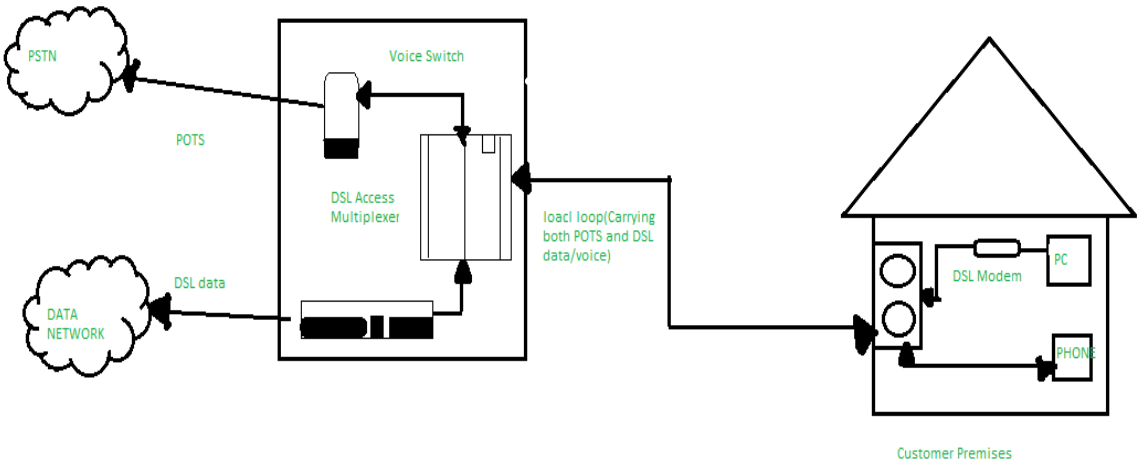
UNIT-5

DSL: (Digital Subscriber Line (O*riginally*, digital subscriber loop)): A technology for high-speed network or Internet access over voice lines. There are various types, including asymmetric DSL (ADSL), high-bit-rate DSL (HDSL), symmetric DSL (SDSL) and very-high-bit-rate DSL (VDSL). The whole group is sometimes referred to as "xDSL."

It is a communication medium, which is used to transfer internet through copper wire telecommunication line. **The DSL technology** is defined as the digital subscriber lines. Here, the data is transmitted to the users over the telephone signal lines.

Voice communication over the telephone is the best example of the digital subscriber lines. Also, there are DSL services that are provided by DSL technology Along with cable internet, DSL is one of the most popular ways *ISPs* provide broadband internet access.

- Its aim is to maintain the high speed of the data being transferred.
- If we ask that how we going to achieve such a thing i.e., both telephone and internet facility, then the answer is by using *splitters or DSL filters*(shown in the below diagram). Basically, the *splitter* is used to splits the frequency and make sure that they can't get interrupted.



Types of DSL –

1. **Symmetric DSL –** SDSL, *splits* the upstream and downstream frequencies evenly, providing equal speeds to both uploading and downloading data transfer. This connection may provide *2 Mbps* upstream and downstream.it is mostly preferred by small organizations.
2. **Asymmetric DSL –** ADSL, provides a wider frequency range for downstream transfers, which offers several times faster downstream speeds. an ADSL connection may offer *20 Mbps downstream and 1.5 Mbps upstream*, it is because most users download more data than they upload.

DSL Benefits –

- **No Additional Wiring –** A DSL connection makes use of your existing telephone wiring, so you will not have to pay for expensive upgrades to your phone system.
- **Cost-Effective –** DSL internet is a very cost-effective method and is best in connectivity
- Availability of DSL modems by the service providers.
- Users can use both telephone lines and the internet at the same time. And it is because the voice and digital signals are transferred in different frequencies.
- Users can choose between different connection *speeds* and *pricing* from various providers.

DSL Internet service only works over a limited physical distance and remains unavailable in many areas where the local telephone infrastructure does not support DSL technology. The service is not available everywhere. The connection is faster for receiving data than it is for sending data over the Internet.

The **services** provided by the companies that provide the DSL are −

- The broadband internet connection
- Voice communication
- Video streaming at low speed is offered by the companies using the DSL network.

Purpose of DSL: The purposes of DSL are explained below −

- DSL is used for maintaining or controlling the transferring speed of the internet.
- With the help of DSL filters or splitters we will be able to get the telephone service and internet service and splitters split the persistence and regularity therefore, it will not be able to disturbed.
- DSL technology is related to the family that comes in the xDSL in which x belongs to Asymmetric digital subscriber line (ADSL) etc.
- It provides better bandwidth of telephone lines as compared to the standard bandwidth. This phenomenon is known as broadband services.

Differences: The difference between digital subscriber line (DSL) and digital subscriber line access multiplexer (DSLAM) −

- The DSL is the network that is the digital subscriber line while the DSLAM is the digital subscriber line access multiplexer that is derived from the DSL network.
- The DSL subscriber line network is used by the single user while the digital subscriber line access multiplexer allows connecting multiple digital subscriber lines that helps to use the networks using the multiplexing.
- The topology used for the cable modem for the data transfer is the star topology that is used for the scale model for the data transfer system.

Network Cabling: Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with

LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

Types of cables used in networks

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable
- Wireless LANs

Twisted pair cabling comes in two varieties: shielded and unshielded. **Unshielded twisted pair** (UTP) is the most popular and is generally the best option for school networks

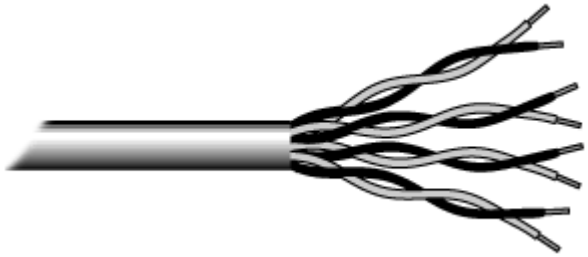


Fig.1. Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire (additional categories are emerging).

Categories of Unshielded Twisted Pair:

Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet

4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair)	100BaseT Ethernet
	1000 Mbps (4 pair)	Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

Unshielded Twisted Pair Connector: The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector. A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

Fig. 2. RJ-45 connector

Shielded Twisted Pair (STP) Cable: Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

Shielded twisted pair cable is available in three different configurations:

1. Each pair of wires is individually shielded with foil.
2. There is a foil or braid shield inside the jacket covering all wires (as a group).
3. There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

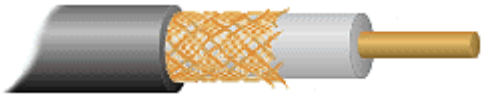


Fig. 3. Coaxial cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable has been popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See fig. 4). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.

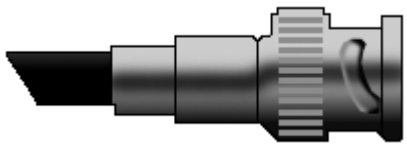


Fig. 4. BNC connector

Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

The center core of fiber cables is made from glass or plastic fibers (see fig 5). A plastic coating then cushions the fiber center, and kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of teflon or PVC.

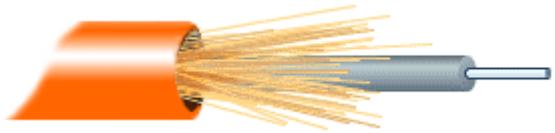


Fig. 5. Fiber optic cable

There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

Specification	Cable Type
10BaseT	Unshielded Twisted Pair
10Base2	Thin Coaxial
10Base5	Thick Coaxial
100BaseT	Unshielded Twisted Pair
100BaseFX	Fiber Optic
100BaseBX	Single mode Fiber
100BaseSX	Multimode Fiber
1000BaseT	Unshielded Twisted Pair
1000BaseFX	Fiber Optic
1000BaseBX	Single mode Fiber
1000BaseSX	Multimode Fiber

Installing Cable - Some Guidelines

When running cable, it is best to follow a few simple rules:

- Always use more cable than you need. Leave plenty of slack.
- Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.

Wireless LANs

More and more networks are operating without cables, in the wireless mode. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations, servers, or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

Wireless networks are great for allowing laptop computers, portable devices, or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network. Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

Wireless standards and speeds

The Wi-Fi Alliance is a global, non-profit organization that helps to ensure standards and interoperability for wireless networks, and wireless networks are often referred to as WiFi (Wireless Fidelity). The original Wi-Fi standard (IEEE 802.11) was adopted in 1997. Since then many variations have emerged (and will continue to emerge). Wi-Fi networks use the Ethernet protocol.

