 marked as upstream w.r.t station 3 and station 4 & 5 are downstream w.r.t station 3. Here in bus A, station 1 is head of the bus as there is no upstream station and station 5 has no downstream station and it is regarded as to end of bus A.

**Working:**  
The head of the bus A i.e. station 1 generates empty slot for use of bus A. Similarly, the head of bus B i.e. station 5 generate empty slot for use of bus B. The empty slot travels down its bus until the transmission station drops data into it and intended destination reads the data.



**Fig.2:-** DQDB Slot traveling

*For example:*  
If station 2 wants to send data to station 4 (Fig.2), it chooses a slot on bus A as station 4 is downstream in bus A. The head of the bus A i.e. station 1 creates an empty slot. Station 2 drops its data & address of destination slot into the passing slot. Station 3 reads the address and passes the slot as unread. Station 4 recognizes its address, reads the data and changes the status of the slot and passes it along with station 5 where it is absorbed.

**How slot reservation is done?**  
To send data downstream, a station must wait for the arrival of the unoccupied slot, but here the question arises that how to stop an upstream station from manipulating the bus due to which the station near the end of the bus suffers, as the imbalance can lead to degraded quality of service. The solution to this problem is to do a reservation at the station. Here station 2 can make a reservation for bus A on bus B. Station 2 sets a reservation bit on a slot on bus B to tell each station it passes through, that the station is reserving a slot on bus A. All the station must respect the reservation of downstream station and leave the slot for requested station.

**SDH Full Form**

Last Updated : 27 Jul, 2020

SDH stands for **Synchronous Digital Hierarchy** and it refers to a multiplex technology used in the telecommunication. Synchronous Optical Network is internationally used and is taken equal to SDH. Both technologies provide quite fast and low-priced network interconnection than PDH which stands for Plesiochronous Digital Hierarchy.

SDH allows the data stream to pass having low bit rates to be combined into high rate data streams. As the entire network is synchronous, individual bitstreams can be embedded into and are extracted from high rate data streams quiet easily. Initially, it was developed back in 1985 in the USA under the name of SONET.

**Functions :**  
SDH used to combine n signals with a bit rate of b to form data streams with bit rates of (n × b) on the synchronously clocked networks. Unlike PDH, the transmission paths that transfer individually have minimal clock discrepancies.

The synchronous mode of operation allows low order multiplex system such as communication links for telephone systems, to be inserted in higher hierarchy levels and then remove again via add and drop. SDH has following Synchronous Transport Modules (STM) and their rates are as follows :

**1.** STM-1 (155 Mbps)

**2.** STM-4 (622 Mbps)

**3.** STM-16 (2.5 Gbps)

**4.** STM-64 (10 Gbps)

**Advantages :**

* The structure is synchronous and is quite flexible.
* It is capable of conveying Broadband signals.
* The format is fully digital and fulfills the criteria of world standard.
* It provides network transport services such as LAN in video conferencing and various interactive multimedia.
* Speed of SDH is high as compared to PDH.
* SDH allows quick recovery from any kind of failures.
* It supports different kinds of operators.

**Disadvantages :**

* The bandwidth utilization ratio is quite low as compared to PDH as because of OH bytes used for OAM.
* There are various software’s being used and so it is more prone to viruses.
* Pointers are being used for the adding or dropping of low rate signals and this causes the circuit to become more complex.
* It requires complicated SDH materials due to a variety of management traffic types.
* It cannot carry E2 due to the unavailability of the container.

**Applications :**

* It is being used in electrical converters.
* It is widely used in optical transports.
* It can be used as carriers in ATM cells.
* It can be used for bandwidth in demand.
* It can be used to cable TV networks.
* It can be used for T1 and T3 carriers.

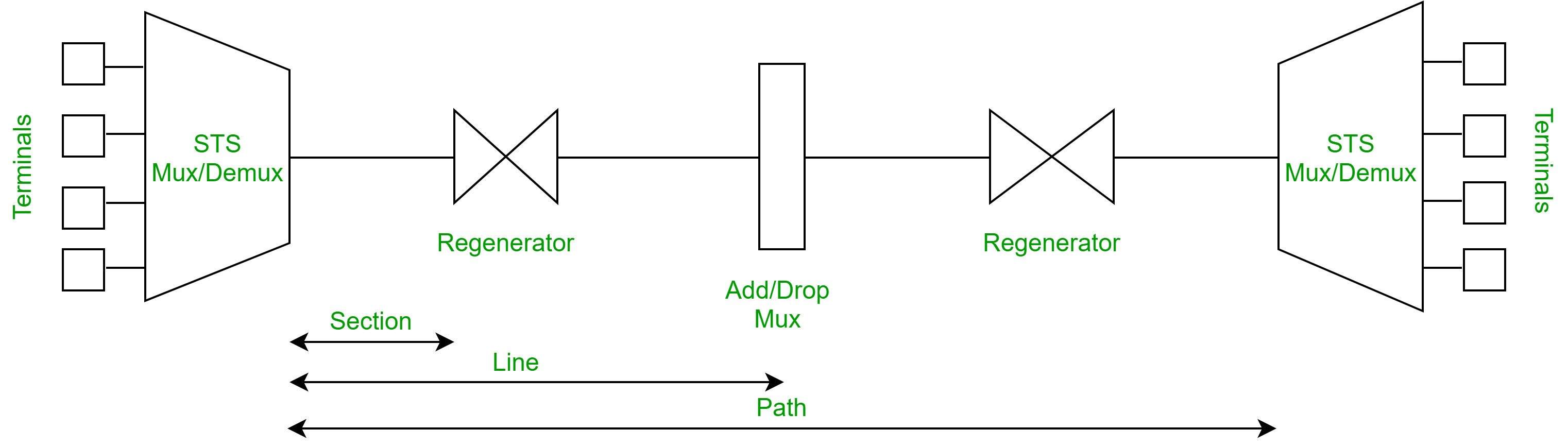
**Synchronous Optical Network (SONET)**

SONET stands for Synchronous Optical Network. SONET is a communication protocol, developed by Bellcore – that is used to transmit a large amount of data over relatively large distances using optical fibre. With SONET, multiple digital data streams are transferred at the same time over the optical fibre.

**Key Points:**

* Developed by Bellcore
* Used in North America
* Standardized by ANSI (American National Standards Institute)
* Similar to SDH (Synchronous Digital Hierarchy) which is used in Europe and Japan.

**Why SONET is called a Synchronous Network?**  
A single clock (Primary Reference Clock, PRC) handles the timing of transmission of signals & equipments across the entire network.  
  
**SONET Network Elements:**



1. **STS Multiplexer:**
   * Performs multiplexing of signals
   * Converts electrical signal to optical signal
2. **STS Demultiplexer:**
   * Performs demultiplexing of signals
   * Converts optical signal to electrical signal
3. **Regenerator:**

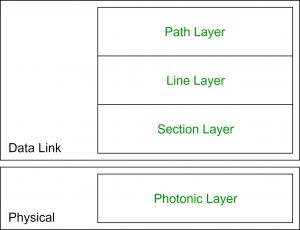
It is a repeater, that takes an optical signal and regenerates (increases the strength) it.

1. **Add/Drop Multiplexer:**

It allows to add signals coming from different sources into a given path or remove a signal.

**Why SONET is used?**  
SONET is used to convert an electrical signal into an optical signal so that it can travel longer distances.  
  
**SONET Connections:**

* **Section:** Portion of network connecting two neighbouring devices.
* **Line:** Portion of network connecting two neighbouring multiplexers.
* **Path:** End-to-end portion of the network.