Standard	Max Speed	Typical Range
802.11a	54 Mbps	150 feet
802.11b	11 Mbps	300 feet
802.11g	54 Mbps	300 feet
802.11n	100 Mbps	300+ feet

Wireless Security

Wireless networks are much more susceptible to unauthorized use than cabled networks. Wireless network devices use radio waves to communicate with each other. The greatest vulnerability to the network is that rogue machines can "eves-drop" on the radio wave communications. Unencrypted information transmitted can be monitored by a third-party, which, with the right tools (free to download), could quickly gain access to your entire network, steal valuable passwords to local servers and online services, alter or destroy data, and/or access personal and confidential information stored in your network servers. To minimize the possibility of this, all modern access points and devices have configuration options to encrypt transmissions. These encryption methodologies are still evolving, as are the tools used by malicious hackers, so always use the strongest encryption available in your access point and connecting devices.

Three basic techniques are used to protect networks from unauthorized wireless use. Use any and all of these techniques when setting up your wireless access points:

Encryption.

Enable the strongest encryption supported by the devices you will be connecting to the network. Use strong passwords (strong passwords are generally defined as passwords containing symbols, numbers, and mixed case letters, at least 14 characters long).

Isolation.

Use a wireless router that places all wireless connections on a subnet independent of the primary private network. This protects your private network data from pass-through internet traffic.

Hidden SSID.

Every access point has a Service Set IDentifier (SSID) that by default is broadcast to client devices so that the access point can be found. By disabling this feature, standard client connection software won't be able to "see" the access point. However, the eves-dropping programs discussed previously can easily find these access points, so this alone does little more than keep the access point name out of sight for casual wireless users.

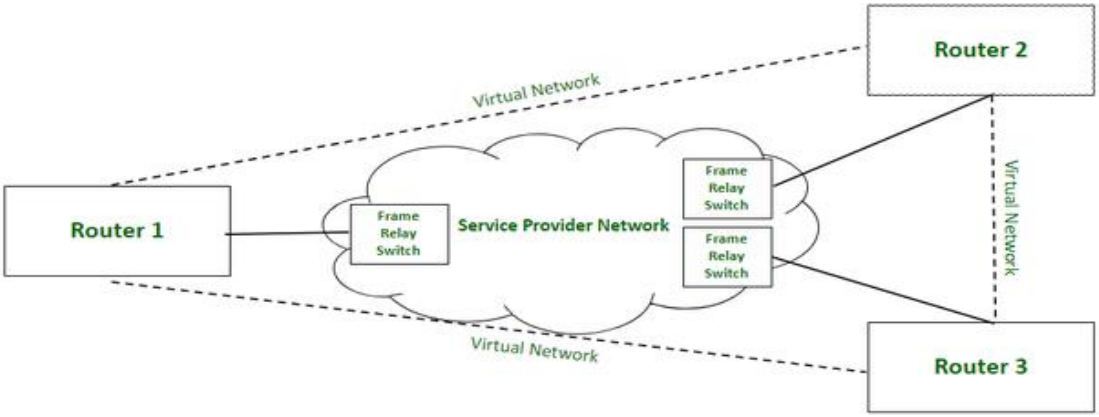
Advantages of wireless networks:

- Mobility - With a laptop computer or mobile device, access can be available throughout a school, at the mall, on an airplane, etc. More and more businesses are also offering free WiFi access ("Hot spots").
- Fast setup - If your computer has a wireless adapter, locating a wireless network can be as simple as clicking "Connect to a Network" -- in some cases, you will connect automatically to networks within range.
- Cost - Setting up a wireless network can be much more cost effective than buying and installing cables.
- Expandability - Adding new computers to a wireless network is as easy as turning the computer on (as long as you do not exceed the maximum number of devices).

Disadvantages of wireless networks:

- Security - Be careful. Be vigilant. Protect your sensitive data with backups, isolated private networks, strong encryption and passwords, and monitor network access traffic to and from your wireless network.
- Interference - Because wireless networks use radio signals and similar techniques for transmission, they are susceptible to interference from lights and electronic devices.
- Inconsistent connections - How many times have you hears "Wait a minute, I just lost my connection?" Because of the interference caused by electrical devices and/or items blocking the path of transmission, wireless connections are not nearly as stable as those through a dedicated cable.
- Speed - The transmission speed of wireless networks is improving; however, faster options (such as gigabit Ethernet) are available via cables. If you are only using wireless for internet access, the actual internet connection for your home or school is generally slower than the wireless network devices, so that connection is the bottleneck. If you are also moving large amounts of data around a private network, a cabled connection will enable that work to proceed much faster.

Frame Relay: 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

VPN : VPN stands for **"Virtual Private Network"** and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in **real time**.

How does a VPN work?

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.

Benefits of a VPN connection: A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can't decipher this data.

Secure encryption: To read the data, you need an *encryption key* . Without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack . With the help of a VPN, your online activities are hidden even on public networks.

Disguising your whereabouts : VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand, record your behavior, but do not pass this information on to third parties. This means that any potential record of your user behavior remains permanently hidden.

Access to regional content: Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With **VPN location spoofing** , you can switch to a server to another country and effectively "change" your location.

Secure data transfer: If you work remotely, you may need to access important files on your company's network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

Why should you use a VPN connection?

Your ISP usually sets up your connection when you connect to the internet. It tracks you via an IP address. Your network traffic is routed through your ISP's servers, which can log and display everything you do online.

Your ISP may seem trustworthy, but it may share your browsing history with advertisers, the police or government, and/or other third parties. ISPs can also fall victim to attacks by cyber criminals: If they are hacked, your personal and private data can be compromised.

This is especially important if you regularly connect to public Wi-Fi networks. You never know who might be monitoring your internet traffic and what they might steal from you, including passwords, personal data, payment information, or even your entire identity.

What should a good VPN do?

You should rely on your VPN to perform one or more tasks. The VPN itself should also be protected against compromise. These are the features you should expect from a comprehensive VPN solution:

- **Encryption of your IP address:** The primary job of a VPN is to hide your IP address from your ISP and other third parties. This allows you to send and receive information online without the risk of anyone but you and the VPN provider seeing it.
- **Encryption of protocols:** A VPN should also prevent you from leaving traces, for example, in the form of your internet history, search history and cookies. The encryption of cookies is especially important because it prevents third parties from gaining access to confidential information such as personal data, financial information and other content on websites.
- **Kill switch:** If your VPN connection is suddenly interrupted, your secure connection will also be interrupted. A good VPN can detect this sudden downtime and terminate preselected programs, reducing the likelihood that data is compromised.
- **Two-factor authentication:** By using a variety of authentication methods, a strong VPN checks everyone who tries to log in. For example, you might be prompted to enter a password, after which a code is sent to your mobile device. This makes it difficult for uninvited third parties to access your secure connection.

History of VPNs

Since humans have been using the internet, there has been a movement to protect and encrypt internet browser data. The US Department of Defense already got involved in projects working on the encryption of internet communication data back in the 1960s.

Predecessors of the VPN

Their efforts led to the creation of **ARPANET** (Advanced Research Projects Agency Network), a packet switching network, which in turn led to the development of the Transfer Control Protocol/Internet Protocol (TCP/IP).
The **TCP/IP** had four levels: **Link, internet, transport and application**. At the internet level, local networks and devices could be connected to the universal network – and this is where the risk of exposure became clear. In 1993, a team from Columbia University and AT&T Bell Labs finally succeeded in creating a kind of first version of the modern VPN, known as swIPe: Software IP encryption protocol.

In the following year, Wei Xu developed the IPSec network, an internet security protocol that authenticates and encrypts information packets shared online. In 1996, a Microsoft employee named Gurdeep Singh-Pall created a Peer-to-Peer Tunneling Protocol (PPTP).

Early VPNs

Contiguous to Singh-Pall developing PPTP, the internet was growing in popularity and the need for consumer-ready, sophisticated security systems emerged. At that time, anti-virus programs were already effective in preventing malware and spyware from infecting a computer system. However, people and companies also started demanding encryption software that could hide their browsing history on the internet.

The first VPNs therefore started in the early 2000s, but were almost exclusively used by companies. However, after a flood of security breaches, especially in the early 2010s, the consumer market for VPNs started to pick up.

VPNs and their current use

According to the ***GlobalWebIndex***, the number of VPN users worldwide increased more than fourfold between 2016 and 2018. In countries such as Thailand, Indonesia and China, where internet use is restricted and censored, **one in fiveinternet users** uses a VPN. In the USA, Great Britain and Germany, the proportion of VPN users is **lowerat around 5%**, but is growing.

One of the biggest drivers for VPN adoption in recent years has been the increasing demand for content with geographical access restrictions. For example, video streaming services such as Netflix or YouTube make certain videos available only in certain countries. With contemporary VPNs, you can encrypt your IP address so that you appear to be surfing from another country, enabling you to access this content from anywhere.

Here's how to surf securely with a VPN

A VPN encrypts your surfing behavior, which can only be decoded with the help of a key. Only your computer and the VPN know this key, so your ISP cannot recognize where you are surfing. Different VPNs use different encryption processes, but generally function in three steps:

1. Once you are online, start your VPN. The VPN acts as a secure tunnel between you and the internet. Your ISP and other third parties cannot detect this tunnel.
2. Your device is now on the local network of the VPN, and your IP address can be changed to an IP address provided by the VPN server.
3. You can now surf the internet at will, as the VPN protects all your personal data.

What kind of VPNs are there?

There are many different types of VPNs, but we should be familiar with the three main types:

1. SSL VPN

Often not all employees of a company have access to a company laptop they can use to work from home. During the corona crisis in Spring 2020, many companies faced the problem of not having enough equipment for their employees. In such cases, use of a private device (PC, laptop, tablet, mobile phone) is often resorted to. In this case, companies fall back on an **SSL-VPN** solution, which is usually implemented via a corresponding hardware box.

The prerequisite is usually an HTML-5-capable browser, which is used to call up the company's login page. HTML-5 capable browsers are available for virtually any operating system. Access is guarded with a username and password.

2. Site-to-site VPN

A **site-to-site VPN** is essentially a private network designed to hide private intranets and allow users of these secure networks to access each other's resources.

A site-to-site VPN is useful if you have multiple locations in your company, each with its own local area network (LAN) connected to the WAN (Wide Area Network). Site-to-site VPNs are also useful if you have two separate intranets between which you want to send files without users from one intranet explicitly accessing the other.

Site-to-site VPNs are mainly used in large companies. They are complex to implement and do not offer the same flexibility as SSL VPNs. However, they are the most effective way to ensure communication within and between large departments.

3. Client-to-Server VPN

Connecting via a **VPN client** can be imagined as if you were connecting your home PC to the company with an extension cable. Employees can dial into the company network from their home office via the secure connection and act as if they were sitting in the office. However, a VPN client must first be installed and configured on the computer.

This involves the user not being connected to the internet via his own ISP, but establishing a direct connection through his/her VPN provider. This essentially shortens the tunnel phase of the VPN journey. Instead of using the VPN to create an encryption tunnel to disguise the existing internet connection, the VPN can automatically encrypt the data before it is made available to the user.

This is an increasingly common form of VPN, which is particularly useful for providers of insecure public WLAN. It prevents third parties from accessing and compromising the network connection and encrypts data all the way to the provider. It also prevents ISPs from accessing data that, for whatever reason, remains unencrypted and bypasses any restrictions on the user's internet access (for instance, if the government of that country restricts internet access).

The advantage of this type of VPN access is greater efficiency and universal access to company resources. Provided an appropriate telephone system is available, the employee can, for example, connect to the system with a headset and act as if he/she were at their company workplace. For example, customers of the company cannot even tell whether the employee is at work in the company or in their home office.

ATM: An ATM, which stands for automated teller machine, is a specialized computer that makes it convenient to manage a bank account holder’s funds. It allows a person to check account balances, withdraw or deposit money, print a statement of account activities or transactions, and even purchase stamps.

An automated teller machine (ATM) is an electronic banking outlet that allows customers to complete basic transactions without the aid of a branch representative or teller. Anyone with a credit card or debit card can access cash at most ATMs, either in the USA or abroad.

ATMs are convenient, allowing consumers to perform quick self-service transactions such as deposits, cash withdrawals, bill payments, and transfers between accounts. Fees are commonly charged for cash withdrawals by the bank where the account is located, by the operator of the ATM, or by both. Some or all of these fees can be avoided by using an ATM operated directly by the bank that holds the account. Using an ATM abroad can cost more than using one in the USA.

ATMs are known in different parts of the world as automated bank machines (ABMs) or cash machines.

ATM examples: An account holder can use an ATM to carry out a number of transactions.

Withdrawals are the most common transaction among ATM cardholders. This allows them to withdraw cash from their accounts. For a withdrawal, account holders just have to key in the amount they wish to take out.

ATM deposits also are becoming popular. Account holders can deposit money and checks if their bank allows it.

Balance inquiries allow account holders to view their current account balance. This feature may be helpful if account holders need to know the amount of money they can spend with their debit card or credit card.

Transfers and payments are also available depending on the bank. This allows account holders to move money from one account to another, without withdrawing cash.

Account holders using an ATM not affiliated with their bank will most likely have to pay a fee. ATMs always disclose these fees on their screens, and they give users an option to cancel the transaction if they do not want to pay the fee.

In the U.S., the average fee for a single ATM withdrawal is about $4.52. This fee usually varies from state to state. Atlanta usually has the highest average fees at about $5.15, while Seattle has the lowest average ATM fees at $4.21.

Users should be aware of the threats that target these machines. For safety reasons, users should transact at ATMs located in well-lit public places.

Types of ATMs

There are two primary types of ATMs. Basic units only allow customers to withdraw cash and receive updated account balances. The more complex machines accept deposits, facilitate line of credit payments and transfers, and access account information.

To access the advanced features of the complex units, a user often must be an account holder at the bank that operates the machine.

Analysts anticipate ATMs will become even more popular and forecast an increase in the number of ATM withdrawals. ATMs of the future are likely to be full-service terminals instead of or in addition to traditional bank tellers.

\

ATM Design Elements

Although the design of each ATM is different, they all contain the same basic parts:

- **Card reader:** This part reads the chip on the front of the card or the magnetic stripe on the back of the card.

- **Keypad:** The keypad is used by the customer to input information, including personal identification number (PIN), the type of transaction required, and the amount of the transaction.
- **Cash dispenser:** Bills are dispensed through a slot in the machine, which is connected to a safe at the bottom of the machine.
- **Printer:** If required, consumers can request receipts that are printed out of the ATM. The receipt records the type of transaction, the amount, and the account balance.
- **Screen:** The ATM issues prompts that guide the consumer through the process of executing the transaction. Information is also transmitted on the screen, such as account information and balances.

Full-service machines now often have slots for depositing paper checks or cash.

How to Use an ATM

Banks place ATMs inside and outside of their branches. Other ATMs are located in high-traffic areas such as shopping centers, grocery stores, convenience stores, airports, bus and railway stations, gas stations, casinos, restaurants, and other locations. Most ATMs that are found in banks are multifunctional, while others that are off-site tend to be primarily or entirely designed for cash withdrawals.

ATMs require consumers to use a plastic card—either a bank debit card or a credit card—to complete a transaction. Consumers are authenticated by a PIN before any transaction can be made.

Many cards come with a chip, which transmits data from the card to the machine. These work in the same fashion as a bar code that is scanned by a code reader.

ATM Fees

Account holders can use their bank's ATMs at no charge, but accessing funds through a unit owned by a competing bank usually incurs a fee. According to MoneyRates.com, the average total fees to withdraw cash from an out-of-network ATM was $4.55 as of 2022.7

Some banks will reimburse their customers for the fee, especially if there is no corresponding ATM available in the area.

So, if you're one of those people who draws weekly spending money from an ATM, using the wrong machine could cost you nearly $240 a year.

ATM Ownership

In many cases, banks and credit unions own ATMs. However, individuals and businesses may also buy or lease ATMs on their own or through an ATM franchise. When individuals or small businesses such as restaurants or gas stations own ATMs, the profit model is based on charging fees to the machine's users.

Banks also own ATMs with this intent. They use the convenience of an ATM to attract clients. ATMs also take some of the customer service burdens from bank tellers, saving banks money in payroll costs.

Using ATMs Abroad

ATMs make it simple for travelers to access their checking or savings accounts from almost anywhere in the world.

Travel experts advise consumers to use foreign ATMs as a source of cash abroad, as they generally receive a more favorable exchange rate than they would at most currency exchange offices.

However, the account holder's bank may charge a transaction fee or a percentage of the amount exchanged. Most ATMs do not list the exchange rate on the receipt, making it difficult to track spending.

How much can you withdraw from an automated teller machine (ATM)?

The amount that you can withdraw from an automated teller machine (ATM) per day, per week, or per month will vary based on your bank and account status at that bank. For most account holders, for instance, Capital One imposes a $1,000 daily ATM withdrawal limit and Well Fargo just $300.8 You may be able to get around these limits by calling your bank to request permission or upgrading your banking status by depositing more funds.

How do you make a deposit at an ATM?

If you are a bank's customer, you may be able to deposit cash or checks via one of their ATMs. To do this, you may simply need to insert the checks or cash directly into the machine. Other machines may require you to fill out a deposit slip and put the money into an envelope before inserting it into the machine. For a check, be sure to endorse the back of your check and note "For Deposit Only" to be safe.