**SONET Layers:**  
  
SONET includes four functional layers:

1. **Path Layer:**
   * It is responsible for the movement of signals from its optical source to its optical destination.
   * STS Mux/Demux provides path layer functions.
2. **Line Layer:**
   * It is responsible for the movement of signal across a physical line.
   * STS Mux/Demux and Add/Drop Mux provides Line layer functions.
3. **Section Layer:**
   * It is responsible for the movement of signal across a physical section.
   * Each device of network provides section layer functions.
4. **Photonic Layer:**
   * It corresponds to the physical layer of the OSI model.
   * It includes physical specifications for the optical fibre channel (presence of light = 1 and absence of light = 0).

**Advantages of SONET:**

* Transmits data to large distances
* Low electromagnetic interference
* High data rates
* Large Bandwidth

**synchronous Transfer Mode (ATM) in Computer Network**

**Why ATM networks?** 

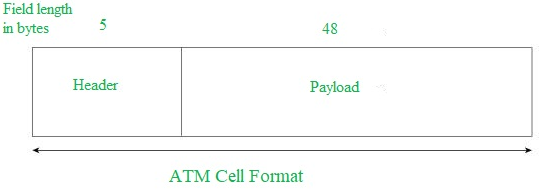
1. Driven by the integration of services and performance requirements of both telephony and data networking: “broadband integrated service vision” (B-ISON).
2. Telephone networks support a single quality of service and are expensive to boot.
3. Internet supports no quality of service but is flexible 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.

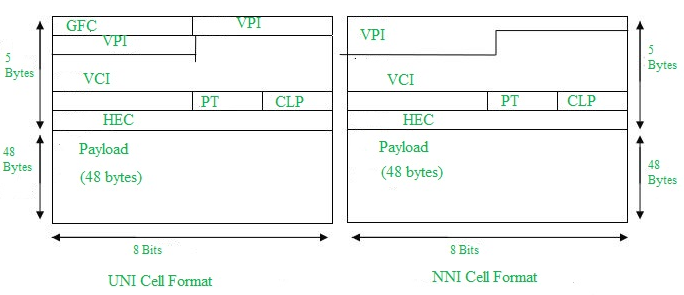
ATM is a technology that has some event in the development of broadband ISDN in the 1970s and 1980s, which can be considered an evolution of packet switching. *Each cell is 53 bytes long* – 5 bytes header and 48 bytes payload. Making an ATM call requires first sending a message to set up a connection.

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.

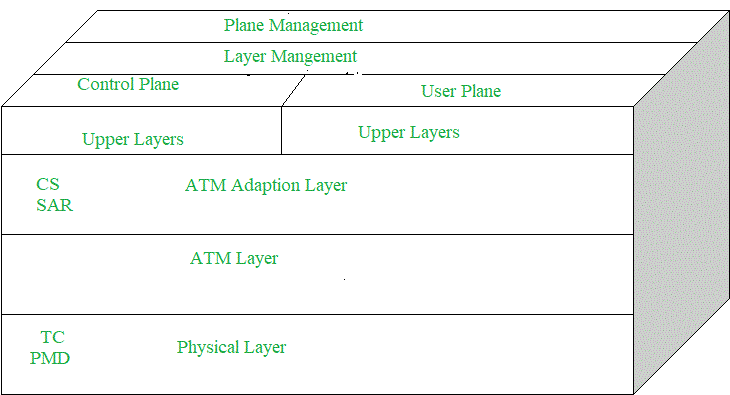
**ATM vs DATA Networks (Internet) –**

* 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.