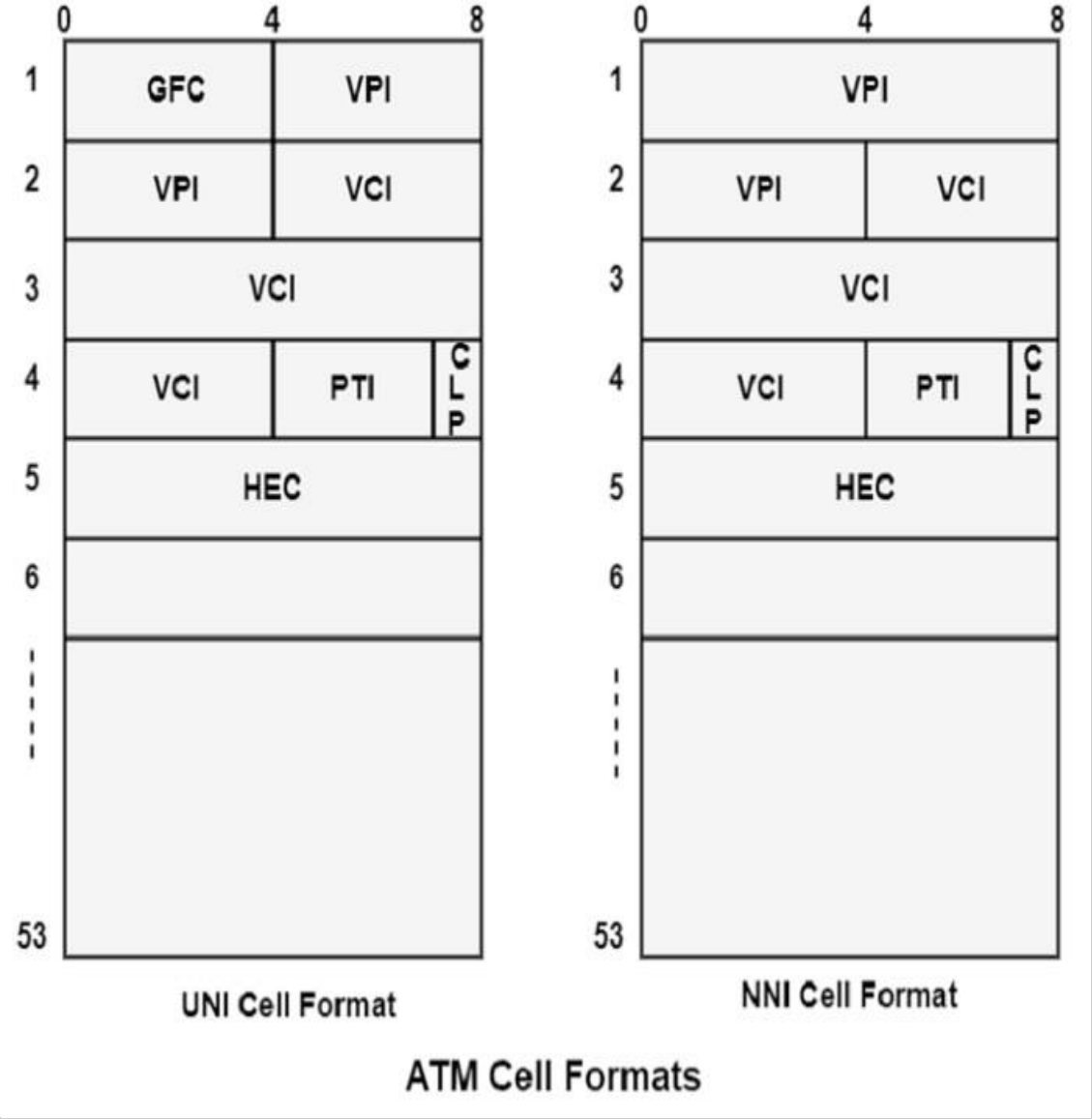
Which bank installed the first ATM in the United States?

The first ATM in the United States was installed by Chemical Bank in Rockville Center (Long Island), N.Y., in 1969 (two years after Barclays installed the first ATM in the United Kingdom). By the end of 1971, more than 1,000 ATMs were installed worldwide.9

ATM Cell Format

An ATM cell header can be two formats, such as User Network Interface (UNI) or Network to Network Interface (NNI). The UNI header can be used for communication between ATM endpoints and ATM switches in private ATM networks. The NNI header can be used for communication between ATM switches.

The figure shows the ATM UNI cell header format and the ATM NNI cell header format. Unlike the UNI, the NNI header does not contain the Generic Flow Control (GFC) field. The NNI header has a Virtual Path Identifier (VPI) field that appears in the first 12 bits. It is allowing for high trunks between public ATM switches.



ATM Cell Header Fields

The following definitions summarise the ATM cell header fields as shown in the figure above −

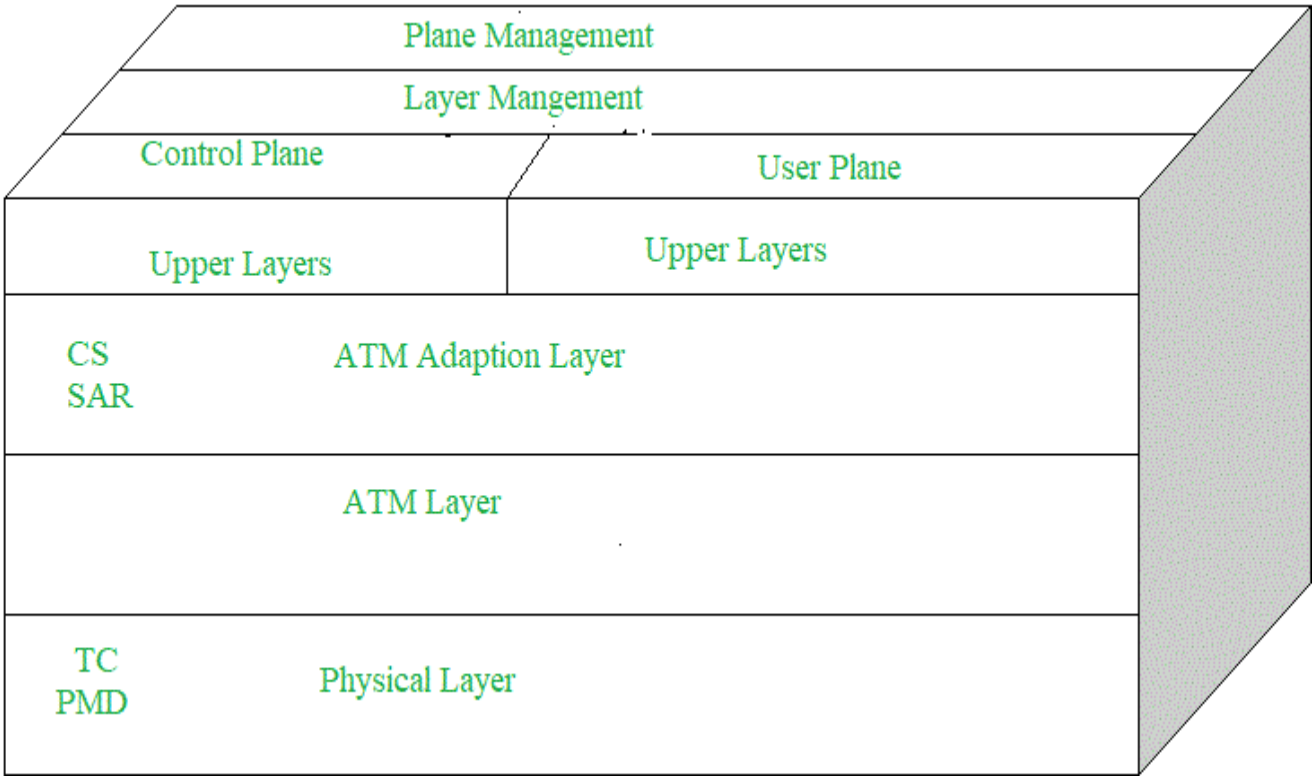
- **Generic Flow Control (GFC)** − It supports local functions, such as recognizing multiple stations that send a single ATM interface. This field is generally not used and is set to its default value of 0 (binary 0000).

- **Virtual Path Identifier (VPI)** − In conjunction with the Virtual Channel Identifier (VCI), it recognises the next destination of a cell as it transfers through a series of ATM switches on the way to its destination.
- **Virtual Channel Identifier (VCI)** − In conjunction with the VPI, it recognizes the next destination of a cell as it transfers through a series of ATM switches on the way to its destination.
- **Payload Type (PT)** − It denotes in the first bit whether the cell includes user data or control data. If the cell includes user data, the bit is set to 0. If it includes control data, it is

set to 1. The second bit denotes congestion (0 = no congestion, 1 = congestion), and the third bit denotes whether the cell is the last in a sequence of cells that define a single AAL5 frame (1 = last cell for the frame).

- **Cell Loss Priority (CLP)** − It denotes whether the cell should be removed if it encounters extreme congestion as it transfers through the network. Suppose the CLP bit similar is to 1, and the cell should be discarded in preference to cells with the CLP bit equal to 0.
- **Header Error Control (HEC)** − It evaluates checksum only on the first 4 bytes of the header. It can be valid a single bit error in these bytes, thereby preserving the cell instead of discarding it.

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.

2. **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.
-

3. **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:

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.

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.

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.

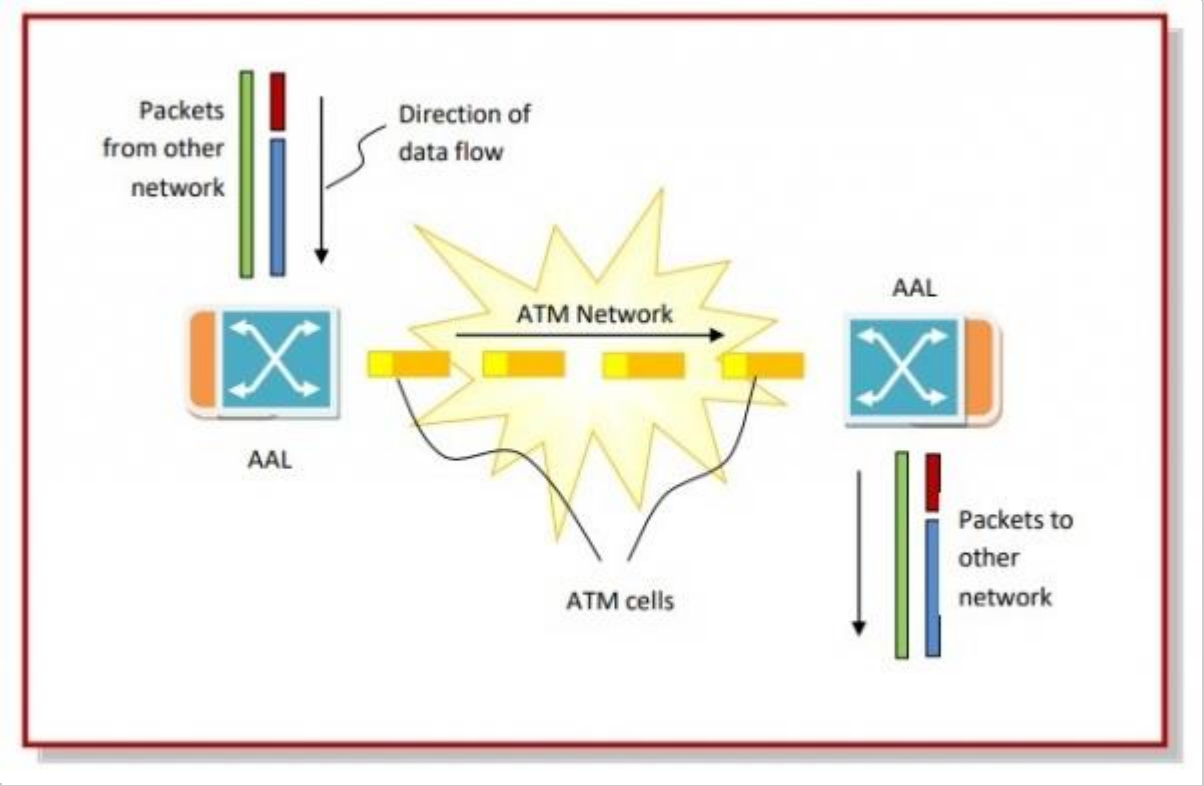
Residential broadband networks – ATM is by choice provides the networking infrastructure for the establishment of residential broadband services in the search of highly scalable solutions.

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.

AAL LAYER: In Asynchronous Transfer Mode (ATM) networks, the ATM Adaptation Layer (AAL) provides facilities for non-ATM based networks to connect to ATM network and use its services.

AAL is basically a software layer that accepts user data, which may be digitized voice, video or computer data, and makes them suitable for transmission over an ATM network. The transmissions can be of fixed or variable data rate. AAL accepts higher layer packets and segments them into fixed sized ATM cells before transmission via ATM. It also reassembles the received segments to the higher layer packets.

The following diagram illustrates the function of AAL −



This layer has two sub layers −

1. Convergence sub layer
2. Segmentation and Reassembly sub layer.

Some networks that need AAL services are Gigabit Ethernet, IP, Frame Relay, SONET/SDH and UMTS/Wireless.

AAL Protocols: International Telecommunication Union Telecommunication Standardization Sector (ITU-T) has defined five AAL protocols to provide the range of services.

AAL Type 0 − This is the simplest service that provides direct interface to ATM services without any restrictions. These cells are called raw cells that contain 48-byte payload field without any special fields. It lacks guaranteed delivery and interoperability.

AAL Type 1 − This service provides interface for synchronous, connection oriented traffic. It supports constant rate bit stream between the two ends of an ATM link. An AAL 1 cell contains a 4-bit sequence number, a 4-bit sequence number protection and a 47-byte payload field.

AAL Type 2 − This service also provides interface for synchronous, connection oriented traffic. However, this is for variable rate bit stream between the two ends of an ATM link. It is used in wireless applications.

AAL Type 3/4 − This includes a range of services for variable rate data or bit stream. It is suitable for both connection – oriented, asynchronous traffic as well as connectionless traffic. These ATM cells contain a 4-byte header.

AAL Type 5 − AAL 5 provides the similar services as AAL 3/4, but with simplified header information. It was originally named Simple and Efficient Adaptation Layer (SEAL). It is used in a number of areas like Internet Protocol (IP) over ATM, Ethernet over ATM and Switched Multimegabit Data Service (SMDS).

PPP Protocol: The PPP stands for Point-to-Point protocol. It is the most commonly used protocol for point-to-point access. Suppose the user wants to access the internet from the home, the PPP protocol will be used.

It is a data link layer protocol that resides in the layer 2 of the OSI model. It is used to encapsulate the layer 3 protocols and all the information available in the payload in order to be transmitted across the serial links. The PPP protocol can be used on synchronous link like ISDN as well as asynchronous link like dial-up. It is mainly used for the communication between the two devices.

It can be used over many types of physical networks such as serial cable, phone line, trunk line, cellular telephone, fiber optic links such as SONET. As the data link layer protocol is used to identify from where the transmission starts and ends, so ISP (Internet Service Provider) use the PPP protocol to provide the dial-up access to the internet

Services provided by PPP

- It defines the format of frames through which the transmission occurs.
- It defines the link establishment process. If user establishes a link with a server, then "how this link establishes" is done by the PPP protocol.
- It defines data exchange process, i.e., how data will be exchanged, the rate of the exchange.
- The main feature of the PPP protocol is the encapsulation. It defines how network layer data and information in the payload are encapsulated in the data link frame.
- It defines the authentication process between the two devices. The authentication between the two devices, handshaking and how the password will be exchanged between two devices are decided by the PPP protocol.

Services Not provided by the PPP protocol

- It does not support flow control mechanism.
- It has a very simple error control mechanism.
- As PPP provides point-to-point communication, so it lacks addressing mechanism to handle frames in multipoint configuration.

It is a byte-oriented protocol as it provides the frames as a collection of bytes or characters. It is a WAN (Wide Area Network) protocol as it runs over the internet link which means between two routers, internet is widely used.

PPP has two main uses which are given below:

- It is widely used in broadband communications having heavy loads and high speed. For example, an internet operates on heavy load and high speed.
- It is used to transmit the multiprotocol data between the two connected (point-to-point) computers. It is mainly used in point-to-point devices, for example, routers are point-to-point devices where PPP protocol is widely used as it is a WAN protocol not a simple LAN ethernet protocol.

Frame format of PPP protocol

- **Flag:** The flag field is used to indicate the start and end of the frame. The flag field is a 1-byte field that appears at the beginning and the ending of the frame. The pattern of the flag is similar to the bit pattern in HDLC, i.e., 01111110.
- **Address:** It is a 1-byte field that contains the constant value which is 11111111. These 8 ones represent a broadcast message.
- **Control:** It is a 1-byte field which is set through the constant value, i.e., 11000000. It is not a required field as PPP does not support the flow control and a very limited error control mechanism. The control field is a mandatory field where protocol supports flow and error control mechanism.
- **Protocol:** It is a 1 or 2 bytes field that defines what is to be carried in the data field. The data can be a user data or other information.
- **Payload:** The payload field carries either user data or other information. The maximum length of the payload field is 1500 bytes.
- **Checksum:** It is a 16-bit field which is generally used for error detection.

Transition phases of PPP protocol

- **Dead:** Dead is a transition phase which means that the link is not used or there is no active carrier at the physical layer.
- **Establish:** If one of the nodes starts working then the phase goes to the establish phase. In short, we can say that when the node starts communication or carrier is detected then it moves from the dead to the establish phase.
- **Authenticate:** It is an optional phase which means that the communication can also moves to the authenticate phase. The phase moves from the establish to the authenticate phase only when both the communicating nodes agree to make the communication authenticated.
- **Network:** Once the authentication is successful, the network is established or phase is network. In this phase, the negotiation of network layer protocols take place.
- **Open:** After the establishment of the network phase, it moves to the open phase. Here open phase means that the exchange of data takes place. Or we can say that it reaches to the open phase after the configuration of the network layer.
- **Terminate:** When all the work is done then the connection gets terminated, and it moves to the terminate phase.