**ATM Layers:**



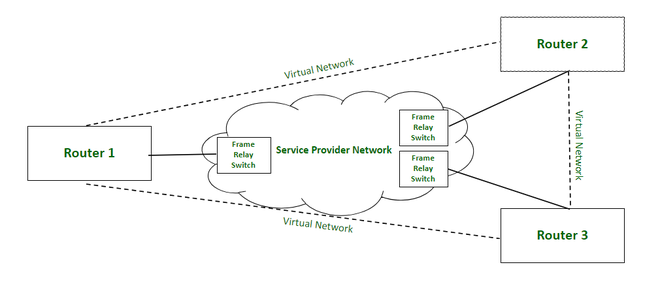
1. **ATM Adaption Layer (AAL) –**   
   It is meant for isolating higher-layer protocols from details of ATM processes and prepares for conversion of user data into cells and segments it into 48-byte cell payloads. AAL protocol excepts transmission from upper-layer services and helps them in mapping applications, e.g., voice, data to ATM cells.

1. **Physical Layer –**   
   It manages the medium-dependent transmission and is divided into two parts physical medium-dependent sublayer and transmission convergence sublayer. The main functions are as follows:
   * It converts cells into a bitstream.
   * It controls the transmission and receipt of bits in the physical medium.
   * It can track the ATM cell boundaries.
   * Look for the packaging of cells into the appropriate type of frames.
2. **ATM Layer –**   
   It handles transmission, switching, congestion control, cell header processing, sequential delivery, etc., and is responsible for simultaneously sharing the virtual circuits over the physical link known as cell multiplexing and passing cells through an ATM network known as cell relay making use of the VPI and VCI information in the cell header.

**ATM Applications:** 

1. **ATM WANs –**   
   It can be used as a WAN to send cells over long distances, a router serving as an end-point between ATM network and other networks, which has two stacks of the protocol.
2. **Multimedia virtual private networks and managed services –**   
   It helps in managing ATM, LAN, voice, and video services and is capable of full-service virtual private networking, which includes integrated access to multimedia.
3. **Frame relay backbone –**   
   Frame relay services are used as a networking infrastructure for a range of data services and enabling frame-relay ATM service to Internetworking services.
4. **Residential broadband networks –**   
   ATM is by choice provides the networking infrastructure for the establishment of residential broadband services in the search of highly scalable solutions.
5. **Carrier infrastructure for telephone and private line networks –**   
   To make more effective use of SONET/SDH fiber infrastructures by building the ATM infrastructure for carrying the telephonic and private-line traffic.

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

**Wireless Links**

* A number of important differences between a wired link and a wireless link:
  + Decreasing signal strength:
    - Electromagnetic radiation attenuates as it passes through matter. Even in free space, the signal will disperse, resulting in decreased signal strength as the distance between sender and receiver increases.
  + Interference from other sources:
    - Radio sources transmission in the same frequency band will interfere with each other.
    - In addition to interference from transmitting sources, electromagnetic noise within the environment can result in interference.
  + Multipath propagation:
    - It occurs when portions of the electromagnetic wave reflect off objects and the ground, taking paths of different lengths between a sender and receiver. Moving objects between the sender and receiver can cause multipath propagation to change over time.
* Wireless links employ powerful CRC error detection codes and link-level reliable-data-transfer protocols that retransmits corrupted frames because bit errors are more common in wireless links.
* The host receives an electromagnetic signal that is a combination of a degraded form of the original signal transmitted by the sender and background noise in the environment.
  + The **Signal-to-noise ratio (SNR)** is a relative measure of the strength of the received signal and this noise.
  + The SNR is typically measured in dB.
    - It is 20\*the ratio of the base-10 logarithms of the amplitude of the receives signal to the amplitude of the noise.
    - A larger SNR makes it easier for the receiver to extract the transmitted signal from the background noise.
* BER = Bit error rate
* Physical-layer characteristics that are important to understand for higher-layer wireless communication protocols:
  + For a given modulation scheme, the higher the SNR, the lower the BER:
    - Since a sender can increase the SNR by increasing its transmission power, a sender can decrease the probability that a frame is received in error by increasing its transmission power.
      * There’s little gain in increasing the power beyond a certain threshold.
    - A disadvantage associated with increasing the transmission power is that it costs more energy for the sender and the sender’s transmissions are more likely to interfere with transmissions of another sender.