On reaching the terminate phase, the link moves to the dead phase which indicates that the carrier is dropped which was earlier created.

There are two more possibilities that can exist in the transition phase:

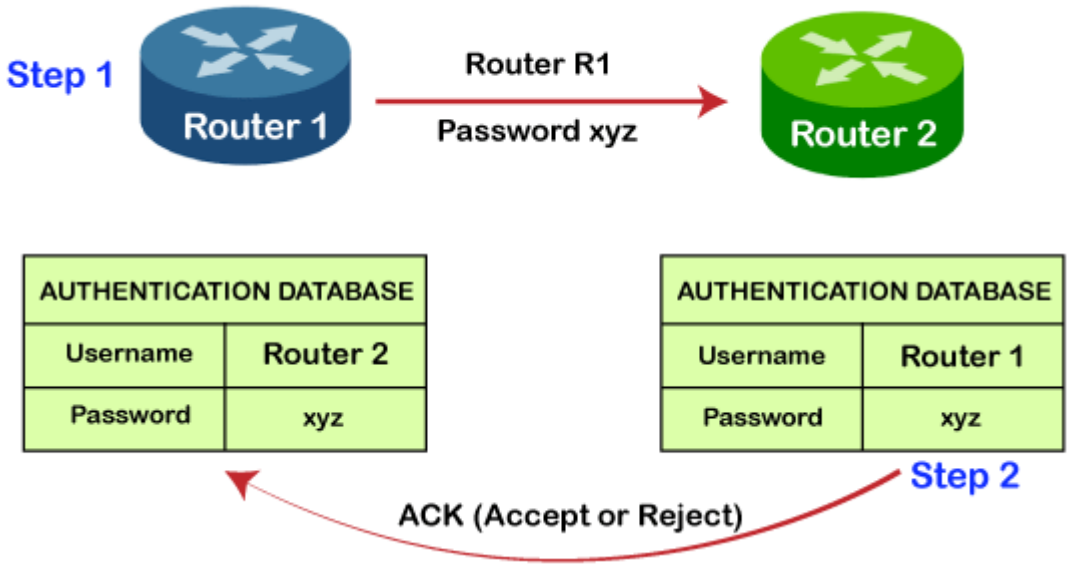
- The link moves from the authenticate to the terminate phase when the authentication is failed.
- The link can also move from the establish to the dead state when the carrier is failed.

PPP Stack: In PPP stack, there are three set of protocols:

- **Link Control Protocol (LCP):** The role of LCP is to establish, maintain, configure, and terminate the links. It also provides negotiation mechanism.

- **Authentication protocols:** There are two types of authentication protocols, i.e., PAP (Password Authenticate protocols), and CHAP (Challenged Handshake Authentication Protocols).

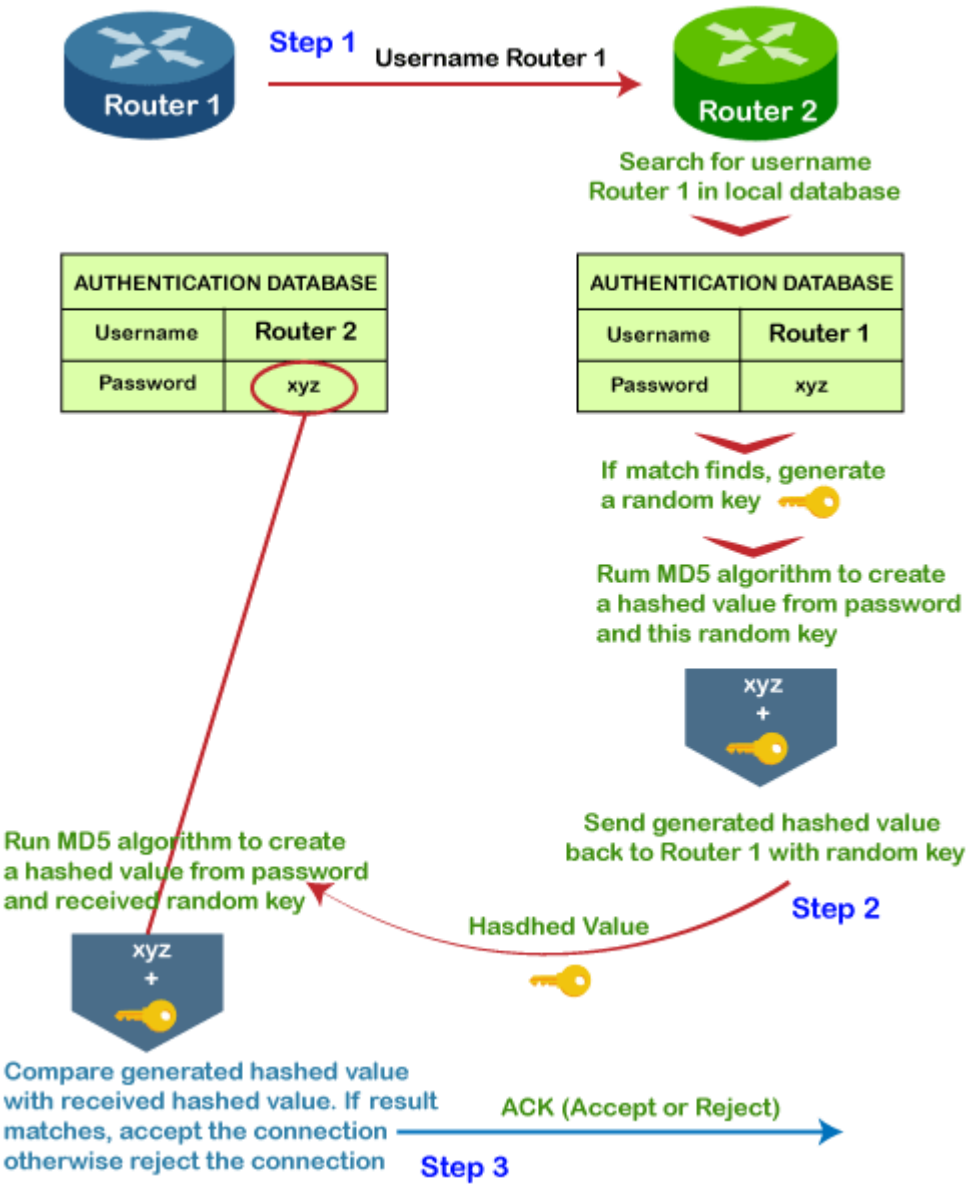
1. PAP (Password Authentication Protocols)



PAP is less secure as compared to CHAP as in case of PAP protocol, password is sent in the form of a clear text. It is a two-step process. Suppose there are two routers, i.e., router 1 and router 2. In the first step, the router 1 wants to authenticate so it sends the username and password for the authentication. In the second step, if the username and password are matched then the router 2 will authenticate the router 1 otherwise the authentication failed.

2. CHAP (Challenged Handshake Authentication Protocol)

CHAP is a three-step process:



Step 1: Suppose there are two routers, i.e., router 1 and router 2. In this step, router 1 sends the username but not the password to the router 2.

Step 2: The router 2 maintains a database that contains a list of allowed hosts with their login credentials. If no data is found which means that the router 1 is not a valid host to connect with it and the connection gets terminated. If the match is found then the random key is passed. This random key along with the password is passed in the MD5 hashing function, and the hashing function generates the hashed value from the password and the random key (password + random key). The hashed value is also known as Challenge. The challenge along with the random key will be sent to the router 1.

Step 3: The router 1 receives the hashed value and a random key from the router 2. Then, the router 1 will pass the random key and locally stored password to the MD5 hashing function. The MD5 hashing function generates the hashed value from the combination of random key and password. If the generated hashed value does not match with the received hashed value then the connection gets terminated. If it is matched, then the connection is granted. Based on

the above authentication result, the authentication signal that could be either accepted or rejected is sent to the router 2.

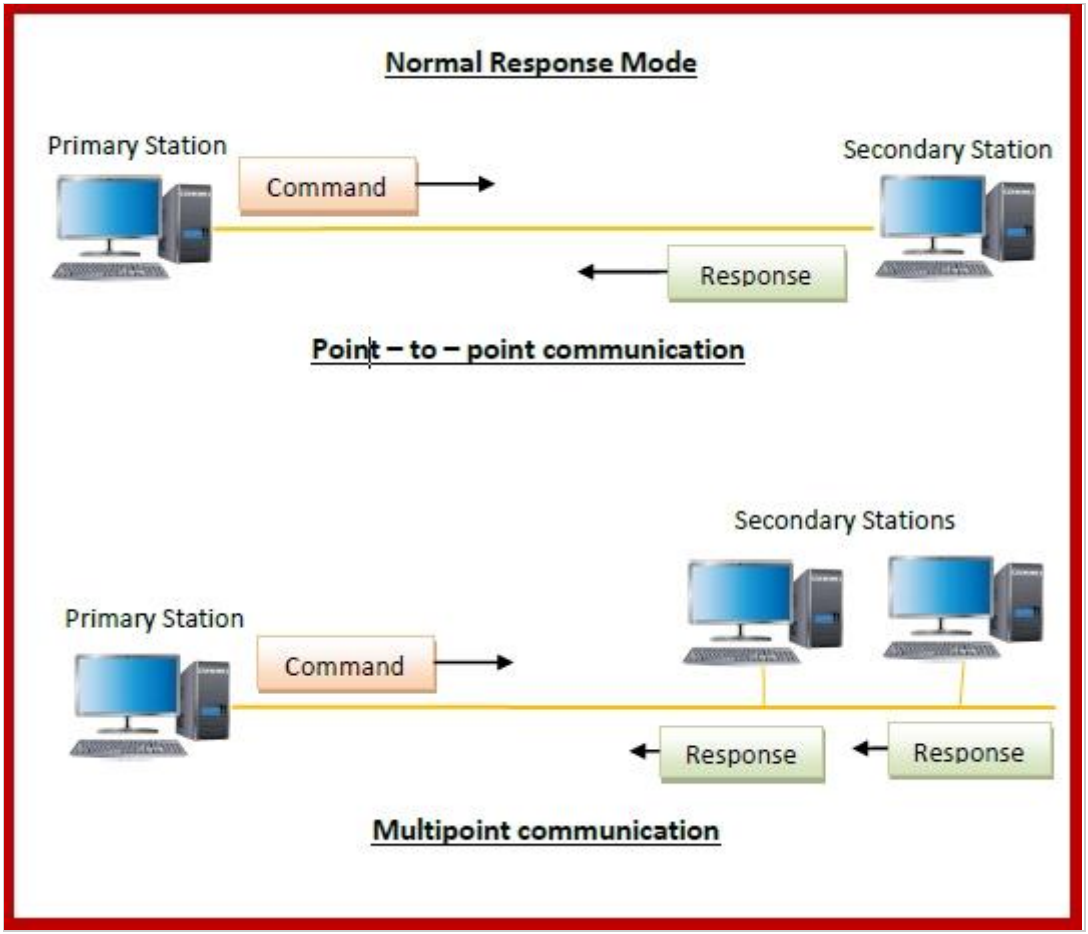
- **Network Control Protocol (NCP):** After the establishment of the link and authentication, the next step is to connect to the network layer. So, PPP uses another protocol known as network control protocol (NCP). The NCP is a set of protocols that facilitates the encapsulation of data which is coming from the network layer to the PPP frames.

High-level Data Link Control (HDLC): It is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

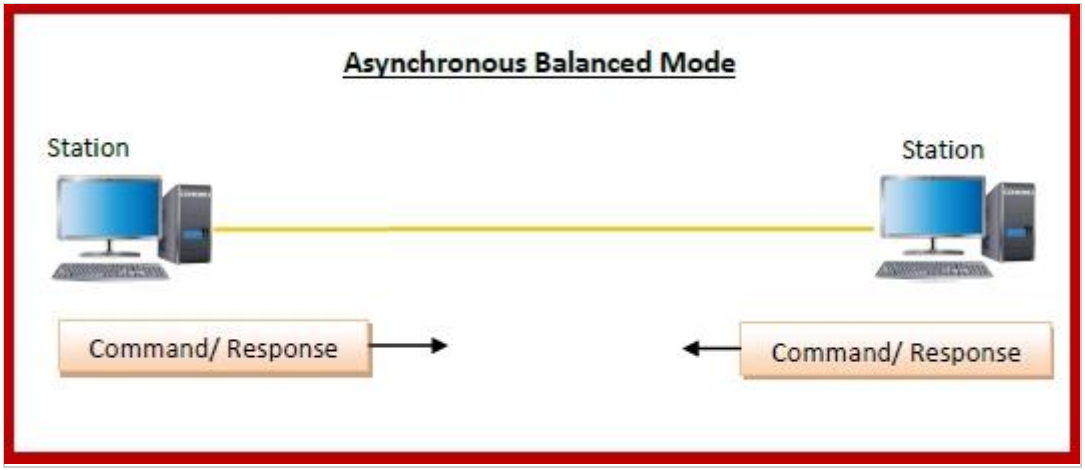
Transfer Modes

HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.

1. **Normal Response Mode (NRM)** − Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.



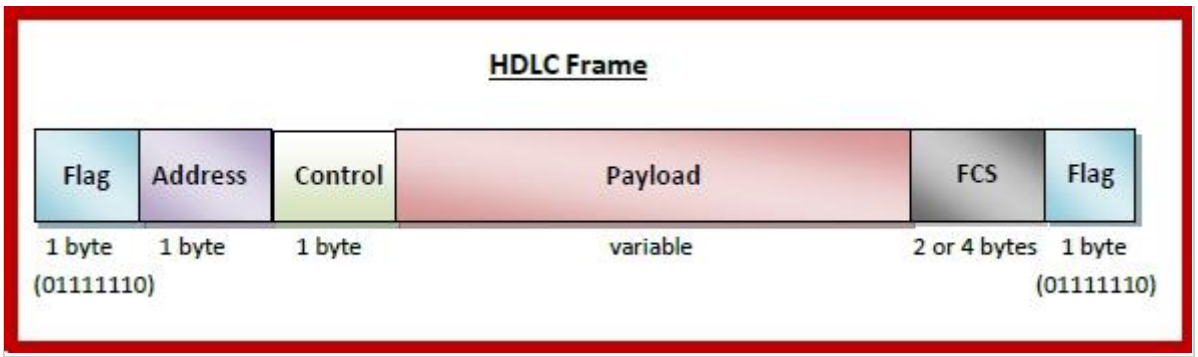
2. **Asynchronous Balanced Mode (ABM)** − Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.



HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are −

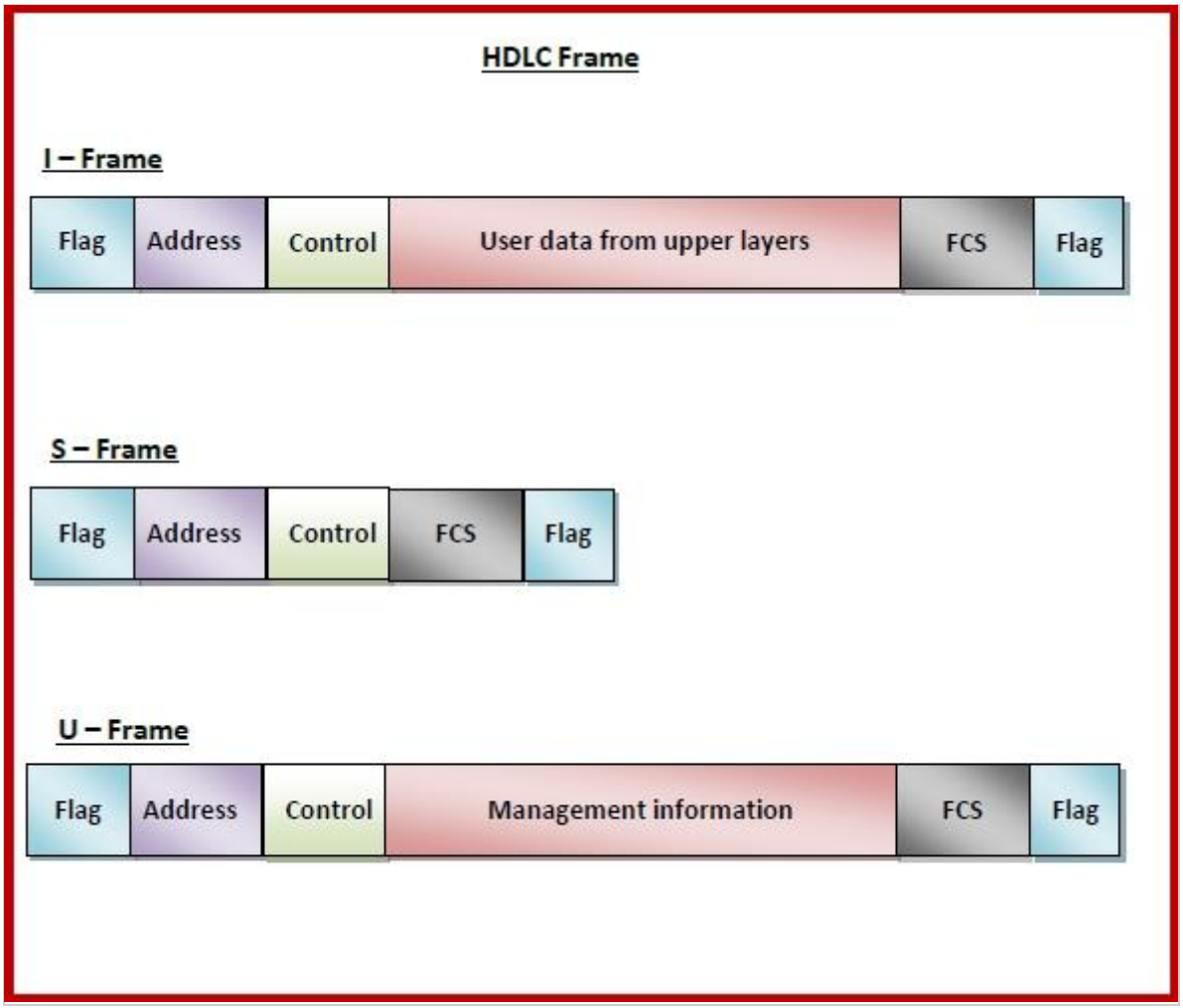
- **Flag** − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- **Control** − It is 1 or 2 bytes containing flow and error control information.
- **Payload** − This carries the data from the network layer. Its length may vary from one network to another.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



Types of HDLC Frames

There are three types of HDLC frames. The type of frame is determined by the control field of the frame −

I-**frame** − I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.
II-**S-frame** − S-frames or Supervisory frames do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10.
III-**U-frame** − U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first two bits of control field of U-frame is 11.



Multi Protocol Label Switching (MPLS): It is an IP packet routing technique that routes IP packet through paths via labels instead of looking at complex routing tables of routers. This feature helps in increasing the delivery rate of IP packets.

MPLS uses layer 3 service i.e, Internet Protocol, and uses router as forwarding device. The traffic of different customers is separated from each other because MPLS works somewhat like VPN. It does not work like regular VPN that encrypts the data but it ensures packet from one customer cannot be received by another customer. An MPLS header is added to packet that lies between layers 2 and 3. Hence, it is also considers to be *Layer 2.5 protocol.*

MPLS Header – The MPLS Header is 32 bit long and is divided into four parts –

- **Label –** This field is 20 bit long and can take value b/w 0 & 220 – 1.
- **Exp –** They are 3 bits long and used for *Quality of Service(QoS)*.
- **Bottom of stack (S) –** It is of size 1 bit. MPLS labels are stacked one over other. If there is only one label remained in MPLS header, then its value is 1 otherwise 0.
- **Time to Live (TTL) –** It is 8 bit long and its value is decreased by one at each hop to prevent packet to get stuck in network.

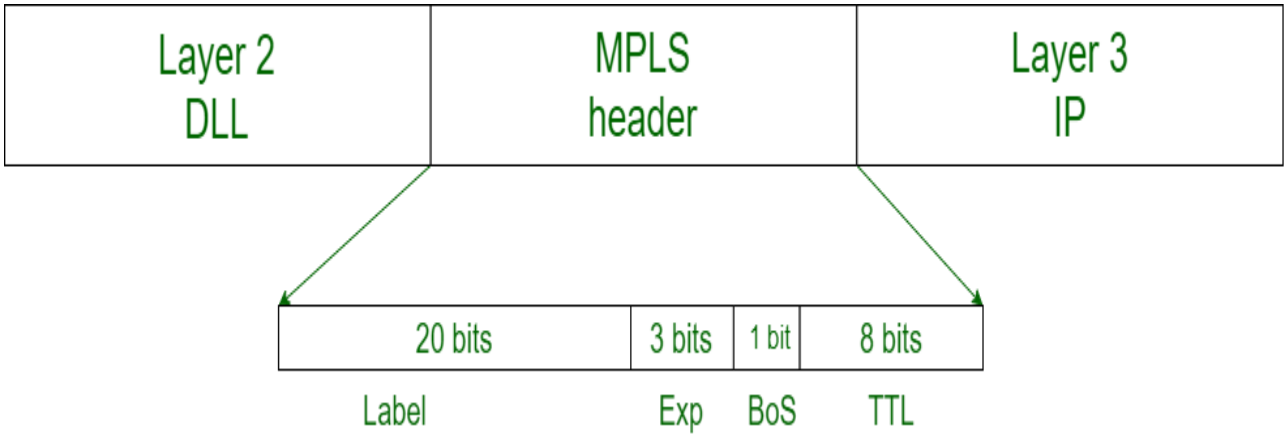


Figure – MPLS Header

Multiprotocol Label Switching (MPLS) Routing :

Forwarding in MPLS :
LSRs receive IP packet CE and add an MPLS header in between layer 3 and layer 2 means it encapsulates the link-layer i.e, layer 2 frames. This feature allows LSRs to support receiving packets containing frames from different protocols like Frame Relay, Metro Ethernet, etc, that's why it is called multi-protocol.

MPLS forwarding is based on label attached to IP packet. This label attachment is regulated by protocol called Label Distribution Protocol(LDP). Each LSR initially learns routes as normal routers do. This learning starts with PE routers. Each PE router learns routes to different subnets from CE router. Suppose PE router PE1 learns route to subnet (say subnet1) from CE router. Now PE1 will add label to packet, forward to its neighboring LSR, and tells them that if you receive packet which destination address to subnet1 then forward it to me.

Again this process is repeated by this LSR. In this way, LSR learns routes and add this information in *Label Forwarding Information Base(LFIB)*. Now if any PE receives packet with destination to subnet1, then looking at labels and LFIB, LSRs can easily forward IP packet.

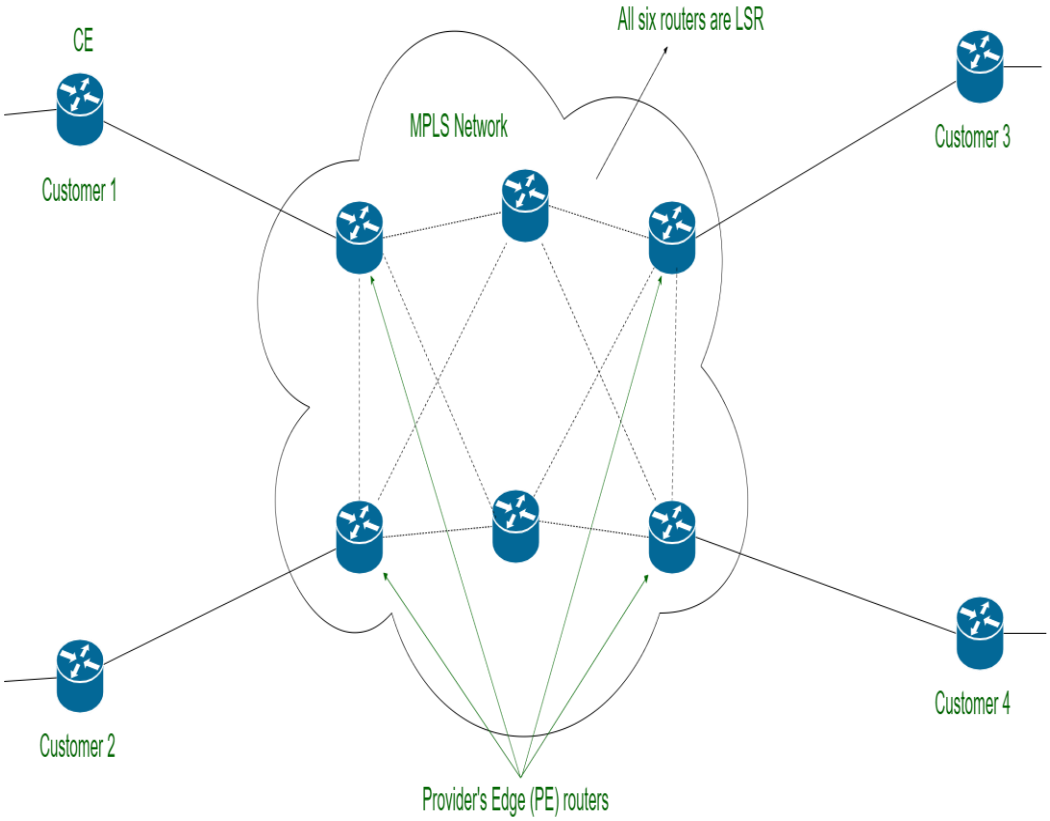


Figure – MPLS Network

Drawbacks of MPLS

Cost: MPLS is more expensive than regular Internet service.

Long setup time: Setting up complicated dedicated paths across one or more large networks takes time. LSPs have to be manually configured by the MPLS vendor or by the organization using MPLS. This makes it difficult for organizations to scale up their networks quickly.

Lack of encryption: MPLS is not encrypted; any attacker that intercepts packets on MPLS paths can read them in plaintext. Encryption has to be set up separately.

Cloud challenges: Organizations that rely on cloud services may not be able to set up direct network connections to their cloud servers, as they do not have access to the specific servers where their data and applications live.